Quantum Information Protocols with Gaussian States of Light

Jacobsen, Christian Scheffmann; Andersen, Ulrik Lund; Berg-Sørensen, Kirstine

Publication date:
2016

Document Version
Publisher's PDF, also known as Version of record

Citation (APA):
Jacobsen, C. S., Andersen, U. L., & Berg-Sørensen, K. (2016). Quantum Information Protocols with Gaussian States of Light. Department of Physics, Technical University of Denmark.

Quantum Information Protocols with Gaussian States of Light

Christian Scheffmann Jacobsen, M.Sc.Eng.

A thesis submitted in partial fulfilment of the requirements
for the PhD degree in Physics

Section for Quantum Physics and Information Technology
Department of Physics
Technical University of Denmark

August 2016

Principal supervisor:
Professor Ulrik Lund Andersen, Technical University of Denmark

PhD committee,
head of: Associate Professor Alexander Huck, Technical University of Denmark
opponent: Associate Professor Romain Alléaume, Télécom ParisTech
opponent: Professor Paolo Villoresi, University of Padova

Thesis,
submitted: August 31, 2016
defended: November 4th, 2016

Abstract

Quantum cryptography is widely regarded as the most mature field within the context of quantum information in the sense that its application and development has produced companies that base their products on genuine quantum mechanical principles. Examples include quantum random number generators and hardware for secure quantum key distribution. These technologies directly exploit quantum effects, and indeed this is where they offer advantages to classical products.

This thesis deals with the development and implementation of quantum information protocols that utilize the rather inexpensive resource of Gaussian states. A quantum information protocol is essentially a sequence of state exchanges between some number of parties and a certain ordering of quantum mechanical unitary operators performed by these parties. An example of this is the famous BB84 protocol for secret key generation, where photons in different polarization states are sent from one party to the other and subsequently detected.

In particular we introduce the idea of measurement device independence for continuous variable states and we present a proof-of-principle implementation of this protocol. Measurement device independence with Gaussian states is a promising avenue for the development of practical quantum key distribution with a relay network structure in environments where the distances are relatively short and there is a high number of users, such as an urban environment.

In addition to this we consider various point-to-point configurations that utilize Gaussian states to achieve security. Notably, we also present a novel experiment demonstrating the feasibility of delegated quantum computing on encrypted data, where we show that we can reliably encrypt and decrypt input and output states when a server with quantum computing capabilities performs Gaussian operations.

Dansk resumé

Kvantekryptografi bliver ofte betragtet som det mest modne felt indenfor kvanteinformationsteknologi, i den forstand at dets anvendelse og udvikling har produceret firmaer der baserer deres produkter på kvantemekaniske principper. Eksempler på dette inkluderer kvantetilfældighedsgeneratorer og hardware til sikker kvantenøgledistribution. Disse teknologier udnytter specifikke kvanteeffekter, og det er nøjagtig også i denne forstand at de er overlegne i forhold til de tilsvarende klassiske produkter.

Denne afhandling beskæftiger sig med udviklingen og implementationen af kvanteinformationsprotokoller der udnytter den relativt billige ressource udgjort af Gaussiske kvantetilstande. En kvanteinformationsprotokol er essentielt set en sekvens af tilstandsudvekslinger mellem et vist antal parter og en tilsvarende ordning af kvantemekaniske unitære operatorer. Et eksempel på dette kunne være den berømte BB84 protokol til at generere hemmelige nøgler, hvor fotoner i forskellige polarisationer bliver sendt fra en part til en anden og derpå bliver detekterede.

Vi introducerer i særdeleshed konceptet bag kvantekryptografi med målingsuafhængighed ved brug af koherente tilstande, og vi præsenterer en foreløbig implementation af denne protokol. Målingsuafhængighed med Gaussiske tilstande er et lovende koncept til udvikling af praktisk kvantenøgledistribution med en simplere netværksstruktur, specielt i miljøer hvor afstandene er relativt korte og der er et højt antal brugere, såsom en storby.

Udover dette betragter vi også flere punkt til punkt konfigurationer der har det til fælles at de udnytter Gaussiske tilstande til at generere kvantesikkerhed. Vi præsenterer desuden et nyt eksperiment der demonstrerer effektiviteten af uddelegerede kvanteberegninger. Vi viser at vi kan kryptere og dekryptere input og output tilstande på en konsistent måde når serveren benytter sig a Gaussiske operationer.

Acknowledgements

This thesis, and certainly the work I have performed over the past three years, would not have been possible without the support of a number of people. This is an attempt to mention them all by name. First of all to Ulrik Andersen, my supervisor. Thank you for keeping me busy, and for offering me this position in the first place. To Tobias Gehring, for being one of the smartest people I have ever met. I doubt that the lab would be what it is today without your insight into physics and electronics, and I am happy to count you as a friend. To Clemens Schäfermeier for being even more insistent upon keeping the lab clean than I ever was, and for sharing the joys and pains of PhD life. To Jonas Neergaard-Nielsen, for the appreciation we both share for clever Python code. To Ulrich Hoff, for all the dad jokes. To Adriano Berni and Hugo Kerdoncuff for sharing the office with me in the beginning, and to Rasmus Jensen for sharing it with me as I write this. To all the members of the QPIT section, past and present. Most of you really like NV centers. Some of us are tired of hearing so much about them.

A special thank you goes out to the brave people who "volunteered" to read parts of this thesis before its submission. Thank you to Tobias Gehring, Kevin Günthner, Mikkel Maag Pedersen, Ulrich Busk Hoff, Sepehr Ahmadi, Jonas Schou Neergaard-Nielsen and Rasmus Jensen. While the present manuscript is clearly much better in light of your constructive criticism, I fear that I can not guarantee the absence of errors within these pages, and I take full responsibility for them wherever they may be found.

Lastly, I would like to thank my family and friends for supporting me, even though most of you probably still do not entirely know what I have been spending so much time on, except that it involves lasers and that they are really cool. Finally, to Maria. You picked me, knowing that I was doing a PhD in physics, and I could not be happier that you did.

Christian Scheffmann Jacobsen
Section for Quantum Physics and Information Technology
Department of Physics
Technical University of Denmark
31st of August 2016

____

Christian Scheffmann Jacobsen

Contents

List of Figures

Mathematical symbols

$|n\rangle$ The n'th Fock state.

$|\alpha\rangle$ Coherent state with complex amplitude α.

$|P\rangle$ Phase quadrature operator eigenstate.

$|Q\rangle$ Amplitude quadrature operator eigenstate.

$\mathcal{F}$ Fidelity.

$\mathcal{N}$ Logarithmic negativity.

$\hat{a}$ The annihilation operator for a quantum harmonic oscillator.

$\hat{a}^\dagger$ The creation operator for a quantum harmonic oscillator.

$\mathbf{\Omega}$ Symplectic form matrix.

$\boldsymbol{Z}$ Mirror matrix.

$\hat{\boldsymbol{a}}$ The vectorized annihilation and creation operators for a quantum harmonic oscillator of N dimensions.

$\hat{\boldsymbol{X}}$ The vectorized quadrature operators for a quantum harmonic oscillator of N dimensions.

$\boldsymbol{X}$ Vector of the mean values of the vectorized quadrature operators for a quantum harmonic oscillator of N dimensions.

$\hat{Q}$ Amplitude quadrature operator.

$\hat{P}$ Phase quadrature operator.

$\hat{D}$ Weyl operator.

$\hat{\rho}$ Density matrix.

$\hbar$ Reduced Planck constant.

$\mathbf{\Gamma}$ Covariance matrix.

ν_k k'th symplectic eigenvalue.

T Optical transmission.

R Secret key rate.

$S(\hat{\rho})$ von Neumann entropy of the state $\hat{\rho}$.

$H(X)$ Shannon entropy of the random variable X.

$I(A:B)$ Classical mutual information between Alice and Bob.

$\chi(E)$ Holevo bound.

$W(\boldsymbol{X})$ Wigner function of $2N$ dimensions in coordinates of $\boldsymbol{X}$.

$\chi_C(\boldsymbol{\xi})$ Characteristic function.

$(\boldsymbol{d}, \boldsymbol{S})$ Mean value displacement and basis change matrix for a symplectic map.

$\mathbf{Var}\hat{A}$ Variance of the arbitrary operator $\hat{A}$.

$\mathbf{Tr}\hat{A}$ Trace of the arbitrary operator $\hat{A}$.

$\mathbb{C}$ The set of complex numbers.

$\mathbb{R}$ The set of real numbers.

$\mathbb{I}$ Identity matrix.

$\mathbb{N}$ The set of positive integers.

Acronyms

QKD quantum key distribution.

CVQKD continuous variable quantum key distribution.

DVQKD discrete variable quantum key distribution.

CV continuous variable.

DV discrete variable.

MDIQKD measurement device independent quantum key distribution.

CVMDIQKD continuous variable measurement device independent quantum key distribution.

EPR Einstein-Podolsky-Rosen.

PMMA PolyMethylMethAcrylate.

TEM transverse electromagnetic mode.

PDH Pound-Drever-Hall.

OPO optical parametric oscillator.

EOM electro-optical modulator.

PBS polarizing beam splitter.

PPKTP periodically poled potassium titanylphosphate.

HR highly reflective.

DC direct current.

AC alternating current.

ELO electronic local oscillator.

Introduction

The quantization of the electromagnetic field, as originally proposed by Planck to explain black-body radiation [1], was an attempt to dispel one of the two famous dark clouds of physics [2], a concept promoted William Thomson, also known as Lord Kelvin. This discovery motivated Einstein to develop a theory explaining the photoelectric effect, which would later earn him the Nobel prize in physics. With these two achievements, the development of quantum mechanics could begin in earnest.

It was soon realized that the very essence of quantum mechanics, the quantization, allowed for a host of phenomena that could not be explained with classical models. Describing light as photons was useful for Planck in describing black-body radiation, but a simple double slit experiment reveals that light can still exhibit wave behaviour and display interference patterns. This was explained by Bohr through the complementarity principle, which allows for both wave and particle behaviour depending on the measurement performed. It was particularly this focus by Bohr and his associates on the action of measurements and observers that caused much debate.

The superposition principle was exemplified by Erwin Schrödinger in his attempt to discredit the Copenhagen interpretation of Bohr and Heisenberg, with the famous cat that was dead and alive at the same time. Another famous paradox was that of Einstein, Podolsky, and Rosen in their argument for why quantum mechanics could not be regarded as complete, or describing physical reality [3]. In their gedanken experiment two particles with indeterminate position and momentum were to be sent far away from each other, for instance separate ends of the galaxy. Then a measurement on one particle, because of momentum conservation, would instantly give information on the other particle. This, Einstein contended, was a violation of locality and indicated the incompleteness of quantum mechanics. This phenomenon, which Einstein famously referred to as "spooky" action at a distance, is what we today name entanglement.

This problem of completeness was later addressed by Bell [4], who showed that a violation of his famous inequality would rule out the proposed model of local hidden variables. Einstein and his associates introduced the hidden variables as parameters that, if they were known, would give complete knowledge of the behaviour of the system and permit a deterministic prediction of its properties. In this way they hoped to avoid the purely probabilistic predictions that quantum mechanics offered. The term local refers to the assumption that the parts of the investigated system are not allowed to communicate faster than the speed of light. This leads in to a larger philosophical debate about the implications of the varying interpretations of quantum mechanics and the meaning of realism, which we will not be concerned with. Suffice to say that while quantum mechanics only provides the probabilities of certain events and no certainties, it is also this which gives the effects that we will exploit.

It was only much later that the quantum weirdness was merged with the ideas of information theory. A mathematical description of information was first developed by Shannon [5]. Classical information theory deals with the problem of how to efficiently encode a message to save space and makes fundamental statements about achievable error rates. In this theory information is quantified through the entropy, or uncertainty, of some probability distribution. Given the connection of quantum mechanics and probabilities it is therefore perhaps not surprising that the ideas that were used to develop information theory also turn out to be useful within quantum theory. The merging of these two fields has been named quantum information theory.

Since Weisner introduced the concept of quantum money in the early 70'ies [6], and with the subsequent invention of quantum key distribution (QKD) through the BB84 protocol by Bennett and Brassard in 1984 [7], the field of quantum information has seen explosive growth. Development of a universal quantum computer, as envisioned by Feynman [8], is pursued by researchers around the world, with many different physical systems as candidates [9].

Universal quantum computing is [10, 11, 12], however, by far not the only useful application of quantum mechanics to the world of information theory. Bit commitment [13, 14], secret sharing [15, 16], quantum key distribution [7, 17, 18], error correction [19], teleportation [20], boson sampling [21], generation of quantum random numbers [22], properties of black holes [23] and fundamental tests of physical reality [24, 25] are but some of the fascinating subjects that make up quantum information processing.

Initially, many of these ideas were developed with quantum bits or qubits in mind. In other words the basic constituents that carry the information are superposition states of the form

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \ ,$$

which can be represented using many different degrees of freedom, such as presence/absence of photons, polarization or electron spins. While classical bits can only take the values 0 and 1, quantum bits are allowed, through the superposition principle, to be 0, 1 and any combination in between. This difference hints at why quantum information processing is superior to what can be achieved classically in some scenarios [26].

An obvious example of this is the BB84 QKD protocol, where a sender Alice prepares a state $|\psi\rangle$ to be one of the four states $|H\rangle$, $|V\rangle$, $|+\rangle = \frac{1}{\sqrt{2}}|H\rangle+|V\rangle$ or $|-\rangle = \frac{1}{\sqrt{2}}|H\rangle-|V\rangle$, where H and V denote horizontal and vertical polarizations, respectively. Alice sends several states, randomly picked from this set, to the receiver Bob, who measures the incoming states either in a $|H\rangle, |V\rangle$ or $|+\rangle, |-\rangle$ basis. Knowing that it is not possible to reliably distinguish all four states at the same time, he picks his detection basis randomly. The protocol uses the properties of this 2-dimensional Hilbert space of linear polarization to provide quantum security. The security of the scheme is essentially a consequence of the no-cloning theorem due to Wootters and Zurek [27]. When Bob picks his detection basis uniformly randomly, he should expect to pick the right basis only half the time. If an eavesdropper attempted to intercept the qubit states when they travel from Alice to Bob, she will have to reproduce her state so Bob does not realize that something is missing. Since the no-cloning theorem states that she is unable to clone the state she steals, she will make errors in her copying procedure. These errors will be apparent to Alice and Bob when they compare the measurements with the prepared states, since the error rate will be above 50 %.

Following the invention of BB84, a host of related protocols were introduced [17, 28, 29] that exploit the properties of single photons in a similar way. We shall label protocols that use the particle properties of light as discrete variable (DV) protocols, with BB84 being the prime example of a discrete variable quantum key distribution (DVQKD) protocol.

In 1991 Ekert demonstrated [18] that quantum mechanical correlations between parts of Einstein-Podolsky-Rosen (EPR) states, i.e. entanglement, could provide the same quantum security that BB84 provides, since disturbance by an eavesdropper would prevent a genuine Bell violation [4] between the measurement outcomes of the honest parties [30, 31]. QKD using discrete variables has since developed into a vast field, leading to interesting concepts such as device independence [32, 33, 34, 35, 36, 37] and counterfactual communication [38]. At the same time, experimental realizations of these ideas have produced incredible results in terms of achievable distances [39] and viable in-field implementations [40, 41], which ensures that quantum cryptography is regarded as the most mature sub-field of quantum information processing.

It was not immediately realized that one does not need to resolve the particle like properties of light to exploit its quantum nature. If one can resolve the noise that results from the quantization of electro-magnetic fields, the so-called quantum or shot noise, it is possible to use continuous states of light to store quantum information, by encoding information in the complex amplitude of the electro-magnetic field. These states are collectively referred to as continuous variable states. This technique of storing information in the phase or amplitude of a laser beam is used in the classical world of optical communication, but here there is no need to build detectors that can resolve the quantum noise of the light or even use sources that allow it to be resolved in the first place.

Using these continuous variable (CV) states for QKD was proposed independently by Hillery, Reid, and Ralph [42, 43, 44]. The idea of using squeezed states to encode quantum information was further developed [45, 46], and not much later coherent states were also used for this purpose [47, 48], as they are simpler to produce experimentally. Since then, alternative protocols have been proposed, for example a simplified two-state protocol [49, 50], reminiscent of the original BB84 or B92 protocol. In 2004, a protocol without quadrature switching in the detection was introduced by Weedbrook *et al.* [51, 52]. More recent developments include the use of modulated entangled states [53], a continuous variable EPR source giving one-sided device independence [54], free space implementations in atmospheric channels [55], and new distance records in fiber [56, 57, 58].

On the theoretical side continuous variable quantum key distribution (CVQKD) works differently from its single photon counterpart. In practice the only difference between a discrete variable protocol with weak coherent pulses and a continuous variable protocol with coherent state encoding is the way the states are detected, but this has a profound impact on the theoretical treatment, as is true for much of quantum mechanics [59]. For discrete variable protocols the Hilbert space is typically of some finite dimension, but for continuous variables such a truncated space is not possible, which may significantly complicate the analysis [60, 61].

Aside from this difference, protocols in both regimes follow the same basic steps:

1. Alice and Bob connect via an authenticated channel. This step is crucial to avoid so-called man-in-the-middle attacks where the eavesdropper pretends to be Bob. This will usually require that Alice and Bob exchange some sort of password or key that they agreed on beforehand.

2. Exchanging randomly chosen quantum states. This step is where most of the variation between different protocols occurs.

3. Parameter estimation. Here Alice, or Bob, communicate some subset of their data to the other party to estimate errors.

4. Error correction. Error correction algorithms are applied to the data that was not revealed.

5. Privacy amplification. The key material produced by the protocol is distilled into a secure key using a certain family of two-universal hash functions [62, 63, 64, 65].

Initially, in step 4 a technique called direct reconciliation was used for CVQKD. Here Alice reveals some of her prepared states and lets Bob correct his measured subset of data to match this. This then lets Bob infer how to perform error correction on the measurements that were not revealed. Reverse reconciliation was conceived by

Grosshans *et al.* [66, 67], and was found to be superior to direct reconciliation, where the transmission loss is intrinsically limited to 3 dB. Here the roles are exactly reversed such that Bob reveals some of his measurements and lets Alice check with what she prepared and correct accordingly.

The sending of the message itself from Alice to Bob then takes place after the key material has been exchanged. In this final step all protocols go back to the only known encryption procedure which is known to have information theoretical security, the Vernam cipher or one-time pad [68]. Indeed, information theoretical security is exactly the motivation for this heavy investment in resources for the development of robust in-field QKD protocols.

Modern cryptography is divided into two parts. Firstly, the public key algorithms which are based on mathematical problems where checking solutions is easy but finding new ones is believed to be hard, such that it is easy to encrypt, but hard to decrypt unless one knows some initial parameter. Secondly, the private key algorithms where key material has been exchanged beforehand, such that Alice and Bob share a key. They then use a private key algorithm and knowledge of the key to encrypt and then decrypt a message. All of these protocols provide what is known as computational security, where security is achievable if one assumes that the eavesdropper has limited computing. So far, only the Vernam cipher is able to provide information theoretical security, where no assumptions on the power of the eavesdropper are made.

The Vernam cipher falls within the category of private key algorithms. It is, compared to the modern crypto algorithms, remarkably simple to implement. The secret key and the message are represented in a binary alphabet. Then, given that the key length is at least that of the message, perform an exclusive-or operation on all bits in the message. This is especially convenient for Bob because the decryption operation is another exclusive-or operation between the bits in the padded message and the secret key. The secret key may only be used once in this way, because a second use allows an eavesdropper to consider the exclusive-or of two padded messages, which is equivalent to an exclusive-or of the plaintexts. Using this fact may give the eavesdropper additional information and information theoretical security can no longer be guaranteed. Other more complicated algorithms allow for the recycling of key material and the process of breaking them is known as differential cryptoanalysis [68]. For certain types of attacks one may set up probability bounds for the likelihood of a security breach, but in general the security of these schemes is unproven.

In this context, QKD may be seen as an attempt at providing information theoretical security, by exchanging key material without limiting the eavesdropper. As an additional motivation, one of the most ubiquitous algorithms in modern cryptosystems, the Rivest-Shamir-Adleman algorithm [68] relies on the difficulty of factorizing prime number products. However, Shor has shown [26] that if a universal quantum computer is ever constructed, there exists an algorithm that can do this factorization efficiently, rendering this encryption technique obsolete.

In this thesis we will mainly be focused on the security provided by CVQKD protocols, and variations in the implementation of the quantum state exchange. In discussing the security of these CVQKD schemes the eavesdropping strategies available to any malicious party on a continuous variable protocol are usually divided into three broad categories. These are, from weakest to strongest, individual attacks, collective attacks, and coherent attacks [69, 70, 30, 71, 72]. When an asymptotic limit of infinitely many exchanged states is taken, one is able to make arguments from symmetry such that the two categories of collective and coherent attacks become equivalent [73]. However, if this assumption is not made the security proofs of continuous variable protocols are not as far along as for their discrete variable counterparts, and in particular the security bounds they provide are not known to be tight, which limits the effective distance [74, 75, 76, 77].

If this challenge is overcome then CVQKD offers interesting advantages over the corresponding DVQKD protocols. Firstly, CVQKD can typically be performed with equipment that is already used for classical optical communication, and so it is technologically closer to an already well developed industry. Secondly, CVQKD could potentially offer much higher rates for the generation of secure keys that comparable DVQKD protocols. This is because DVQKD protocols tend to be limited by the source repetition rate, but CVQKD does not suffer from this problem as the light phase and amplitude can be modulated well into the GHz range.

An interesting subclass of continuous variable states, especially for the purpose of QKD, are the Gaussian states, that is states where the probability distributions of the components of the complex electro-magnetic field amplitude are Gaussian distributions [71]. Indeed, many of the protocols described above make use of exactly this class of states.

It turns out that such states can be described rather simply and conveniently by the so-called covariance matrix formalism and symplectic spaces [71]. If the detection scheme can also be described in a Gaussian way there are no-go theorems that somewhat limit what can be achieved with these states [78, 79, 80]. In spite of this however, these systems have several satisfying properties in the context of information theory [5, 81]. This thesis deals with protocols that employ these states and detection schemes, particularly continuous variable quantum key distribution protocols.

We shall in particular investigate relay configurations of three parties for the purposes of QKD, the effects of correlated noise in such relay configurations and how this affects the distribution of entanglement, the effects of trusted thermal noise in standard coherent state protocols, a way to simplify the practical implementation of the standard coherent state protocol, the use of squeezing together with coherent state alphabets, and the use of thermal noise for one-party encryption.

This one-party encryption is motivated by the wish to implement secure delegated quantum computing. Secure in this context means that the server providing the quantum computing capabilities cannot be trusted, and so the input and output states are hidden from it, through an encryption procedure that uses purely Gaussian operations.

Thesis structure

- Chapter 2 serves as an introduction to the theory behind the field of Gaussian quantum information.

- Chapter 3 introduces the experimental techniques and tools that were used in the experiments described in the later chapters

- Chapter 4 presents the theory and proof-of-principle experiment of the first ever continuous variable measurement device independent quantum key distribution (CVMDIQKD) protocol.

- Chapter 5 presents the theory of the measurement device independent quantum key distribution (MDIQKD) protocol in the context of non-Markovian noise and what this noise implies for other related protocols that utilize, either virtual or real, entanglement. These predictions are investigated through an experiment on a noisy MDIQKD protocol which is also presented.

- Chapter 6 restates a theoretical prediction regarding the performance of point-to-point CVQKD protocols with coherent states in the presence of preparation noise and tests this prediction through an experimental implementation.

- Chapter 7 presents the theory behind and the first experimental implementation of a CVQKD protocol utilizing a continuous coherent state alphabet in only one quadrature.

- Chapter 8 presents a novel approach to decoupling a potential eavesdropper from a quantum channel through the use of squeezed states. The conditions for the validity of this decoupling scheme are discussed and it is tested experimentally.

- Chapter 9 introduces the idea of delegated continuous variable quantum computing with encrypted input states, and the encryption scheme is tested on a number of relatively simple gates from the continuous variable universal quantum computing set.

- Chapter 10 provides a comprehensive conclusion on the work performed in the previous chapters.

Theory

The purpose of this chapter is to introduce the theoretical tools we require to describe Gaussian quantum states. We follow mainly the review of Weedbrook *et al.* [71].

Quantization of the electromagnetic field

The first section of this chapter deals with the theory describing the various optical elements and tools that are available in the laboratory for performing experiments with continuous variable states of light. Consider the electromagnetic field of a light beam confined to propagation in a cavity of length L along the z-axis [29],

$$E_x(z,t) = \sqrt{\frac{2\omega^2}{V\varepsilon_0}} q(t)\sin(kz) \ , \tag{2.1.1}$$

where the field is polarized along the x-axis. ω is the angular frequency of the light, $k = \frac{\omega}{c}$ is the wave number and V is the cavity volume. c is the speed of light in vacuum and ε_0 is the vacuum permittivity. $q(t)$ is a time dependent factor, that we shall essentially use as a rescaled field amplitude. It serves the purpose of a canonical position. The corresponding magnetic field is

$$B_y(z,t) = \frac{\mu_0\varepsilon_0}{k}\sqrt{\frac{2\omega^2}{V\varepsilon_0}} \dot{q}(t)\cos(kz) \ , \tag{2.1.2}$$

where $\dot{q}(t) = p(t)$ is the canonical momentum and μ_0 is the vacuum permeability. The energy of this field can be represented by a Hamiltonian H, such that

$$H = \frac{1}{2}(p^2 + \omega^2 q^2) \ . \tag{2.1.3}$$

This expression is immediately recognized as a harmonic oscillator. The procedure for the quantization of the harmonic oscillator is well known [59], and we therefore introduce the ladder operators,

$$\hat{a} = \frac{1}{\sqrt{2\hbar\omega}}(\omega\hat{q} + i\hat{p}) \qquad , \qquad \hat{a}^\dagger = \frac{1}{\sqrt{2\hbar\omega}}(\omega\hat{q} - i\hat{p}) \ , \tag{2.1.4}$$

where $\hbar$ is the reduced Planck constant. These operators fulfil the relation,

$$[\hat{a}, \hat{a}^\dagger] = 1 \; . \tag{2.1.5}$$

These operators are not Hermitian and are therefore not observable variables. We may further define the photon number operator,

$$\hat{n} = \hat{a}^\dagger \hat{a} \; . \tag{2.1.6}$$

Setting $\hbar = 2$, for normalization purposes, we may write the unitless Hermitian quadrature operators for the electromagnetic field as,

$$\hat{Q} = \hat{a} + \hat{a}^\dagger \qquad , \qquad \hat{P} = i(\hat{a}^\dagger - \hat{a}) \; , \tag{2.1.7}$$

and their commutation relation is,

$$[\hat{Q}, \hat{P}] = 2i \; . \tag{2.1.8}$$

This commutation relation implies that $\hat{Q}$ and $\hat{P}$ are canonically conjugate operators, such that they fulfil a Heisenberg inequality of the form,

$$\mathrm{Var}(\hat{Q}) \cdot \mathrm{Var}(\hat{P}) \geq 1 \; , \tag{2.1.9}$$

where the variance of an operator $\hat{A}$ is defined such that,

$$\mathrm{Var}(\hat{A}) = \langle \hat{A}^2 \rangle - \langle \hat{A} \rangle^2 \; , \tag{2.1.10}$$

where $\langle \hat{A} \rangle$ is the mean or expectation value of $\hat{A}$ [59]. In general, we may consider the electromagnetic field as having a complex field amplitude, where $\hat{Q}$ and $\hat{P}$ are components of this complex number. In this sense, we may choose to view $\hat{Q}$ as an operator governing the amplitude of a complex number, and $\hat{P}$ as the operator governing the phase of this complex number. The fact that the mathematical structure of these operators mimics that of a quantum harmonic oscillator is part of what has made quantum optics such a rich field [82].

We are typically interested in interactions between electromagnetic fields, and to describe these interactions we shall have need of the concept of a mode. The concept of a mode is sometimes ambiguous and used for various purposes in the literature. A mode is in this thesis understood to refer to one or more of the following:

- Spatial mode. Various patterns of light intensity distribution in the plane orthogonal to the polarization. Transverse electromagnetic modes (TEMs) are a common example of this [83].

- Frequency mode. States of light generated at varying frequencies occupy different modes even though they might be spatially identical.

- Polarization mode. The orientation of the electromagnetic field oscillations with respect to the direction of propagation.

Each mode has its own creation and annihilation operators, $\hat{a}_{\Omega,\sigma,p}$ and $\hat{a}^{\dagger}_{\Omega,\sigma,p}$, where the subscripts are used to denote frequency, polarization and spatial profile. These subscripts are typically understood from the context. Operators in different modes commute by default, such that we only expect interactions between modes with the same features, i.e. for two electromagnetic fields to interfere, they need to have identical spatial, frequency and polarization mode numbers.

It is convenient to vectorize the commutation relations above, such that for N modes, we have the vector of ladder operators and the vector of quadrature operators,

$$\hat{\boldsymbol{a}} = \begin{pmatrix} \hat{a}_1 \\ \hat{a}_1^{\dagger} \\ \hat{a}_2 \\ \hat{a}_2^{\dagger} \\ \vdots \\ \hat{a}_N \\ \hat{a}_N^{\dagger} \end{pmatrix} \quad , \quad \hat{\boldsymbol{X}} = \begin{pmatrix} \hat{Q}_1 \\ \hat{P}_1 \\ \hat{Q}_2 \\ \hat{P}_2 \\ \vdots \\ \hat{Q}_N \\ \hat{P}_N \end{pmatrix} . \tag{2.1.11}$$

Then the commutation relations become,

$$[\hat{\boldsymbol{a}}_i, \hat{\boldsymbol{a}}_j] = \boldsymbol{\Omega}_{ij} \quad , \quad [\hat{\boldsymbol{X}}_i, \hat{\boldsymbol{X}}_j] = i2\boldsymbol{\Omega}_{ij} \ , \tag{2.1.12}$$

where $\boldsymbol{\Omega}$ is a matrix of the form

$$\boldsymbol{\Omega} = \bigoplus_{k=1}^{N} \boldsymbol{\omega} \quad , \quad \boldsymbol{\omega} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} . \tag{2.1.13}$$

For a single mode the quadrature operators have the eigenstates,

$$\hat{Q}|Q\rangle = Q|Q\rangle \quad , \quad \hat{P}|P\rangle = P|P\rangle \ . \tag{2.1.14}$$

The eigenvalues Q and P form a continuous spectrum, such that $Q \in \mathbb{R}$ and $P \in \mathbb{R}$, i.e. they are continuous variables as opposed to the number of photons in the state, which takes integer values. These quadrature states form a complete and orthonormal basis, such that the conditions for orthogonality,

$$\langle Q|Q'\rangle = \delta(Q - Q') \quad , \quad \langle P|P'\rangle = \delta(P - P') \ , \tag{2.1.15}$$

and completeness,

$$\int |Q\rangle\langle Q| \,\mathrm{d}Q = \int |P\rangle\langle P| \,\mathrm{d}P = 1 \ , \tag{2.1.16}$$

are fulfilled. The spectral decompositions of the quadrature operators are

$$\hat{Q} = \int_{-\infty}^{\infty} Q|Q\rangle\langle Q| \,\mathrm{d}Q \quad , \quad \hat{P} = \int_{-\infty}^{\infty} P|P\rangle\langle P| \,\mathrm{d}P \ . \tag{2.1.17}$$

We may express any state $|\Psi\rangle$ in the basis formed by the quadrature states, such that we obtain the quadrature wave functions,

$$\Psi(Q) = \langle Q|\Psi\rangle \qquad , \qquad \tilde{\Psi}(P) = \langle P|\Psi\rangle \ , \tag{2.1.18}$$

which are related by the Fourier transform,

$$\Psi(Q) = \frac{1}{2\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-iPQ/2}\tilde{\Psi}(P)\,\mathrm{d}P \ . \tag{2.1.19}$$

In fact, for the quadrature states,

$$|Q\rangle = \frac{1}{2\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-iQP/2}|P\rangle\,\mathrm{d}P \tag{2.1.20}$$

$$|P\rangle = \frac{1}{2\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-iQP/2}|Q\rangle\,\mathrm{d}Q \ . \tag{2.1.21}$$

The probability distributions $|\Psi(Q)|^2$ and $|\tilde{\Psi}(P)|^2$ determine the measurement outcomes Q and P respectively. Continuous variable detection methods such as homodyne and heterodyne detection, described in Sections 3.7.1 and 3.7.2, have the variables Q and P as measurement outcomes, and so with successive measurements of the same state they generate statistics that follow the distributions $|\Psi(Q)|^2$ and $|\tilde{\Psi}(P)|^2$.

Phase space

Classically, phase spaces are employed to depict the evolution of two or more parameters, for example position and momentum, bound to each other by some mathematical constraint describing a physical process, such as a set of differential equations. One famous example of this is the Lorentz attractor from the field of chaos theory [84]. In quantum optics, phase spaces are also used for illustrative purposes, but in a somewhat different manner. Because of the inherent uncertainty in quantum mechanics a physical state is never located in a specific point in phase space, but is rather smeared out over an area to indicate the probability distribution of the particular variable. In the case of continuous variable quantum optics, the two operators of importance are the quadrature operators $\hat{Q}$ and $\hat{P}$. To define a phase space of N modes, suppose we have a vector $\boldsymbol{X} \in \mathbb{R}^{2N}$ of eigenvalues of $\hat{\boldsymbol{X}}$,

$$\boldsymbol{X} = \begin{pmatrix} Q_1 \\ P_1 \\ Q_2 \\ P_2 \\ \vdots \\ Q_N \\ P_N \end{pmatrix} \ . \tag{2.2.1}$$

We define a real symplectic space by $\boldsymbol{\mathcal{K}} = (\mathbb{R}^{2N}, \boldsymbol{\Omega})$, such that the vector $\boldsymbol{X}$ takes its values in this symplectic space, and $\boldsymbol{\Omega}$ is defined in Equation (2.1.13). This space is also called phase space [71]. Loosely speaking, the symplectic form enforces a structure on phase space, that forces it to obey the vectorized commutation relation defined in Equation (2.1.12). To see this, consider two arbitrary vectors $\boldsymbol{X}$ and $\boldsymbol{\xi}$, that each have $2N$ real values and live in the symplectic space. The scalar product in the symplectic space is defined as [85],

$$(\boldsymbol{\xi}, \boldsymbol{X}) = \boldsymbol{\xi}^T \cdot \boldsymbol{\Omega} \cdot \boldsymbol{X} = \sum_{i,j=1}^{2N} \boldsymbol{\Omega}_{ij} \boldsymbol{\xi}_i \boldsymbol{X}_j \ . \tag{2.2.2}$$

Basis changes in the symplectic space must preserve the scalar product. For some arbitrary basis change matrix $\boldsymbol{S}$ we may therefore write,

$$\boldsymbol{\xi}^T \cdot \boldsymbol{\Omega} \cdot \boldsymbol{X} = (\boldsymbol{S}\boldsymbol{\xi})^T \cdot \boldsymbol{\Omega} \cdot (\boldsymbol{S}\boldsymbol{X}) \tag{2.2.3}$$

$$\Updownarrow$$

$$\boldsymbol{\xi}^T \cdot \boldsymbol{\Omega} \cdot \boldsymbol{X} = \boldsymbol{\xi}^T \cdot \boldsymbol{S}^T \boldsymbol{\Omega} \boldsymbol{S} \cdot \boldsymbol{X} \ . \tag{2.2.4}$$

We require that this holds for all $\boldsymbol{\xi}, \boldsymbol{X}$, and therefore arrive at the condition,

$$\boldsymbol{\Omega} = \boldsymbol{S}^T \boldsymbol{\Omega} \boldsymbol{S} \ . \tag{2.2.5}$$

In other words, any transformation in the symplectic space must preserve the commutation relation in Equation (2.1.12). Any transformation that does not preserve this structure of phase space is considered unphysical.

The density matrix

In general we describe a quantum state by its density matrix [59],

$$\hat{\rho} = \sum_i p_i |\phi_i\rangle\langle\phi_i| \ , \tag{2.3.1}$$

such that the state $\hat{\rho}$ is constructed from the basis states $|\phi_i\rangle$ in the Hilbert space $\mathcal{H}$, weighted with the probabilities p_i. These probabilities must sum to one, such that

$$\sum_i p_i = 1 \ . \tag{2.3.2}$$

A proper density matrix fulfils three properties, those of hermiticity $\hat{\rho} = \hat{\rho}^\dagger$, positive semi-definiteness $\langle u|\hat{\rho}|u\rangle \geq 0$, where $|u\rangle$ is a state in an arbitrary basis, and normalization $\mathrm{Tr}\hat{\rho} = 1$. Here the trace of an operator $\hat{A}$ is the sum of the diagonal elements,

$$\mathrm{Tr}\hat{A} = \sum_i \langle u_i|\hat{A}|u_i\rangle, \tag{2.3.3}$$

where $|u_i\rangle$ is an arbitrary set of complete orthonormal basis states for the Hilbert space in which $\hat{A}$ is defined. Thus, the trace is invariant under basis changes. In particular,

$$\mathrm{Tr}\hat{A} = \sum_i \lambda_i \ , \tag{2.3.4}$$

where λ_i are the eigenvalues of $\hat{A}$. For a pure state we have $\hat{\rho} = |\phi\rangle\langle\phi|$, and equivalently, a density matrix representing a pure state fulfils $\mathrm{Tr}\hat{\rho}^2 = 1$.

We generalize the mean value of an arbitrary operator $\hat{A}$, where for pure states $\langle\hat{A}\rangle = \langle\phi|\hat{A}|\phi\rangle$. For a density matrix, that may or may not be pure, we instead define the mean value as [59],

$$\langle\hat{A}\rangle = \mathrm{Tr}(\hat{A}\hat{\rho}) \ . \tag{2.3.5}$$

Fidelity

We define the fidelity between two quantum states, $\hat{\rho}_0$ and $\hat{\rho}_1$, by the expression [71, 86, 87],

$$\mathcal{F} = \left(\mathrm{Tr}\sqrt{\sqrt{\hat{\rho}_0}\hat{\rho}_1\sqrt{\hat{\rho}_0}}\right)^2 \ , \tag{2.3.6}$$

which is a real number between 0 and 1, that indicates how close two states are to each other. When $\mathcal{F} = 0$, the two states are orthogonal, and when $\mathcal{F} = 1$, the two states are exactly identical. This serves as a distance measure between states, and is typically used to quantify the performance of a protocol, a common example being that of quantum state teleportation [20]. In particular for Gaussian states we have,

$$\mathcal{F} = \frac{2}{\sqrt{\Delta+\delta}-\sqrt{\delta}} \exp\left(-\frac{1}{2}\boldsymbol{X}_\Delta^T(\boldsymbol{\Gamma}_{\hat{\rho}_0}+\boldsymbol{\Gamma}_{\hat{\rho}_1})^{-1}\boldsymbol{X}_\Delta\right) , \tag{2.3.7}$$

with the determinants $\Delta = \det(\boldsymbol{\Gamma}_{\hat{\rho}_0} + \boldsymbol{\Gamma}_{\hat{\rho}_1})$ and $\delta = (\det\boldsymbol{\Gamma}_{\hat{\rho}_0} - 1)(\det\boldsymbol{\Gamma}_{\hat{\rho}_1} - 1)$, and the vectorized mean value $\boldsymbol{X}_\Delta = \boldsymbol{X}_{\hat{\rho}_1} - \boldsymbol{X}_{\hat{\rho}_1}$.

Wigner functions

The main object of interest in the quantum mechanical phase space is the Wigner function. To define the concept of the Wigner function, we introduce the Weyl, or displacement, operator [29, 71],

$$\hat{D}(\boldsymbol{\xi}) = \exp(i\hat{\boldsymbol{X}}^T\boldsymbol{\Omega}\boldsymbol{\xi}) \ , \tag{2.4.1}$$

where $\hat{\boldsymbol{X}}$ is the vector of quadrature operators of N modes, and $\boldsymbol{\xi}$ is a vector that contains the displacements in phase space. We further introduce the characteristic function,

$$\chi_C(\boldsymbol{\xi}) = \mathrm{Tr}(\hat{\rho}\hat{D}(\boldsymbol{\xi})) \ , \tag{2.4.2}$$

where $\hat{\rho}$ is a density matrix describing the state in question. To define the Wigner function, we take the Fourier transform of the characteristic function in Equation (2.4.2) of N modes,

$$W(\boldsymbol{X}) = \frac{1}{(2\sqrt{\pi})^{2N}} \int_{\mathbb{R}^{2N}} \exp(-i\boldsymbol{X}^T\boldsymbol{\Omega}\boldsymbol{\xi}/2)\chi_C(\boldsymbol{\xi})\,\mathrm{d}^{2N}\boldsymbol{\xi} \ , \tag{2.4.3}$$

In this way, for an arbitrary $\hat{\rho}$, there exists a unique Wigner representation of the form given in Equation (2.4.3). The Wigner function is a pseudo-probability distribution, in the sense that it may take negative values for some $\hat{\rho}$, and this negativity is a clear sign of a non-classical state, which occurs for example for the single photon state. It is also normalized so that,

$$\int_{\mathbb{R}^{2N}} W(\boldsymbol{X})\mathrm{d}^{2N}\boldsymbol{X} = 1 \ . \tag{2.4.4}$$

For a single mode, we may rewrite Equation (2.4.3), such that it depends explicitly on $\hat{\rho}$,

$$W(Q,P) = \frac{1}{4\pi}\int_{-\infty}^{\infty} e^{iPx/2}\langle Q + x/2|\hat{\rho}|Q - x/2\rangle\,\mathrm{d}x \ . \tag{2.4.5}$$

The marginal distributions of $W(Q,P)$,

$$W_Q(Q) = \int_{-\infty}^{\infty} W(Q,P)\,\mathrm{d}P \qquad , \qquad W_P(P) = \int_{-\infty}^{\infty} W(Q,P)\,\mathrm{d}Q \ , \tag{2.4.6}$$

are exactly the quadrature probability distributions defined through Equation (2.1.18). For Gaussian states, the measurement outcomes Q and P are probabilistically distributed according to Gaussian distributions defined purely by their first and second moments, i.e. mean value and variance. In particular for a Gaussian state of N modes with a $2N \times 2N$ covariance matrix $\boldsymbol{\Gamma}_{\hat{\rho}}$ and a mean value vector $\bar{\boldsymbol{X}}$ of $2N$ components, we have

$$W(\boldsymbol{X}) = \frac{1}{(2\pi)^N\sqrt{\det\boldsymbol{\Gamma}_{\hat{\rho}}}}\exp\left(-\frac{1}{2}(\boldsymbol{X}-\bar{\boldsymbol{X}})^T\boldsymbol{\Gamma}_{\hat{\rho}}^{-1}(\boldsymbol{X}-\bar{\boldsymbol{X}})\right) \ , \tag{2.4.7}$$

such that the Wigner function itself is also a Gaussian. For a single mode, the covariance matrix is,

$$\boldsymbol{\Gamma}_{\hat{\rho}} = \begin{bmatrix} \mathrm{Tr}(\hat{\rho}\hat{Q}^2) - \mathrm{Tr}(\hat{\rho}\hat{Q})^2 & \mathrm{Tr}(\hat{\rho}\hat{Q}\hat{P}) - \mathrm{Tr}(\hat{\rho}\hat{Q})\mathrm{Tr}(\hat{\rho}\hat{P}) \\ \mathrm{Tr}(\hat{\rho}\hat{Q}\hat{P}) - \mathrm{Tr}(\hat{\rho}\hat{Q})\mathrm{Tr}(\hat{\rho}\hat{P}) & \mathrm{Tr}(\hat{\rho}\hat{P}^2) - \mathrm{Tr}(\hat{\rho}\hat{P})^2 \end{bmatrix} \ . \tag{2.4.8}$$

Fock states and the vacuum

With the creation and annihilation operators defined, we may consider a special basis of the Hilbert space that contains the wavefunctions for the quantum harmonic oscillator. These special basis states are directly related to the number of excitations, in this case photons, in the oscillator, and we call these states the Fock states. They are labelled as $|n\rangle$, where $n \in \mathbb{N}$. They form a complete and orthonormal basis in the Hilbert space and so they fulfil,

$$\langle n|m\rangle = \delta_{nm} \qquad , \qquad \sum_n |n\rangle\langle n| = \mathbb{I} \ . \tag{2.5.1}$$

The creation and annihilation operators act on these states such that,

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle \qquad , \qquad \hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle \ , \tag{2.5.2}$$

with the special case,

$$\hat{a}|0\rangle = 0 \ . \tag{2.5.3}$$

$|0\rangle$ is also called the vacuum state, and is the state which contains no photons, but has $\frac{1}{2}\hbar\omega$ energy, also called the zero point energy. Measuring a vacuum state in the quadrature basis gives a Gaussian marginal distribution, that is rotationally symmetric in phase space. By finding the quadrature wavefunction $\langle Q|0\rangle$, and using Equation (2.4.5), we can calculate the Wigner function for a vacuum state,

$$W_{\text{vac}}(Q,P) = \frac{1}{2\pi}\exp\left(-\frac{1}{2}(Q^2+P^2)\right) \ . \tag{2.5.4}$$

We recognize this as a Gaussian of zero mean and covariance,

$$\mathbf{\Gamma}_{\text{vac}} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \ . \tag{2.5.5}$$

Another important state, expressed in the Fock basis, is the thermal state,

$$\hat{\rho}_{\text{th}} = \sum_{m=0}^{\infty} \frac{\bar{n}^m}{(\bar{n}+1)^{m+1}}|m\rangle\langle m| \ . \tag{2.5.6}$$

It is a statistical mixture of Fock states, with no correlations between the excitations. Indeed, it directly follows the form of Equation (2.3.1), as a statistical mixture of Fock states, and we see that the probability of a certain photon contribution is given by the factor,

$$p_m = \frac{\bar{n}^m}{(\bar{n}+1)^{m+1}} \ , \tag{2.5.7}$$

which is determined solely by the mean photon number $\bar{n}$. In phase space, the thermal state is described by the Wigner function,

$$W_{\mathrm{th}}(Q,P) = \frac{1}{2\pi(2\bar{n}+1)} \exp\left(-\frac{1}{2(2\bar{n}+1)}(Q^2+P^2)\right) \ . \tag{2.5.8}$$

It is a Gaussian distribution of mean value **0** and covariance matrix,

$$\mathbf{\Gamma}_{\mathrm{th}} = \begin{bmatrix} 2\bar{n}+1 & 0 \\ 0 & 2\bar{n}+1 \end{bmatrix} \ . \tag{2.5.9}$$

The vacuum state and the thermal state may be regarded as the most fundamental Gaussian states, and we will see in Section 2.7 that the vacuum state can be transformed into any Gaussian state.

Coherent states

We introduce the coherent state, as it is what we shall use to store our quantum information in many of the protocols described later. The coherent state is defined as the eigenstate of the annihilation operator,

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle \ , \tag{2.6.1}$$

where $\alpha \in \mathbb{C}$. This relation can be used to show that, in the Fock basis,

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle \ . \tag{2.6.2}$$

From this, we can show that for two coherent states, $|\alpha\rangle$ and $|\beta\rangle$, the overlap is [29, 71],

$$|\langle\beta|\alpha\rangle|^2 = e^{-|\beta-\alpha|^2} \ . \tag{2.6.3}$$

This is important for quantum key distribution, because it implies that no two coherent states are perfectly orthogonal. This provides security through the no-cloning theorem [27]. It also implies that the coherent states form an overcomplete basis for the Hilbert space, so the identity becomes [29],

$$\mathbb{I} = \frac{1}{\pi} \int_{\mathbb{C}} |\alpha\rangle\langle\alpha| \, \mathrm{d}^2\alpha \ . \tag{2.6.4}$$

The coherent state $|\alpha\rangle$ has the Wigner function,

$$W_{\mathrm{coh}}(Q,P) = \frac{1}{2\pi} e^{-\frac{1}{2}((Q-\Re[\alpha])^2+(P-\Im[\alpha])^2)} \ , \tag{2.6.5}$$

which we recognize as a 2D Gaussian of variance 1 and mean value $\boldsymbol{\alpha} = (\Re[\alpha], \Im[\alpha])^T$. For this reason, coherent states are also referred to as displaced vacuum states. They are generated from the vacuum state by the Weyl operator,

$$|\alpha\rangle = \hat{D}(\boldsymbol{\alpha})|0\rangle \ , \tag{2.6.6}$$

from Equation (2.4.1). We can express a thermal state as a Gaussian distribution of coherent states, since a properly weighted summation over coherent state Wigner functions will produce the Wigner function of a thermal state [11]. In that sense we may consider a thermal state as an alphabet, where every coherent state is a letter. We call this a Gaussian continuous alphabet, and we will see in Section 2.13, that this choice of alphabet maximizes the information content if there is a constraint on how large α is allowed to be, which must be the case physically, since having no limit on α implies infinite energy.

Covariance matrices in symplectic spaces

Covariance matrices are a useful way of describing Gaussian states. Any 2-dimensional Gaussian function can, up to a mean value, be described by a 2×2 matrix containing the variances and the correlations between the variables. More simply, we may uniquely describe any Gaussian state in a phase space of the quadratures by a 2×2 matrix and a 2-component vector of mean values. In the context of quantum mechanics, these covariance matrices live in the symplectic space defined in Section 2.2. We may set up a $2N \times 2N$ covariance matrix which describes N Gaussian modes, and we can use symplectic transformations to represent interactions between these modes, or transformations on the individual modes.

Covariance matrices have two useful forms, which they may always transform into. One is called the Simon normal form [88, 89, 90], and is related to the separability of multi-mode states. For two modes it has the form

$$\mathbf{\Gamma}_{\mathrm{SNF}} = \begin{bmatrix} a & 0 & c_1 & 0 \\ 0 & a & 0 & c_2 \\ c_1 & 0 & b & 0 \\ 0 & c_2 & 0 & b \end{bmatrix} . \tag{2.7.1}$$

In this form, the covariance matrix expresses how two 2D Gaussian distributions, rotationally symmetric in their subspaces, are correlated through the covariance coefficients c_1 and c_2. Another useful form is the Williamson form [91], which is a diagonalization that has a special structure due to the symplectic space. There exists a transformation $\boldsymbol{S}_W$ such that,

$$\boldsymbol{S}_W \mathbf{\Gamma} \boldsymbol{S}_W^T = \bigoplus_{k=1}^{N} \nu_k \mathbb{I}_2 , \tag{2.7.2}$$

where the values ν_k are the moduli of the spectrum of eigenvalues of the matrix $i\mathbf{\Omega}\mathbf{\Gamma}$. The Heisenberg inequality is also easily expressed through the symplectic matrix [92],

$$\mathbf{\Gamma} + i\mathbf{\Omega} \geq 0 . \tag{2.7.3}$$

There are several ways to determine if this inequality holds. The easiest is usually to check that all the eigenvalues of the matrix $\mathbf{\Gamma} + i\mathbf{\Omega}$ are bigger than or equal to zero.

Alternatively, we may check that $\nu_k \geq 1 \; \forall \; k$.

All Gaussian operations that can be performed on a Gaussian state can be represented by symplectic transformations on the corresponding covariance matrix. These transformations all have the property that they preserve the symplectic space, so they fulfil the condition of Equation (2.2.5). For an input with covariance matrix $\boldsymbol{\Gamma}$ and mean value vector $\bar{\boldsymbol{X}}$, the mapping is,

$$\bar{\boldsymbol{X}}' = \boldsymbol{S}\bar{\boldsymbol{X}} + \boldsymbol{d} \qquad , \qquad \boldsymbol{\Gamma}' = \boldsymbol{S}\boldsymbol{\Gamma}\boldsymbol{S}^T \; , \tag{2.7.4}$$

where $\boldsymbol{d}$ and $\boldsymbol{S}$ are a vector and matrix respectively, representing the transformation. The set $(\boldsymbol{d}, \boldsymbol{S})$ is called a symplectic map. The transformations that will be required are displacement, single mode rotation, the beamsplitting operation and the single mode squeezing operation.

Displacements

The displacement operation, through the use of the Weyl operator, is defined by the map,

$$\boldsymbol{d}_{\text{disp}} = \boldsymbol{\alpha} \qquad , \qquad \boldsymbol{S}_{\text{disp}} = \mathbb{I}_2 \; , \tag{2.7.5}$$

This transformation enables the description of a Gaussian state purely through the covariance matrix, since the mean value may always be displaced to zero, without loss of generality.

Rotations

We define local single mode rotations through the map,

$$\boldsymbol{d}_{\text{rot}} = \boldsymbol{0} \qquad , \qquad \boldsymbol{S}_{\text{rot}} = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \; , \tag{2.7.6}$$

where $\theta \in [0, 2\pi]$. This transformation is implemented through single mode phase shifts, and it allows us to always bring a state into the Simon normal form.

Beam splitters

The beam splitter is a transformation on two modes, which are coupled with a transmission $T \in [0, 1]$.

$$\boldsymbol{d}_{\text{BS}} = \boldsymbol{0} \qquad , \qquad \boldsymbol{S}_{\text{BS}} = \begin{bmatrix} \sqrt{T}\mathbb{I}_2 & \sqrt{1-T}\mathbb{I}_2 \\ -\sqrt{1-T}\mathbb{I}_2 & \sqrt{T}\mathbb{I}_2 \end{bmatrix} \; , \tag{2.7.7}$$

It is implemented either through a $T/(1-T)$ beam splitter or a combination of a waveplate and a polarizing beam splitter.

Squeezing

Squeezing of a single mode is defined through the squeezing parameter r, and the transformation,

$$\boldsymbol{d}_{\text{sqz}} = \mathbf{0} \qquad , \qquad \boldsymbol{S}_{\text{sqz}} = \begin{bmatrix} V & 0 \\ 0 & V^{-1} \end{bmatrix} , \tag{2.7.8}$$

where $V = e^{2r}$, with $r \in \mathbb{R}$. This transformation is difficult to implement in general. Generation of vacuum squeezing is well established [93, 94, 95, 96], while the squeezing transformation of an arbitrary input state is significantly harder to achieve.

EPR states

With the operations described above, one can represent any Gaussian state that can be produced in the laboratory. Most importantly, they can be used to construct the famous Einstein-Podolsky-Rosen state [3], which has a special role in proving security in quantum key distribution protocols with continuous variables, due to Ekert showing that testing for a Bell inequality violation is the same as certifying security between two honest parties [18, 71]. We generate the EPR state by interfering two squeezed states on a 50/50 beamsplitter. We use the two mode vacuum state as an input state,

$$\boldsymbol{\Gamma}_{\text{vac}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} . \tag{2.8.1}$$

We squeeze these two vacuum modes, but in conjugate quadratures, with the outcome,

$$\boldsymbol{\Gamma}_{\text{sqz}} = \begin{bmatrix} V & 0 & 0 & 0 \\ 0 & V^{-1} & 0 & 0 \\ 0 & 0 & V^{-1} & 0 \\ 0 & 0 & 0 & V \end{bmatrix} . \tag{2.8.2}$$

These squeezed modes are then interfered on a 50/50 beam splitter, with the symplectic operation $\boldsymbol{S}_{\text{BS}}(T)$, where $T = \frac{1}{2}$,

$$\boldsymbol{\Gamma}_{\text{EPR}} = \begin{bmatrix} \frac{V}{2} + \frac{1}{2V} & 0 & -\frac{V}{2} + \frac{1}{2V} & 0 \\ 0 & \frac{V}{2} + \frac{1}{2V} & 0 & -\frac{V}{2} + \frac{1}{2V} \\ -\frac{V}{2} + \frac{1}{2V} & 0 & \frac{V}{2} + \frac{1}{2V} & 0 \\ 0 & -\frac{V}{2} + \frac{1}{2V} & 0 & \frac{V}{2} + \frac{1}{2V} \end{bmatrix} . \tag{2.8.3}$$

Introducing the parameter $\mu = \frac{V}{2} + \frac{1}{2V}$, this matrix can be rewritten into,

$$\boldsymbol{\Gamma}_{\text{EPR}} = \begin{bmatrix} \mu & 0 & \sqrt{\mu^2 - 1} & 0 \\ 0 & \mu & 0 & -\sqrt{\mu^2 - 1} \\ \sqrt{\mu^2 - 1} & 0 & \mu & 0 \\ 0 & -\sqrt{\mu^2 - 1} & 0 & \mu \end{bmatrix} , \tag{2.8.4}$$

where the variance $\mu \geq 1$ quantifies the size of the state. We will discuss a way to quantify the amount of entanglement in Section 2.9. Consider now the situation where Alice has distributed such an EPR state between herself and Bob. Suppose Alice performs a heterodyne measurement on the mode she kept for herself. Conditioned on her measurement, Bob will then receive a coherent state with a mean value determined by Alice's measurement outcome [97]. From Bob's point of view there is therefore no difference between Alice exchanging the EPR states with him and Alice performing some conditioning, or Alice preparing coherent states by some random process and sending these. This is, roughly speaking, the argument for the equivalence between entanglement based protocols and prepare-and-measure protocols [67, 98, 99].

Separability and logarithmic negativity

A sufficient condition for the separability of a two-mode state is that the partial transpose of the state is positive (PPT) [100, 101],

$$\hat{\rho}^{T_B} \geq 0 \ . \tag{2.9.1}$$

Conversely, having,

$$\hat{\rho}^{T_B} \leq 0 \ , \tag{2.9.2}$$

is a sufficient condition for $\hat{\rho}$ to be entangled. For an $N \times M$ bipartite Gaussian state, where $\mathbf{\Gamma}$ has a block matrix $\boldsymbol{A}$ of N modes and a block $\boldsymbol{B}$ of M modes, the partially transposed state has the covariance matrix,

$$\tilde{\mathbf{\Gamma}} = \mathbf{\Lambda}_{\mathrm{PPT}} \mathbf{\Gamma} \mathbf{\Lambda}_{\mathrm{PPT}} \ , \tag{2.9.3}$$

where $\mathbf{\Lambda}_{\mathrm{PPT}} = \mathbb{I}_A \oplus \mathbf{\Lambda}_B$, $\mathbf{\Lambda}_B = \oplus_{k=1}^{M} \boldsymbol{Z}$ and,

$$\boldsymbol{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \ . \tag{2.9.4}$$

If $\tilde{\mathbf{\Gamma}}$ is not a physical covariance matrix, the positivity of the partial transpose (PPT) does not hold. For the mode partition $1 \times M$, this is a necessary and sufficient requirement for entanglement [102]. The logarithmic negativity,

$$\mathcal{N}(\hat{\rho}) = \log ||\hat{\rho}^{T_B}||_1 \ , \tag{2.9.5}$$

where $||\hat{\rho}^{T_B}||_1$ is the trace norm of the partially transposed state, is an attempt to quantify how much the PPT condition is violated [103]. For Gaussian states it can be calculated in terms of the symplectic eigenvalues of the partially transposed covariance matrix,

$$\mathcal{N}(\hat{\rho}) = \sum_k f(\tilde{\nu}_k) \ , \tag{2.9.6}$$

where,

$$f(x) = \begin{cases} -\log_2(x) & \text{when } x < 1 \\ 0 & \text{when } x \geq 1 \end{cases} \tag{2.9.7}$$

Thus, for every physical eigenvalue, $\nu_k \geq 1$, the logarithmic negativity is unchanged, while for every unphysical eigenvalue, $\nu_k < 1$, the logarithmic negativity becomes further negative.

Homodyne measurements

Homodyne detection is a fundamental tool for quantum optics in continuous variables. The practical description of homodyne detection is done in Section 3.7.1. We will here be especially concerned with conditioning one mode on the outcome of another, in this case where the outcome is measured through homodyne detection. For this purpose, consider a Gaussian state of $N+1$ modes described by the covariance matrix,

$$\mathbf{\Gamma}_{AB} = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{C} \\ \boldsymbol{C}^T & \boldsymbol{B} \end{bmatrix} , \tag{2.10.1}$$

where $\boldsymbol{A}$ is a $2N \times 2N$ block matrix, $\boldsymbol{B}$ is a 2×2 block matrix and $\boldsymbol{C}$ is a rectangular block of the form $2N \times 2$. $\boldsymbol{A}$ and $\boldsymbol{B}$ describe the reduced states in modes A and B respectively, while $\boldsymbol{C}$ describes the correlations between them. Suppose that we project mode B onto the squeezed vacuum state,

$$\mathbf{\Gamma}_d = \begin{bmatrix} d & 0 \\ 0 & \frac{1}{d} \end{bmatrix} , \tag{2.10.2}$$

so we get the projected state

$$\mathbf{\Gamma}_{ABd} = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{C} \\ \boldsymbol{C}^T & \boldsymbol{D} \end{bmatrix} , \tag{2.10.3}$$

with $\boldsymbol{D} = \boldsymbol{B} + \mathbf{\Gamma}_d$. We wish to condition this on the outcome of the measurement of the projected mode D, by considering the zero mean Wigner function corresponding to this covariance matrix and integrating out the quadrature variables in this single mode subspace of the symplectic space [104],

$$W_{A|B}(\boldsymbol{X}_A) = \frac{1}{(2\pi)^N \sqrt{\det \mathbf{\Gamma}_{ABd}}} \int_{\mathbb{R}^2} \exp\left(-\frac{1}{2}\boldsymbol{X}^T \mathbf{\Gamma}_{ABd}^{-1} \boldsymbol{X}\right) \mathrm{d}^2\boldsymbol{X}_D , \tag{2.10.4}$$

where $\boldsymbol{X} = (\boldsymbol{X}_A, \boldsymbol{X}_D)^T$, with $\boldsymbol{X}_A$ having $2N$ quadrature coordinate components and $\boldsymbol{X}_D = (Q_D, P_D)^T$. Partitioned in this way, the inverted covariance matrix is given by,

$$\mathbf{\Gamma}_{ABd}^{-1} = \begin{bmatrix} \boldsymbol{U} & \boldsymbol{V} \\ \boldsymbol{V}^T & \boldsymbol{W} \end{bmatrix}$$

$$\Updownarrow$$

$$\boldsymbol{\Gamma}_{ABd}^{-1} = \begin{bmatrix} (\boldsymbol{A} - \boldsymbol{C}\boldsymbol{D}^{-1}\boldsymbol{C}^T)^{-1} & -\boldsymbol{A}^{-1}\boldsymbol{C}(\boldsymbol{D} - \boldsymbol{C}^T\boldsymbol{A}^{-1}\boldsymbol{C})^{-1} \\ -\boldsymbol{D}^{-1}\boldsymbol{C}^T(\boldsymbol{A} - \boldsymbol{C}\boldsymbol{D}^{-1}\boldsymbol{C}^T)^{-1} & (\boldsymbol{D} - \boldsymbol{C}^T\boldsymbol{A}^{-1}\boldsymbol{C})^{-1} \end{bmatrix} . \tag{2.10.5}$$

We rewrite the integrand product in terms of the renamed sub-matrices,

$$\boldsymbol{X}^T\boldsymbol{\Gamma}_{ABd}^{-1}\boldsymbol{X} = \boldsymbol{X}_A^T\boldsymbol{U}\boldsymbol{X}_A + \boldsymbol{X}_A^T\boldsymbol{V}\boldsymbol{X}_D + \boldsymbol{X}_D^T\boldsymbol{V}^T\boldsymbol{X}_A + \boldsymbol{X}_D^T\boldsymbol{W}\boldsymbol{X}_D . \tag{2.10.6}$$

The first term is independent of the integration variables, so

$$\begin{aligned} W_{A|B}(\boldsymbol{X}_A) = {} & \frac{1}{(2\pi)^N\sqrt{\det\boldsymbol{\Gamma}_{ABd}}}\exp\left(-\frac{1}{2}\boldsymbol{X}_A^T\boldsymbol{U}\boldsymbol{X}_A\right) \\ & \times \int_{\mathbb{R}^2}\exp\left(-\frac{1}{2}(\boldsymbol{X}_A^T\boldsymbol{V}\boldsymbol{X}_D + \boldsymbol{X}_D^T\boldsymbol{V}^T\boldsymbol{X}_A + \boldsymbol{X}_D^T\boldsymbol{W}\boldsymbol{X}_D)\right) \mathrm{d}^2\boldsymbol{X}_D , \end{aligned} \tag{2.10.7}$$

The exponent inside the integration can be further rewritten,

$$\begin{aligned} & \boldsymbol{X}_A^T\boldsymbol{V}\boldsymbol{X}_D + \boldsymbol{X}_D^T\boldsymbol{V}^T\boldsymbol{X}_A + \boldsymbol{X}_D^T\boldsymbol{W}\boldsymbol{X}_D = \\ & (\boldsymbol{X}_D + \boldsymbol{W}^{-1}\boldsymbol{V}^T\boldsymbol{X}_A)^T\boldsymbol{W}(\boldsymbol{X}_D + \boldsymbol{W}^{-1}\boldsymbol{V}^T\boldsymbol{X}_A) + \boldsymbol{X}_A^T\boldsymbol{V}\boldsymbol{W}^{-1}\boldsymbol{V}^T\boldsymbol{X}_A . \end{aligned} \tag{2.10.8}$$

With this rewriting, the integral becomes,

$$\begin{aligned} W_{A|B}(\boldsymbol{X}_A) = {} & \frac{1}{(2\pi)^N\sqrt{\det\boldsymbol{\Gamma}_{ABd}}}\exp\left(-\frac{1}{2}\boldsymbol{X}_A^T(\boldsymbol{U} + \boldsymbol{V}\boldsymbol{W}^{-1}\boldsymbol{V}^T)\boldsymbol{X}_A\right) \\ & \times \int_{\mathbb{R}^2}\exp\left(-\frac{1}{2}(\boldsymbol{X}_A^T\boldsymbol{V}\boldsymbol{X}_D + \boldsymbol{X}_D^T\boldsymbol{V}^T\boldsymbol{X}_A + \boldsymbol{X}_D^T\boldsymbol{W}\boldsymbol{X}_D)\right) \mathrm{d}^2\boldsymbol{X}_D , \end{aligned} \tag{2.10.9}$$

which evaluates to,

$$\begin{aligned} W_{A|B}(\boldsymbol{X}_A) = {} & \frac{1}{(2\pi)^{N-1}\sqrt{\det\boldsymbol{\Gamma}_{ABd}\det\boldsymbol{W}}} \\ & \times \exp\left(-\frac{1}{2}\boldsymbol{X}_A^T(\boldsymbol{U} + \boldsymbol{V}\boldsymbol{W}^{-1}\boldsymbol{V}^T)\boldsymbol{X}_A\right) , \end{aligned} \tag{2.10.10}$$

so we recover a Wigner function of the remaining N modes of the projected state with the covariance matrix,

$$\boldsymbol{\Gamma}_{A|B} = (\boldsymbol{U} + \boldsymbol{V}\boldsymbol{W}^{-1}\boldsymbol{V}^T)^{-1} = \boldsymbol{A} + \boldsymbol{C}\boldsymbol{D}^{-1}\boldsymbol{C}^T . \tag{2.10.11}$$

We now wish to let d go to zero, as this corresponds to projecting mode B onto an infinitely squeezed state, which is equivalent to a homodyne detection [78, 79]. Expressing D in terms of the elements of B,

$$\boldsymbol{D} = \begin{bmatrix} \boldsymbol{B}_{11} + d & \boldsymbol{B}_{21} \\ \boldsymbol{B}_{21} & \boldsymbol{B}_{22} + \frac{1}{d} \end{bmatrix} . \tag{2.10.12}$$

We see from Equation (2.10.11) that $\boldsymbol{D}^{-1}$ is the relevant quantity. We find that

$$\lim_{d\to 0} \boldsymbol{D}^{-1} = (\boldsymbol{\Pi B \Pi})^{MP} = \boldsymbol{B}_{11}^{-1}\boldsymbol{\Pi} \ , \tag{2.10.13}$$

where

$$\boldsymbol{\Pi} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \ , \tag{2.10.14}$$

and the superscript MP denotes the Moore-Penrose pseudoinverse of a singular matrix [105]. We therefore arrive at the following formula for conditioning homodyne detection in the Q quadrature,

$$\boldsymbol{\Gamma}_{A|B} = \boldsymbol{A} + \boldsymbol{B}_{11}^{-1}\boldsymbol{C\Pi C}^T \ . \tag{2.10.15}$$

For homodyne detection in the phase quadrature, we choose instead,

$$\boldsymbol{\Pi} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \ , \tag{2.10.16}$$

and Equation (2.10.15) becomes,

$$\boldsymbol{\Gamma}_{A|B} = \boldsymbol{A} + \boldsymbol{B}_{22}^{-1}\boldsymbol{C\Pi C}^T \ . \tag{2.10.17}$$

Heterodyne measurements

In a manner similar to Section 2.10, we wish to investigate how the outcome of a heterodyne detection transforms the remaining modes. The practical description of heterodyne detection is done in Section 3.7.2. We consider a Gaussian state of $N+1$ modes with the covariance matrix,

$$\Gamma = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{C} \\ \boldsymbol{C}^T & \boldsymbol{B}^{(2)} \end{bmatrix} \ . \tag{2.11.1}$$

$\boldsymbol{A}$ is a matrix of N modes, the 4×4 block $\boldsymbol{B}^{(2)}$ is,

$$\boldsymbol{B}^{(2)} = \begin{bmatrix} \boldsymbol{B} & \boldsymbol{0} \\ \boldsymbol{0} & \mathbb{I}_2 \end{bmatrix} \ , \tag{2.11.2}$$

where $\boldsymbol{B}$ is the covariance matrix of the mode to be measured by heterodyne detection, and $\mathbb{I}_2$ is in the other block as the vacuum that enters through the balanced beam splitter. $\boldsymbol{C}$ is a $2N \times 4$ matrix that contains the correlations between $\boldsymbol{A}$ and $\boldsymbol{B}^{(2)}$. It may be decomposed into

$$\boldsymbol{C} = \begin{bmatrix} \boldsymbol{C}_1 & \boldsymbol{0} \end{bmatrix} \ , \tag{2.11.3}$$

since $\boldsymbol{A}$ is not correlated with the vacuum mode, and $\boldsymbol{C}_1$ contains the correlations between $\boldsymbol{A}$ and $\boldsymbol{B}$. Applying the balanced beamsplitter operation between mode B and the vacuum, we get the global state

$$\mathbf{\Gamma}' = \begin{bmatrix} \boldsymbol{A} & \frac{1}{\sqrt{2}}\boldsymbol{C}_1 & -\frac{1}{\sqrt{2}}\boldsymbol{C}_1 \\ \frac{1}{\sqrt{2}}\boldsymbol{C}_1^T & \frac{1}{2}(\boldsymbol{B}+\mathbb{I}_2) & \frac{1}{2}(\mathbb{I}_2-\boldsymbol{B}) \\ -\frac{1}{\sqrt{2}}\boldsymbol{C}_1^T & \frac{1}{2}(\mathbb{I}_2-\boldsymbol{B})^T & \frac{1}{2}(\boldsymbol{B}+\mathbb{I}_2) \end{bmatrix} . \tag{2.11.4}$$

Now, performing homodyne conditioning in opposite quadratures in each of the mixed modes that do not belong to $\boldsymbol{A}$, after some algebra we get [71, 105],

$$\mathbf{\Gamma}_{A|B} = \boldsymbol{A} - \frac{1}{\theta_1}\boldsymbol{C}_1(\mathbf{\Omega}\boldsymbol{B}\mathbf{\Omega}^T + \mathbb{I}_2)\boldsymbol{C}_1^T , \tag{2.11.5}$$

where $\theta_1 = \det \boldsymbol{B} + \mathrm{Tr}\boldsymbol{B} + 1$. This expression may be rewritten into the simpler form,

$$\mathbf{\Gamma}_{A|B} = \boldsymbol{A} - \boldsymbol{C}_1(\boldsymbol{B}+\mathbb{I}_2)^{-1}\boldsymbol{C}_1^T , \tag{2.11.6}$$

which is essentially a quadrature symmetric version of Equation (2.10.15), with the addition of the vacuum variance.

Bell measurements

Bell detection may be regarded as a generalization of heterodyne detection, in the sense that the vacuum mode introduced for heterodyne detection may also contain a signal, such that the two signal modes are interfered before being measured in orthogonal quadratures with homodyne detection. We here investigate the transformation realized by such a conditional measurement. Consider a Gaussian state of $N+2$ modes with the covariance matrix,

$$\mathbf{\Gamma} = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{C} \\ \boldsymbol{C}^T & \boldsymbol{B}^{(2)} \end{bmatrix} , \tag{2.12.1}$$

where A is a matrix of n modes and the 4×4 block $B^{(2)}$ is,

$$\boldsymbol{B}^{(2)} = \begin{bmatrix} \boldsymbol{B}_1 & \boldsymbol{D} \\ \boldsymbol{D}^T & \boldsymbol{B}_2 \end{bmatrix} , \tag{2.12.2}$$

which is to be measured by the Bell detection and $\boldsymbol{D}$ contains the correlations between the measured modes. $\boldsymbol{C}$ is a $2N \times 4$ matrix that contains the correlations between $\boldsymbol{A}$ and $\boldsymbol{B}^{(2)}$. It may be decomposed into

$$\boldsymbol{C} = \begin{bmatrix} \boldsymbol{C}_1 & \boldsymbol{C}_2 \end{bmatrix} , \tag{2.12.3}$$

where $\boldsymbol{C}_1$ contains the correlations between $\boldsymbol{A}$ and $\boldsymbol{B}_1$, and $\boldsymbol{C}_2$ between $\boldsymbol{A}$ and $\boldsymbol{B}_2$. Then, the N mode conditional state is found to be [105],

$$\mathbf{\Gamma}_{A|B} = \mathbf{\Gamma}_A - \frac{1}{2\det\mathbf{\Theta}} \sum_{i,j=1}^{2} \boldsymbol{C}_i(\boldsymbol{X}_i^T \mathbf{\Theta} \boldsymbol{X}_j)\boldsymbol{C}_j^T , \tag{2.12.4}$$

where $\mathbf{\Theta} = \frac{1}{2}(\boldsymbol{Z}\boldsymbol{B}_1\boldsymbol{Z} + \boldsymbol{B}_2 - \boldsymbol{Z}\boldsymbol{D} - \boldsymbol{D}^T\boldsymbol{Z})$ and,

$$\boldsymbol{X}_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad , \quad \boldsymbol{X}_2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \tag{2.12.5}$$

A compact way to implement this detection method is described in Section 3.7.2.

Classical information theory

This section deals with the mathematical concepts of information theory without reference to any quantum mechanical phenomena. An excellent reference on this topic is the book by Cover and Thomas [5].

We begin by introducing the concept of Shannon entropy $H(A)$ of some random variable A, the outcomes of which are distributed according to the probability distribution $P(a)$. Inspired by statistical mechanics,

$$H(A) = -\sum_{a \in \mathcal{A}} P(a) \log_2 P(a) \ , \tag{2.13.1}$$

where a are then the outcomes of the random variable A that belong to the alphabet $\mathcal{A}$. For continuous probability distributions we have the analogous definition,

$$H(A) = -\int_{\mathbb{S}} P(a) \log_2 P(a) \, \mathrm{d}a \ . \tag{2.13.2}$$

Here $P(a)$ is a continuous probability distribution, and $\mathbb{S}$ is the support of the random variable A. The support is the set for which $P(a) > 0$. We limit the integral to this set, since $\log_2(x)$ is ill defined when $x = 0$. For a Gaussian distribution of $2N$ modes with zero mean and covariance matrix $\boldsymbol{\Gamma}$,

$$H(\boldsymbol{\Gamma}) = \frac{1}{2} \log_2((2\pi e)^{2N} \det \boldsymbol{\Gamma}) \ . \tag{2.13.3}$$

We will typically be interested in the entropy of the encoded signal rather than the quantum state itself. For a collection of coherent states that form a single mode thermal state with the variance $V_S + 1$, we shall call V_S the signal variance. The entropy of the encoding is therefore the entropy of the thermal state generated by the encoding minus the entropy of the vacuum,

$$H(S) = H(\boldsymbol{\Gamma}) - H(\boldsymbol{\Gamma}_{\text{vac}}) = \frac{1}{2} \log_2 V_S \ . \tag{2.13.4}$$

In fact a Gaussian probability distribution is guaranteed to maximize this entropy out of all probability distributions with the same variance.

To see this, let $P(\boldsymbol{X})$ be a classical probability distribution of N modes, where it has a covariance matrix with its components defined through the integral,

$$\mathbf{\Gamma}_{ij} = \int_{\mathbb{S}} P(\boldsymbol{X})\boldsymbol{X}_i\boldsymbol{X}_j \,\mathrm{d}^N\boldsymbol{X} \ . \tag{2.13.5}$$

Since this is an arbitrary distribution it may have arbitrary values for its k'th moment. We then define a unique Gaussian probability distribution, $G(\boldsymbol{X})$, with the covariance matrix $\mathbf{\Gamma}$ and zero mean. The difference between these two distributions may be quantified through the Kullback-Leibler distance [5],

$$D(P||G) = \int_{\mathbb{S}} P(\boldsymbol{X}) \log_2 \left(\frac{P(\boldsymbol{X})}{G(\boldsymbol{X})} \right) \mathrm{d}^N\boldsymbol{X} \geq 0 \ , \tag{2.13.6}$$

which is zero if and only if the distributions are identical. Using the definition of the entropy on this expression, we obtain the inequality,

$$H(P) \leq H(G) \ . \tag{2.13.7}$$

A similar result exists in quantum information theory, where a Gaussian Wigner function will maximize the von Neumann entropy described in Section 2.14 [71, 81].

We may also consider the probability distribution of two variables, which gives us the joint entropy,

$$H(AB) = -\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}} P(a,b)\log_2 P(a,b) \ , \tag{2.13.8}$$

Conditioning distribution A on the outcomes of distribution B, we get the conditional entropy,

$$H(A|B) = H(AB) - H(B) = -\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}} P(a|b)\log_2 P(a|b) \ , \tag{2.13.9}$$

which for Gaussian states is,

$$H(A|B) = \frac{1}{2}\log_2\left(V_A - \frac{C^2}{V_B} \right) \ , \tag{2.13.10}$$

where C is the covariance between the distributions, and V_A and V_B are the variances of Alice's Gaussian input alphabet and Bob's measurements respectively. With these quantities defined, we may also define the mutual information,

$$I(A:B) = H(A) - H(A|B) \ , \tag{2.13.11}$$

which quantifies the entropy reduction on distribution A by the measurement of distribution B. The quantity is symmetric such that,

$$H(A) - H(A|B) = H(B) - H(B|A) \ . \tag{2.13.12}$$

For a two-mode Gaussian distribution, the mutual information is,

$$I(A:B) = \frac{1}{2}\log_2\left(\frac{V_A}{V_A - \frac{C^2}{V_B}} \right) \ . \tag{2.13.13}$$

Quantum information theory

This section considers what consequences the existence of quantum mechanics has upon information theory and extends these principles accordingly. Useful introductions to this topic are the book by Wilde [11] and the book by Nielsen and Chuang [12]. We first define the notion of von Neumann entropy of a quantum state $\hat{\rho}$, in analogy with Equation (2.13.1),

$$S(\hat{\rho}) = -\mathrm{Tr}\hat{\rho}\log_2\hat{\rho} \ . \tag{2.14.1}$$

This entropy is a measure of the amount of uncertainty that remains after a measurement of the state $\hat{\rho}$. For a pure state, where $\mathrm{Tr}\hat{\rho}^2 = 1$, we have that

$$S(\hat{\rho}) = 0 \ , \tag{2.14.2}$$

so if one picks a proper basis to measure $\hat{\rho}$, no uncertainty remains. Von Neumann entropy is invariant under unitary operations, such that,

$$S(\hat{\rho}) = S(\hat{U}\hat{\rho}\hat{U}^{\dagger}) \ . \tag{2.14.3}$$

This also implies that von Neumann entropy does not change under symplectic transformations, since these transformations have a corresponding unitary operator that transforms the associated density matrix. For separable states von Neumann entropy is additive such that

$$S(\hat{\rho}_A \otimes \hat{\rho}_B) = S(\hat{\rho}_A) + S(\hat{\rho}_B) \ . \tag{2.14.4}$$

For a general two-mode state $\hat{\rho}_{AB}$ we define the joint entropy as,

$$S(\hat{\rho}_{AB}) = -\mathrm{Tr}(\hat{\rho}_{AB}\log_2\hat{\rho}_{AB}) \ , \tag{2.14.5}$$

and the marginal entropies,

$$S(\hat{\rho}_A) = -\mathrm{Tr}(\hat{\rho}_A\log_2\hat{\rho}_A) \qquad , \qquad S(\hat{\rho}_B) = -\mathrm{Tr}(\hat{\rho}_B\log_2\hat{\rho}_B) \ , \tag{2.14.6}$$

where $\hat{\rho}_A = \mathrm{Tr}_B\hat{\rho}_{AB}$ is the density matrix after a partial trace over mode B, and similarly for $\hat{\rho}_B$. Consider a general two-mode pure state written in its Schmidt decomposition [10, 29],

$$|\psi\rangle_{AB} = \sum_n a_n|\lambda_n\rangle_A|\phi_n\rangle_B \ . \tag{2.14.7}$$

Expressed as a density matrix,

$$\hat{\rho}_{AB} = |\psi\rangle_{AB}\langle\psi| = \sum_{nm} a_n a_m^* |\lambda_n\rangle_A|\phi_n\rangle_B\langle\lambda_m|_A\langle\phi_m|_B \ . \tag{2.14.8}$$

Taking the partial trace over mode A and B, respectively,

$$\hat{\rho}_A = \mathrm{Tr}_B \hat{\rho}_{AB} = \sum_i \langle \phi_i |_B \sum_{nm} a_n a_m^* |\lambda_n\rangle_A |\phi_n\rangle_B \langle \lambda_m|_A \langle \phi_m |_B \phi_i\rangle_B \tag{2.14.9}$$

$$\Updownarrow$$

$$\hat{\rho}_A = \sum_n |a_n|^2 |\lambda_n\rangle\langle\lambda_n| \ , \tag{2.14.10}$$

since we may take the trace in any basis. Similarly, we have,

$$\hat{\rho}_B = \sum_n |a_n|^2 |\phi_n\rangle\langle\phi_n| \ . \tag{2.14.11}$$

Using the definition from Equation (2.14.1), we see that

$$S(\hat{\rho}_A) = S(\hat{\rho}_B) = -\sum_n |a_n|^2 \log_2 |a_n|^2 \ , \tag{2.14.12}$$

such that the reduced states of a two-mode pure state have the same von Neumann entropy, while the global state has $S(\hat{\rho}_{AB}) = 0$. This property generalizes to any number of modes, such that, for example, for a pure three-mode state $\hat{\rho}_{ABE}$, we have $S(AB) = S(E)$, $S(A) = S(EB)$ and $S(B) = S(AE)$. This property is sometimes referred to as self-duality [11, 85].

For Gaussian states there is a straightforward way of calculating von Neumann entropy. Consider the Gaussian N-mode state described by the covariance matrix $\mathbf{\Gamma}$ of size $2N \times 2N$. We know that there exists a transformation $\boldsymbol{S}_W$ that transforms this matrix into the Williamson form,

$$\boldsymbol{S}_W \mathbf{\Gamma} \boldsymbol{S}_W^T = \bigoplus_{k=1}^{N} \nu_k \mathbb{I}_2 \ . \tag{2.14.13}$$

In this form, the state is equivalent to N uncoupled thermal states with mean photon numbers $\bar{n}_k = \frac{1}{2}(\nu_k - 1)$. Using the additive property of von Neumann entropy, defined in Equation (2.14.4),

$$S(\boldsymbol{S}_W \mathbf{\Gamma} \boldsymbol{S}_W^T) = \sum_{k=1}^{N} S(\nu_k \mathbb{I}_2) \ . \tag{2.14.14}$$

Recalling also that von Neumann entropy is invariant under unitary transformations,

$$S(\mathbf{\Gamma}) = \sum_{k=1}^{N} S(\nu_k \mathbb{I}_2) \ , \tag{2.14.15}$$

since $S(\boldsymbol{S}_W \mathbf{\Gamma} \boldsymbol{S}_W^T) = S(\mathbf{\Gamma})$. From Equation (2.5.6),

$$\hat{\rho}_{\mathrm{th}} = \sum_{m=0}^{\infty} \frac{\bar{n}^m}{(1+\bar{n})^{m+1}} |m\rangle\langle m| \ , \tag{2.14.16}$$

the von Neumann entropy of a single thermal state of mean photon number $\bar{n}$ can be calculated through the definition in Equation (2.14.1). Since $\hat{\rho}_{\text{th}}$ is already diagonal this yields,

$$S(\hat{\rho}_{\text{th}}) = -\frac{1}{1+\bar{n}} \sum_{m=0}^{\infty} \left(\frac{\bar{n}}{1+\bar{n}}\right)^m \log_2 \frac{\bar{n}^m}{(1+\bar{n})^{m+1}} \tag{2.14.17}$$

$$\Updownarrow$$

$$\begin{aligned} S(\hat{\rho}_{\text{th}}) = \frac{1}{1+\bar{n}} \Bigg(&- \sum_{m=0}^{\infty} \left(\frac{\bar{n}}{1+\bar{n}}\right)^m m \log_2 \bar{n} \\ &+ \sum_{m=0}^{\infty} \left(\frac{\bar{n}}{1+\bar{n}}\right)^m (m+1) \log_2 (1+\bar{n}) \Bigg) \ . \end{aligned} \tag{2.14.18}$$

The identities,

$$\sum_{m=0}^{\infty} \left(\frac{\bar{n}}{1+\bar{n}}\right)^m = 1+\bar{n} \quad , \quad \sum_{m=0}^{\infty} \left(\frac{\bar{n}}{1+\bar{n}}\right)^m m = \bar{n}(1+\bar{n}) \ , \tag{2.14.19}$$

permit a rewriting into the expression,

$$S(\hat{\rho}_{\text{th}}) = \bar{n} \log_2 \frac{1+\bar{n}}{\bar{n}} + \log_2(1+\bar{n}) \ . \tag{2.14.20}$$

To express this in terms of the symplectic eigenvalues ν_k, we introduce the bosonic information function,

$$g(x) = \frac{x+1}{2} \log_2 \left(\frac{x+1}{2}\right) - \frac{x-1}{2} \log_2 \left(\frac{x-1}{2}\right) \ , \tag{2.14.21}$$

such that for a single mode thermal state, and by extension an arbitrary Gaussian state, we have,

$$S(\hat{\rho}_{th}) = g(\nu) \ , \tag{2.14.22}$$

with $\nu = 2\bar{n} + 1$. In general we therefore have,

$$S(\mathbf{\Gamma}) = \sum_{k=1}^{N} g(\nu_k) \ . \tag{2.14.23}$$

In this way we have conveniently expressed the von Neumann entropy of an arbitrary Gaussian state through the symplectic spectrum of its covariance matrix. The conditional von Neumann entropy is defined in analogy to the conditional Shannon entropy in Equation (2.13.9),

$$S(A|B) = S(AB) - S(B) \ . \tag{2.14.24}$$

Unlike classical conditional entropy, conditional von Neumann entropy can be negative. The EPR state from Equation (2.8.4) is pure when considered as two modes but any single mode by itself, not conditioned on the outcome of the other, is a thermal state. Therefore, the conditional entropy for an EPR state of size μ is,

$$S(A|B) = -g(\mu) \ , \tag{2.14.25}$$

which is negative. This is a significant departure from classical information theory.

The property of self-duality also applies to conditional entropies. Consider the pure tripartite state $\hat{\rho}_{ABE}$ and suppose that a conditional measurement is performed on mode B that leaves the state $\hat{\rho}_{AE|B}$ pure. The entropy of the conditional state is then,

$$S(AE|B) = 0 \ , \tag{2.14.26}$$

but the entropies of the conditioned reduced states maintain self-duality such that,

$$S(A|B) = S(E|B) \ . \tag{2.14.27}$$

With the conditional entropy defined, we may also define the quantum mutual information,

$$S(A:B) = S(A) - S(A|B) = S(B) - S(B|A) \ , \tag{2.14.28}$$

which has the same symmetry properties as the classical quantity, and where we have the bound,

$$I(A:B) \leq S(A:B) \ . \tag{2.14.29}$$

Related to the mutual information, we introduce the Holevo quantity [11, 12, 71],

$$\chi(A:B) = S(\hat{\rho}_B) - \sum_x P_A(x) S(\hat{\rho}_B^x) \ , \tag{2.14.30}$$

where Alice prepares the quantum state $\hat{\rho}_B^x$ with probability $p_A(x)$, such that Bob receives the state,

$$\hat{\rho}_B = \sum_x P_A(x) \hat{\rho}_B^x \ . \tag{2.14.31}$$

The purpose of the Holevo quantity is to bound the amount of information extractable by an optimal measurement of the state $\hat{\rho}_B$. This quantity is particularly relevant for quantum key distribution, where we wish to bound the amount of information available to the eavesdropper without knowing what strategy she is going to employ. For a typical Gaussian QKD configuration with the two honest parties Alice and Bob exchanging states and Eve implementing some Gaussian unitary through the quantum channel, the Holevo bound on Eve's information gain is [97, 106],

$$\chi(E:X) = S(E) - S(E|X) \ , \tag{2.14.32}$$

where X is either A or B, depending on the reconciliation [71, 107]. For reverse reconciliation [48] $X = B$. Here the outcomes of Bob's measurements are estimated by Alice. Conversely, for direct reconciliation [47, 108] $X = A$ and it is up to Bob to estimate the initial states prepared by Alice. We then have, for a generic quantum key distribution protocol, the secret key rate bound in the limit of infinite state exchanges,

$$R = I(A : B) - \chi(E : X) \ . \tag{2.14.33}$$

This bound is sometimes referred to as the Devetak-Winter bound [109]. Since Eve's modes are not known to the honest parties, this quantity is hard to estimate in practice. However, assuming that Eve is able to purify the global state $\hat{\rho}_{ABE}$ we arrive at the bound,

$$\chi(E : X) = S(AB) - S(\tilde{X}|X), \tag{2.14.34}$$

where $\tilde{X}$ is the opposite of X, so if $X = A$, then $\tilde{X} = B$. This assumption sets a further upper bound on Eve's information gain as it is the most pessimistic choice possible. When an infinite identically and independently distributed (iid) number of state exchanges are assumed, the law of large numbers ensures that all the entropy quantities defined here are valid [5, 12]. Additionally, symmetry considerations and the use of the so called de Finetti theorem [110] lead to the conclusion that coherent attacks reduce to collective attacks [73, 107] when there are infinite iid state exchanges.

Collective attacks allow for the eavesdropper to apply any quantum unitary to the individual exchanged states, but this selected unitary must be applied to all the states. Eve is then allowed to save her output states in a quantum memory and measure them collectively once the state transfer is complete. Coherent attacks are a step up from this in that for each exchanged state, Eve may select a new optimal unitary operator and still perform a collective measurement at the end. In addition to the equivalence of coherent and collective attacks, we may also use the fact that Gaussian distributions maximize entropy to show that Gaussian attacks are optimal in this limit [81], which limits Eve to attacks that use Gaussian states. This will be exploited extensively in the chapters on QKD protocols that follow.

It is unknown if similar symmetry considerations imply the equivalence of collective and coherent attacks if infinite state exchanges are not assumed. In fact, one important caveat of the Devetak-Winter bound is that it does not guarantee composability of the generated secret key in the finite state exchange limit [76, 77, 111], though this complication is outside the scope of this thesis. In spite of these difficulties, finite size security proofs for continuous variable quantum key distribution have made a number of recent advances [60, 61, 74, 75, 112].

Experimental techniques

Laser light generation

The experiments described in this thesis all made use of a 1064 nm Nd:YAG laser from Coherent, with a 400 mW output beam. The laser had a built in cavity with a lithium niobate ($\mathrm{LiNbO_3}$) crystal to generate 532 nm light. This was used to pump the optical parametric oscillator (OPO) described in Section 3.5. The cavity for second harmonic generation was locked with a Pound-Drever-Hall (PDH) lock [113], and the modulation at 12 MHz and servo controller was integrated into the laser control unit. The PDH locking technique is described in detail in Section 3.6.1. Figure 3.1 shows the arrangement of optical elements inside the laser.

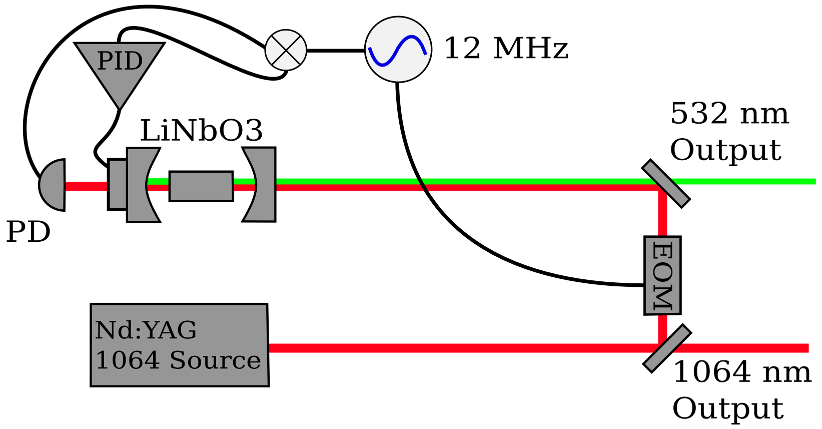


Figure 3.1: An Nd:YAG crystal in a non-planar ring cavity functions as a 1064 nm laser source. The output was split with one part going to the experiment, and the other part being phase modulated at 12 MHz to generate a sideband for locking a linear cavity with a lithium niobate crystal. The crystal is pumped by the 1064 nm source beam to power the second harmonic generation, producing photons at 532 nm, which are a secondary output from the laser housing. PD: Photo detector, EOM: Electro-optical modulator, PID: Servo controller, LiNbO3: Lithium Niobate crystal.

Sidebands

The carrier beam generated by the laser source is quite noisy because of amplitude and phase noise, which comes about from a number of sources, one of which is the so-called relaxation noise [114]. Typically, the quantum states under investigation are produced at a frequency shifted away from the frequency of the carrier to avoid this noise, as it generally decays with increased frequency. By selecting a sufficiently high frequency, one can ensure that the only remaining noise at that frequency is the quantum shot noise that originates from the quantization of the harmonic oscillator. We call states generated at these frequencies away from the carrier frequency sideband states.

The frequency of a sideband state is always described relative to the carrier, and mathematically all calculations take place in a frame rotating with the laser carrier frequency. For this particular laser source 10.5 MHz is a convenient choice for a sideband frequency as the laser noise decays sufficiently fast for 10.5 MHz to be prepared in a vacuum state. We then say that the laser is shot noise limited at this frequency, since the shot noise can be resolved. This might be confirmed experimentally by checking that the noise power doubles with a doubling in the carrier power.

We denote the sideband operators, $\hat{a}_\Omega$ and $\hat{a}_{-\Omega}$, where we have suppressed the other mode indices, and Ω is the sideband frequency. Because every mode has separate operators we may also define separate phase spaces for them, and so the theory developed in Chapter 2 applies directly to phase spaces on these sidebands. Shot noise limited sidebands are convenient because they are automatically prepared in the vacuum state $|0\rangle$. We may then use the experimental techniques described in this chapter to transform this vacuum state into some other Gaussian state.

Modulation of light

To encode information onto the carrier beam we use electro-optical modulators (EOMs) that change the phase and amplitude quadratures. In this sense they function as the displacement operator $\hat{D}(\boldsymbol{\xi})$, defined in Equation (2.4.1). Electro-optical modulators utilize a birefringent crystal with a significant electro-optical effect to change the refractive index as a function of applied voltage. This is also sometimes called the Pockels effect and it is potentially very fast. The modulators used in the laboratory can generate displacements on sidebands anywhere between direct current (DC) and 200 MHz with respect to the carrier frequency.

A change in the refractive index directly translates into a phase shift of the signal beam relative to the local oscillator corresponding to a displacement in the P quadrature. For a classical plane wave the electromagnetic field changes from,

$$E(t) = E_0 e^{i\omega t} \ , \tag{3.3.1}$$

into,

$$E(t) = E_0 e^{i(\omega t + \eta \sin(\Omega t))} \ , \tag{3.3.2}$$

which, expanded in Bessel functions [113, 114], becomes,

$$E(t) \approx E_0 \left(J_0(\eta) e^{i\omega t} + J_1(\eta) e^{i(\omega+\Omega)t} - J_1(\eta) e^{i(\omega-\Omega)t} \right) \ , \tag{3.3.3}$$

where ω is the angular carrier frequency, Ω is the sideband frequency, η is modulation depth, and J_k is the k'th Bessel function [115]. This expression implies that there are sidebands oscillating at $\pm\Omega$ with respect to the carrier frequency. Homodyne and heterodyne detection methods are not able to distinguish these sidebands. In fact, entanglement between sidebands is what generates quadrature squeezing when detected with homodyne detection [114].

It is less obvious why a phase modulation can be used to modulate the amplitude or Q quadrature. Here it is useful to remember that the crystal is birefringent. If the input beam is split between horizontal and vertical polarization modes, these will experience different phase shifts. A polarizing beam splitter after the modulator will then perform a projective measurement on the output, and the modes will interfere destructively or constructively depending on the relative phase shift induced by the modulator, the net effect being that the amplitude is modulated [114]. The crystal, together with the polarizing beam splitter, essentially realizes a Mach-Zender interferometer [83]. The birefringence is highly temperature dependent, but rather than control the temperature of the crystal, manufacturers usually use two crystals, with their optical axes perpendicular to each other, which causes this drift to average out.

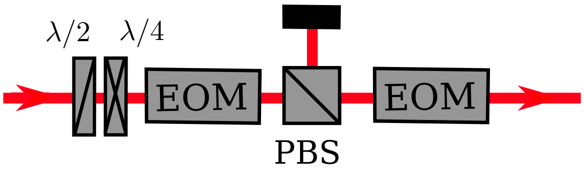


Figure 3.2: Modulator configuration where the first EOM functions as an amplitude modulator, and the last EOM functions as the phase modulator. The polarizing beam splitter (PBS) after the first EOM interferes the polarization components exiting the EOM and dumps half the power. The incoming polarization is adjusted through a combination of a half-wave and a quarter-wave plate.

To make sure that such a modulator only shifts the sideband along Q, it is quite important that the input polarization is clean. The reason for this is that a slight misadjustment leads to the amplitude modulator also modulating the conjugate quadrature. Typically, one wants there to be no correlations between the quadratures, since this complicates the analysis. Therefore, it is important to secure the orthogonality of the two modulations. This orthogonality also depends on the modulation depth, such that it becomes hard to obtain it above 15 to 18 dB of modulation relative to the shot noise.

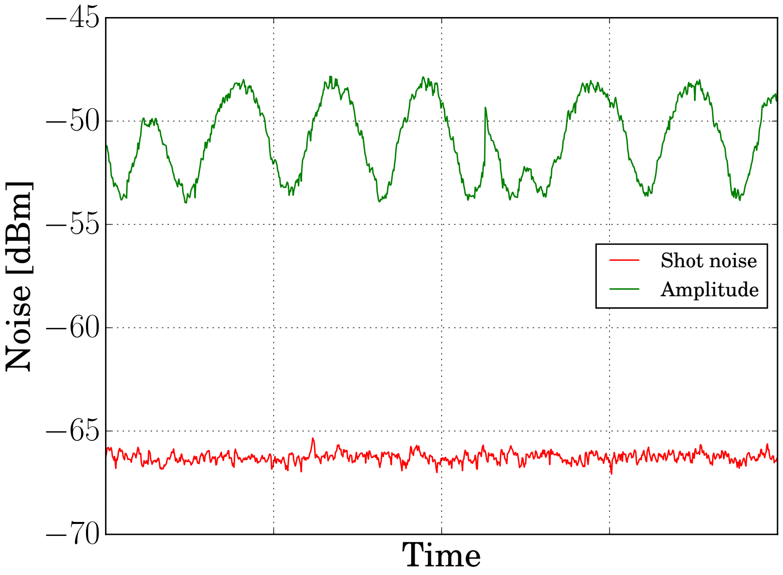


Figure 3.3: A zero span spectrum analyzer measurement of an asymmetric thermal state, caused by unbalanced input polarization into the amplitude modulator. The measurement is performed with a homodyne detector, where the relative phase between the signal and local oscillator is continuously scanned, which gives a time dependence on the measured quadrature. The sinusoidal pattern appears because once quadrature is significantly more noisy than the other.

We consider a configuration of an amplitude and a phase modulator as shown in Figure 3.2. Detecting a modulation along one axis in phase space with a quadrature scanned homodyne detector, both modulators will be able to produce such a quadrature asymmetric signal, but the recorded signal does not show what the alignment relative to our preferred coordinate system is, or even how the two modulations are orientated relative to each other if both modulators are enabled at the same time. We can however make use of a geometrical argument to show orthogonality. Suppose both modulations are of the same absolute magnitude. If we enable them simultaneously and they are orthogonal we would expect to produce a symmetric thermal state. If they are not, we create an elliptical noise shape in phase space. On the spectrum analyzer this will look like in Figure 3.3.

Now the task is simply to adjust the incoming polarization to flatten this line. This will typically require a combination of a half-wave and a quarter-wave plate. In the configuration shown in Figure 3.2, the phase modulator is located after the amplitude modulator. This means that when adjusting the polarization going into the amplitude modulator, one is also adjusting the power going into the phase modula-

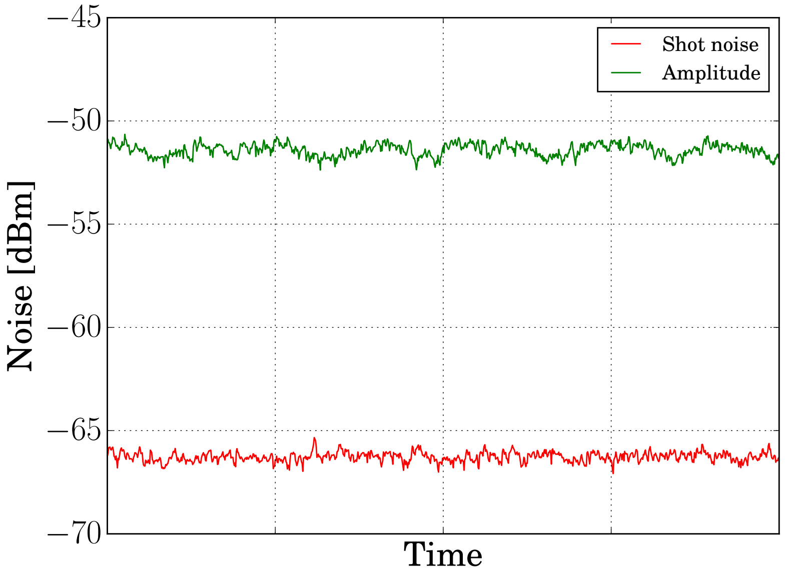


Figure 3.4: A zero span spectrum analyzer measurement of a symmetric thermal state, where the input polarization into the amplitude modulator is chosen correctly. The measurement is performed with a homodyne detector, where the relative phase between the signal and local oscillator is continuously scanned, which gives a time dependence on the measured quadrature. Here, the sinusoidal pattern is mostly gone because the two applied modulations are close to being orthogonal.

tor, affecting the size of the modulation there. Since this approach of attempting to flatten the line only works if the modulations are equal, this is important to keep in mind. One therefore has to adopt an iterative approach where the wave plates are adjusted, followed by a check of the individual modulation depths and then further wave plate adjustment. This can be partially remedied by monitoring the amount of power dumped after the amplitude modulator. If this stays constant, then the power forwarded to the phase modulator will also stay constant, and so the modulation will stay the same. However, to do this one needs to compensate with the half wave plate, and this will shift the transfer function of the amplitude modulator, and effectively change the modulation depth. So either way it is important to monitor the relative modulation depth. Typically, the fluctuations in the flatness can be reduced well below 1 dB for 15 dB of modulation relative to the shot noise, but this depends critically on the purity of the incoming polarization. The zero span measurement will then look like on Figure 3.4. It is often useful to use a series of polarizing beam splitters in transmission to properly "clean" the polarization before the modulators.

To sum up, the algorithm to orthogonalize two polarizations consists of the following steps:

1. Input two independent noise signals to the pair of modulators shown in Figure 3.2

2. Measure these modulations on a scanned homodyne detector
3. Adjust input polarization with the half wave plate such that the PBS after the modulator removes half the optical power
4. Check that the modulations have equal absolute magnitude
5. Measure both modulations simultaneously
6. Adjust the quarter wave plate to minimize the oscillation seen in Figure 3.3
7. Go to step 3 and repeat the procedure until the measurement looks like Figure 3.4

Mode cleaning cavity

One type of cavity that was used extensively in the laboratory was the mode cleaning cavity. This was a travelling wave type cavity with an arrangement of three mirrors as shown in Figure 3.5. The purpose of this type of cavity was, as the name implies, to function as a filter for the light beam. The cavity filtered the spatial and polarization modes, and it effectively dampened any laser noise beyond its bandwidth. It was also used as a reference when interfering beams. Two beams that both fit into such a cavity are guaranteed to have the same mode characteristics, and so they will automatically interfere well.

The rear mirror was curved with a radius of curvature of 1 m, which ensured a focus between the two incoupling mirrors. The effective cavity length was 0.5 meters, and this length was scanned within a single wavelength by having a piezo electric actuator push the mirror back and forth depending on the applied voltage. For locking the cavity the reflected input was used to generate an error signal through a PDH scheme as described in Section 3.6.1. Unlike a linear cavity the reflected beam was returned at an angle to the incoming beam. It was therefore quite simple to measure the reflected input without the use of a Faraday rotator.

Squeezing cavities

Bowtie cavity

Figure 3.6 shows the squeezer that was initially used in the laboratory to generate squeezed states. This was subsequently replaced by the linear squeezer described in Section 3.5.2. The bowtie cavity had an arrangement of 4 cavity mirrors, with a periodically poled potassium titanylphosphate (PPKTP) crystal located between the two internal mirrors on a copper stage, temperature controlled by a Peltier element to stay near 30 °C. The pump beam was dumped directly after passing through the crystal. The effective cavity length was 25 cm with a tight beam waist in the center

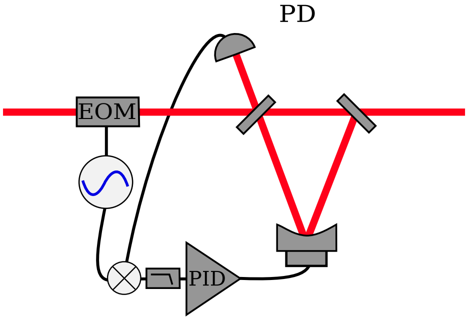


Figure 3.5: Sketch of the ring cavity with three mirrors used as a mode cleaning cavity. The input beam is phase modulated on a sideband, and the reflected part of the input beam is detected, mixed down and low-pass filtered to generate an error signal for a PDH lock, described in Section 3.6.1. This cavity has a high finesse and filters polarization, spatial mode and sideband noise. The rear mirror is actuated by a voltage controlled piezo crystal, to change the effective cavity length, thereby changing the resonance condition. EOM: Electro-optical modulator, PD: Photo detector, PID: Servo controller.

of the crystal. The incoupling mirror was highly reflective at 99.8 % while the outcoupling mirror had a reflectivity of 90 % resulting in a cavity finesse of 55 and a cavity bandwidth around 25 MHz [116].

The seed beam was injected into the cavity and served as a carrier for the generated squeezing, while the cavity was held resonant for this beam by counter-propagating a phase modulated TEM 01 beam, which had been frequency shifted by an acousto-optical modulator to coincide with the frequency of the seed beam, such that these modes overlapped in the cavity spectrum. The locking beam was kept in a different spatial mode to prevent interference between the locking and seed beams. The outcoupled locking beam was measured in cavity transmission by a photo detector and the output of this measurement was mixed down from the sideband frequency to generate an error signal, as described in Section 3.6.1.

The phase of the injected pump relative to the seed was locked by tapping off 1 % of the output squeezing and measuring it on a photo detector. The 12 MHz pump sideband that was also used for the second harmonic generation in the laser was imprinted on the squeezed output, and so the photo detector measurement of the tap-off was mixed down with this signal to generate an error signal that was able to lock the pump phase.

Linear cavity

Figure 3.7 shows the scheme for generating squeezing with a semi-monolithic linear cavity. The outer crystal face was coated to be highly reflective at 99.9 % for 1064 nm light. The curved mirror had a curvature of -20 mm, a reflectivity of 90 % for 1064 nm

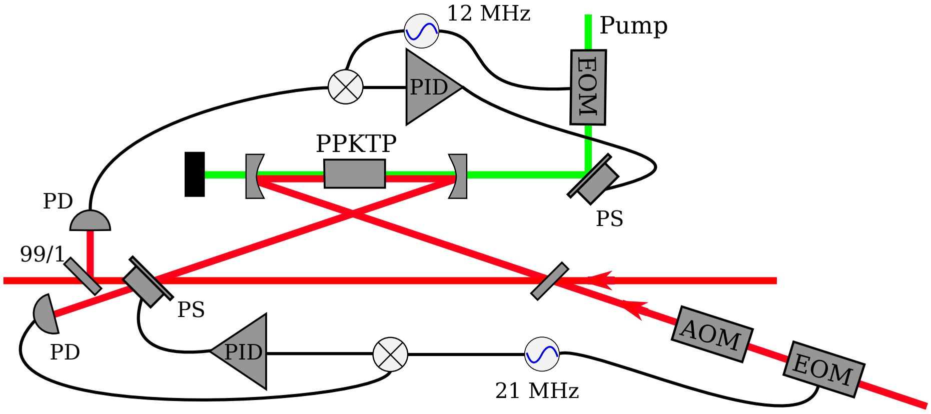


Figure 3.6: Scheme for producing vacuum squeezing with a bowtie cavity. The cavity is locked with a beam which propagates counter to the seed beam. The pump is dumped after the first crystal pass. EOM: Electro-optical modulator, AOM: Acousto-optical modulator, PD: Photo detector, PPKTP: Periodically poled potassium titanyl phosphate crystal, PS: Phase shifter, PID: Servo controller.

light, and 20 % reflectivity for 532 nm. The crystal was kept at a constant 36.7 °C, by a having a Peltier element heat a copper mount thermally coupled to the crystal by a layer of Indium foil, to satisfy the phase matching criterion [117]. The airgap between the crystal and the curved mirror determined the cavity length, which was chosen to be 23 mm. The airgap was adjustable by exchanging the PolyMethylMethAcrylate (PMMA) spacer plate with one of a different thickness. The cavity length was varied on the order of the light wavelength by the actuation of the curved mirror through a piezo electric transducer receiving an input from a high voltage amplifier.

An EOM modulated a sideband in the phase quadrature onto the 1064 nm control beam, at 37 MHz. This was sent to the side of the cavity with the highly reflective (HR) incoupling mirror, while a pump beam at 532 nm was sent in from the non-HR side. The reflection was sent to a photo detector by a Faraday rotator and a polarizing beam splitter. The two outputs of the detector were demodulated with a sine and a cosine respectively, both with a frequency of 37 MHz. This was achieved by adjusting the relative phases $\Delta\varphi$ and $\Delta\theta$ from Figure 3.7, respectively. One signal was used as an error signal for locking the cavity length through a servo controller. The other signal was used to fix the phase of the pump relative to the injected control beam, to prevent the squeezing ellipse from rotating in phase space. The squeezed beam exited through the non-HR side, and was reflected by a dichroic beam splitter such that it could be safely detected without the pump beam influencing the detector.

If the seed beam is shot noise limited, this scheme generates vacuum squeezing, and so it typically does not represent the general transformation defined in Equation 2.7.8. The experiment described in Chapter 9 required an in-line squeezing transform of an, in principle, arbitrary input state. For this purpose the control beam was injected from the non-HR side to minimize loss to the input state, which necessitated a different

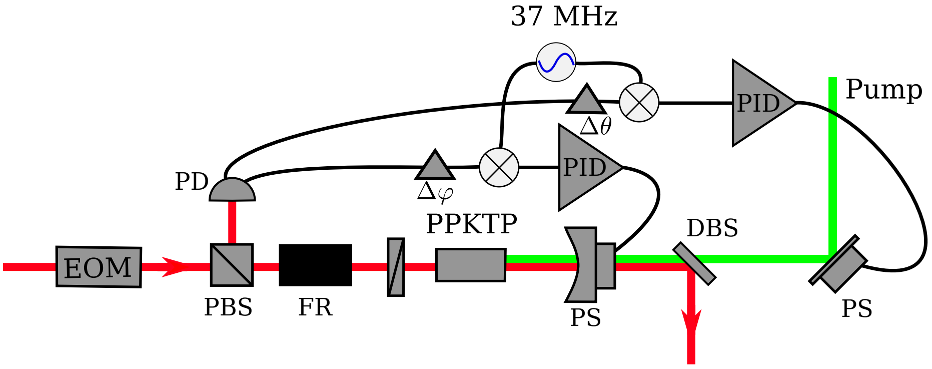


Figure 3.7: Scheme for producing vacuum squeezing with a linear cavity. The control beam was phase modulated by an EOM and was largely reflected by the HR coated incoupling crystal facet, before being redirected to a photo detector by a Faraday rotator. The photo detector generated two out of phase error signals to lock the cavity length and relative pump phase. The pump was sent in from the non-HR side, encountering a weak cavity with 20 % reflectivity at the incoupling mirror and 99.9 % at the outer crystal face. The squeezing propagated out of the cavity through the non-HR side and was separated from the pump beam by a dichroic beam splitter. EOM: Electro-optical modulator, FR: Faraday rotator, PD: Photo detector, PPKTP: Periodically poled potassium titanyl phosphate crystal, PS: Phase shifter, PID: Servo controller, DBS: Dichroic beam splitter, PBS: Polarizing beam splitter.

locking scheme. This scheme is shown in Figure 3.8. Here, having two error signals out of phase turns out to not be possible, because the resonant cavity induces an extra phase shift of the sideband locking modulation that cannot readily be compensated for. Instead, the cavity length was locked with a Hänsch-Couillaud locking technique, described in Section 3.6.2, and the pump phase was locked through the conventional sideband lock.

Locking techniques

Pound-Drever-Hall

To show the working principle of the Pound-Drever-Hall locking technique [114, 118, 119], we follow the analysis of Black [113]. Consider an empty Fabry-Perot cavity, as depicted in Figure 3.9. In front of the incoupling mirror to this cavity, we have the electric field components,

$$E_{\text{in}} = E_0 e^{i\omega t} \qquad , \qquad E_{\text{ref}} = E_1 e^{i\omega t} \ , \tag{3.6.1}$$

where E_0 and E_1 are field amplitudes represented by complex numbers with some relative phase, ω is the angular frequency, and t is time. E_{in} is the incoming field and E_{ref} is the field component reflected from the incoupling cavity mirror. The reflection coefficient is,

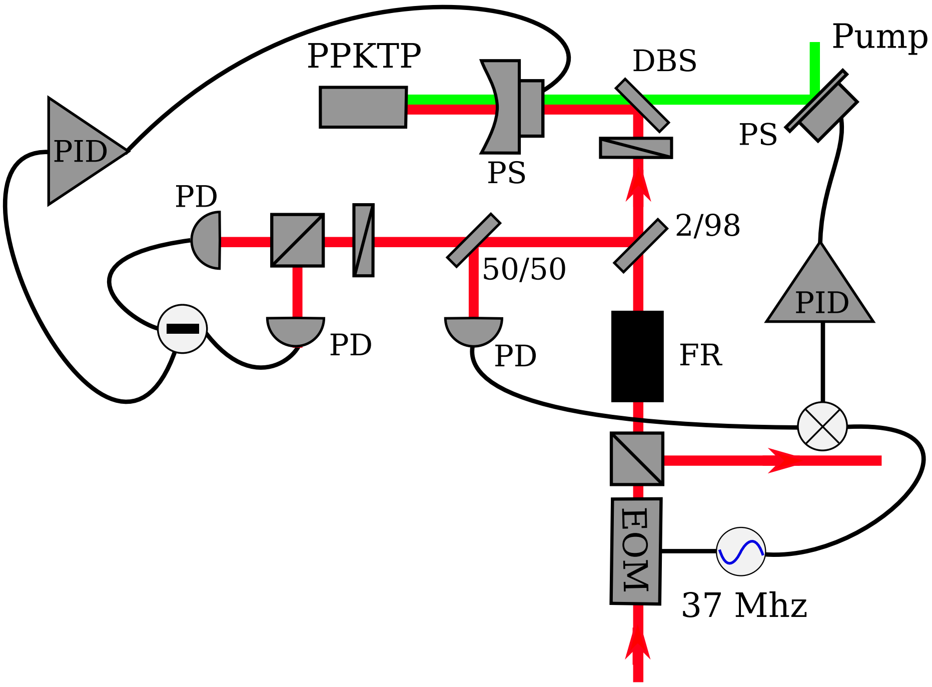


Figure 3.8: Scheme for producing vacuum squeezing with a linear cavity, with reverse injection of the control beam. The control beam was phase modulated by an EOM. For reverse injection, the beam was coupled into the cavity by the 90 % reflectivity piezo mounted mirror, and the output of the cavity was redirected by a Faraday rotator. The output beam had a 2 % tap-off, which was split in two, one for a Hänsch-Couillaud cavity length lock, and one for a sideband pump phase lock. The squeezing propagated out of the cavity through the non-HR side and was separated from the pump beam by a dichroic beam splitter. EOM: Electro-optical modulator, FR: Faraday rotator, PD: Photo detector, PPKTP: Periodically poled potassium titanyl phosphate crystal, PS: Phase shifter, PID: Servo controller, DBS: Dichroic beam splitter, PBS: Polarizing beam splitter.

$$F(L) = \frac{E_{\text{ref}}}{E_{\text{in}}} = \frac{R\left(\exp\left(i\frac{\omega}{\Delta\nu_{\text{fsr}}}\right) - 1\right)}{1 - R^2\exp\left(i\frac{\omega}{\Delta\nu_{\text{fsr}}}\right)}\ , \tag{3.6.2}$$

with R as the reflection coefficient of both cavity mirrors, $\Delta\nu_{\text{fsr}} = \frac{c}{2L}$ being the free spectral range of the cavity, L is the cavity length, and c is the speed of light in vacuum. Changing L changes the ratio, such that when the cavity is resonant, $F = 0$, though in general F is a complex number that depends on how close to resonance the cavity is. The phase of the reflected beam is changed depending on whether the cavity is too long or too short, and so knowing this phase will let us know how to compensate for this. We may obtain indirect knowledge of this phase through a determination of $F(L)$.

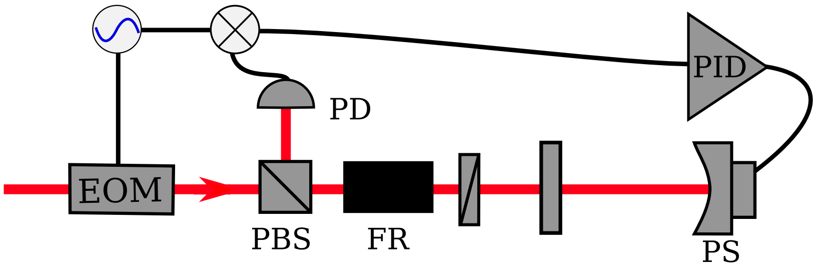


Figure 3.9: A Fabry-Perot cavity with a Pound-Drever-Hall locking scheme. The input beam is phase modulated before being sent towards the cavity. The beam reflected by the cavity is redirected by a Faraday rotator and a polarizing beam splitter. This reflected beam is measured by a photo detector, and the output is mixed with a sine at the sideband frequency. This downmixed signal is the error signal, and it is forwarded to a PID circuit, which controls the cavity length. PBS: Polarizing beam splitter, PD: Photo detector, FR: Faraday rotator, PS: Phase shifter, PID: Servo controller.

Suppose we inject an electric field, modulated with a frequency Ω. For a plane wave, we have the field from Equation (3.3.3),

$$E_{\text{in}} \approx E_0(J_0(\eta)e^{i\omega t} + J_1(\eta)e^{i(\omega-\Omega)t} - J_1(\eta)e^{i(\omega-\Omega)t}) \ , \tag{3.6.3}$$

injected into the cavity. Then the reflected field is given by,

$$E_{\text{ref}} = E_0(F(\omega)J_0(\eta)e^{i\omega t} + F(\omega+\Omega)J_1(\eta)e^{i(\omega+\Omega)t} - F(\omega-\Omega)J_1(\eta)e^{i(\omega-\Omega)t}) \ . \tag{3.6.4}$$

The reflected power is measured by a photo detector, so we measure $|E_{\text{ref}}|^2$, which may be expressed as,

$$\begin{aligned} |E_{\text{ref}}|^2 = P_c|F(\omega)|^2 + P_s(|F(\omega+\Omega)|^2 + |F(\omega-\Omega)|^2) \\ + 2\sqrt{P_cP_s}(\Re[F(\omega)F^*(\omega+\Omega) - F^*(\omega)F(\omega-\Omega)]\cos(\Omega t) \\ + \Im[F(\omega)F^*(\omega+\Omega) - F^*(\omega)F(\omega-\Omega)]\sin(\Omega t) + h(t) \ , \end{aligned} \tag{3.6.5}$$

where $h(t)$ is a function that oscillates with a period of 2Ω, which is not important for the analysis. Thus, in the rotating carrier frame, the photodetector returns a signal which has a DC component and a component that oscillates with the sideband frequency. Mixing this output down with the sideband frequency gives the needed error signal. Here, the phase of the mixing is important, depending on whether it is the real or the imaginary part of $F(\omega)F^*(\omega+\Omega) - F^*(\omega)F(\omega-\Omega)$ that provides the necessary information. In the case of the pumped semi-monolithic linear cavity described in Section 3.5.2, the real and imaginary parts both contribute, in the sense that one contains information of the pump phase and the other contains information of the cavity length detuning.

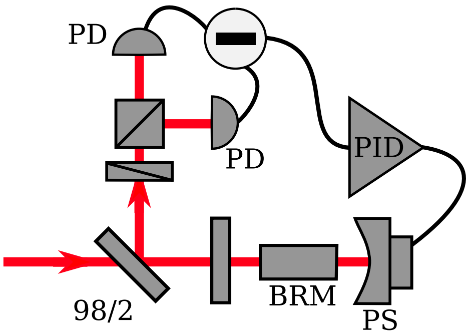


Figure 3.10: A Fabry-Perot cavity with a Hänsch-Couillaud locking scheme. The beam reflected from the cavity is tapped off, and the polarization components are mixed on a polarizing beam splitter to generate an interference signal. The interference is measured by subtracting two photocurrents, and this error signal is forwarded to a servo controller, which controls the cavity length. This scheme only works if the polarization modes in the cavity spectrum are not degenerate. BRM: Birefrigent medium, PS: Phase shifter, PD: Photo detector, PID: Servo controller.

Hänsch-Couillaud

Consider a linear cavity, as in Figure 3.10, with some birefringent quality that causes a splitting of the polarization modes in the spectrum. As demonstrated by Hänsch and Couillaud [120], this birefringence can be used to lock the length of a cavity without the use of a modulation sideband. In fact, all that is required is polarization optics and an intensity measurement.

Suppose the incoming beam is split into a horizontal and a vertical component, where the splitting ratio is determined by the angle θ. Then we may write the incoming field components as,

$$E_{\mathrm{in},||} = E_{\mathrm{in}} \cos(\theta) \qquad , \qquad E_{\mathrm{in},\perp} = E_{\mathrm{in}} \sin(\theta) \ . \tag{3.6.6}$$

For a particular cavity length, the mode of horizontal polarization is admitted, while for another cavity length the vertical polarization mode is admitted. In either case, the component parallel to the cavity polarization axis fits into the cavity mode, and so the component of it reflected by the cavity experiences a phase shift from travelling through the cavity and back. The perpendicular component never enters the cavity, but is instead promptly reflected and experiences no such phase shift. This phase difference between the reflected components is exactly what is needed to generate an error signal.

In terms of the cavity parameters, we may write the reflected field components as [83, 120],

$$E_{\mathrm{ref},||} = E_{\mathrm{in},||} \left(\sqrt{R} - TR^{3/2} \frac{\cos(\delta) - R^2 + i\sin(\delta)}{(1-R^2)^2 + 4R^2 \sin(\delta/2)^2} \right) \ , \tag{3.6.7}$$

$$E_{\mathrm{ref},\perp} = E_{\mathrm{in},\perp}\sqrt{R}\ , \tag{3.6.8}$$

where R and T are the reflectivity and transmissivity for the incoupling mirror.

When the cavity is resonant we have $\delta = 2m\pi$ and the field amplitudes of the reflected fields are real numbers, which means that they are linearly polarized. If the cavity is off resonance, the parallel reflected field component, $E_{\mathrm{ref},||}$ becomes complex, and so acquires a relative phase to the perpendicular reflected component. This will make the polarization of the reflected beam elliptic. The reflected beam is sent to a polarizing beam splitter, which separates it into a vertical and a horizontal component. By rotating the incoming polarization components appropriately, we can force an interference between the parallel and perpendicular polarization components. The intensities of these components are measured and subtracted, which gives an error signal caused by the interference phenomenon. The strength of the error signal depends on the polarization of the incoming beam, such that an incoming beam polarized in only one direction will not produce an error signal, so at least a small asymmetry is required. In fact it turns out that an equal distribution of polarization components into the cavity will maximize the error signal.

Implementing this locking scheme on the linear cavity described in Section 3.5.2 resulted in a transmission spectrum and a corresponding error signal as seen in Figure 3.11. One drawback of this locking technique is that it is power dependent, so that when the gain medium in the cavity is pumped and the pump phase is not locked, the servo controller in the Hänsch-Couillaud lock will try to compensate the resulting sinusoidal behaviour in the error signal. However, because of the strength of the error signal and the moderate pump power this fluctuation was not enough to break the lock before the locking mechanism for the pump phase could be activated.

Measurements

Homodyne detection

A conditional measurement on Gaussian states by homodyne detection was described in terms of covariance matrices in Section 2.10. Here, we will explain how a homodyne detection is implemented in the laboratory. The scheme is illustrated in Figure 3.12.

A strong carrier beam, the local oscillator, is sent to a 50/50 beamsplitter, to be interfered with the signal beam. We write the ladder operators for these modes in the form [29, 85],

$$\hat{\boldsymbol{X}} = (\hat{b}e^{i\phi}, \hat{b}^\dagger e^{-i\phi}, \hat{a}, \hat{a}^\dagger)^T\ , \tag{3.7.1}$$

where $\hat{b}$ is for the local oscillator mode, $\hat{a}$ is for the signal mode, and ϕ is the relative phase between the two modes. Applying a 50/50 beamsplitter through the symplectic transformation $\boldsymbol{S}_{BS}(T)$,

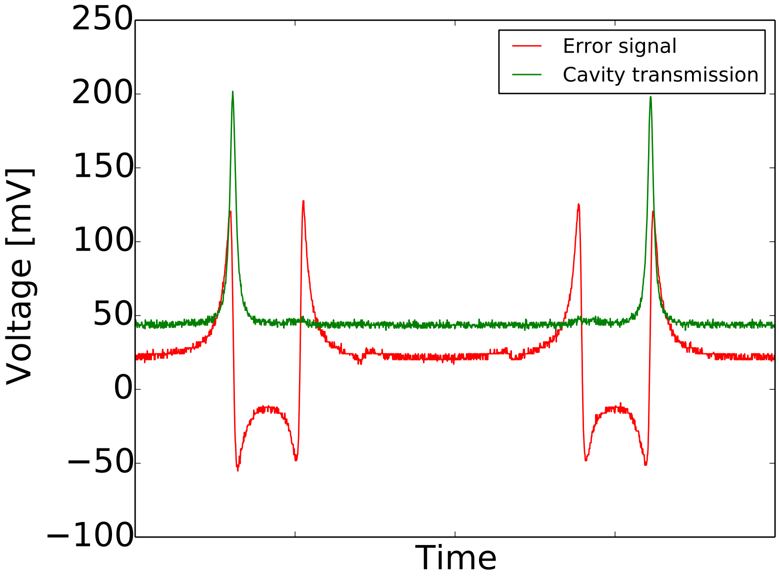


Figure 3.11: Airy peaks and corresponding error signal from the implementation of a Hänsch-Couillaud locking technique on a linear cavity with a birefringent PPKTP crystal. There is a strong error signal for both horizontal and vertical polarization, but the incoming beam is only 2 % horizontal, so the transmission peak for horizontal polarization is correspondingly tiny.

$$\boldsymbol{S}_{\mathrm{BS}}\left(\frac{1}{2}\right)\hat{\boldsymbol{X}}=\begin{pmatrix}\frac{1}{\sqrt{2}}(\hat{b}e^{i\phi}+\hat{a})\\ \frac{1}{\sqrt{2}}(\hat{b}^{\dagger}e^{-i\phi}+\hat{a}^{\dagger})\\ \frac{1}{\sqrt{2}}(-\hat{b}e^{i\phi}+\hat{a})\\ \frac{1}{\sqrt{2}}(-\hat{b}^{\dagger}e^{-i\phi}+\hat{a}^{\dagger})\end{pmatrix}=\begin{pmatrix}\hat{c}\\ \hat{c}^{\dagger}\\ \hat{d}\\ \hat{d}^{\dagger}\end{pmatrix}\ . \tag{3.7.2}$$

We define the photocurrent operators as proportional to the counting operators, $\hat{n}_c = \hat{c}^\dagger\hat{c}$ and $\hat{n}_d = \hat{d}^\dagger\hat{d}$, so

$$\hat{i}_c \propto \hat{c}^\dagger\hat{c}\ , \tag{3.7.3}$$

$$\Updownarrow$$

$$\hat{i}_c \propto \frac{1}{2}(\hat{b}^\dagger e^{-i\phi}+\hat{a}^\dagger)(\hat{b}e^{i\phi}+\hat{a})\ , \tag{3.7.4}$$

$$\Updownarrow$$

$$\hat{i}_c \propto \frac{1}{2}(\hat{b}^\dagger\hat{b}+\hat{b}^\dagger\hat{a}e^{-i\phi}+\hat{a}^\dagger\hat{b}e^{i\phi}+\hat{a}^\dagger\hat{a})\ . \tag{3.7.5}$$

Similarly, the photocurrent from the other photo detector is given by,

$$\hat{i}_d \propto \hat{d}^\dagger\hat{d}\ , \tag{3.7.6}$$

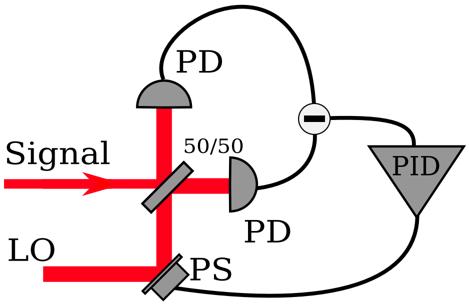


Figure 3.12: A scheme illustrating a homodyne detection of the quadratures of a signal beam. A strong local oscillator is interfered with a comparatively weak signal beam on a 50/50 beam splitter and a relative phase controlled by a phase shifter. The two output modes are measured by photo detectors, and the photocurrents generated by these photo detectors are subtracted to give a measurement outcome with a high common mode rejection. In addition, the subtraction of the DC outputs gives an error signal for locking the relative phase as $\frac{\pi}{2}$ to the local oscillator, to reliably measure the P quadrature. PS: Phase shifter, PD: Photo detector, PID: Servo controller, LO: Local oscillator.

$$\Updownarrow$$

$$\hat{i}_d \propto \frac{1}{2}(\hat{b}^\dagger\hat{b} - \hat{b}^\dagger\hat{a}e^{-i\phi} - \hat{a}^\dagger\hat{b}e^{i\phi} + \hat{a}^\dagger\hat{a}) \; . \tag{3.7.7}$$

If the photodetectors amplify their photocurrents by the same gain factor, subtracting the photocurrents gives us

$$\hat{i}_c - \hat{i}_d \propto \hat{b}^\dagger\hat{a}e^{-i\phi} + \hat{a}^\dagger\hat{b}e^{i\phi} \; . \tag{3.7.8}$$

We may linearize this expression by rewriting the ladder operators $\hat{a} = |\alpha| + \delta\hat{\alpha}$ and $\hat{b} = |\beta| + \delta\hat{\beta}$. In this way we have written the operators into classical constant parts, $|\alpha|$ and $|\beta|$, and fluctuating parts, $\delta\hat{\alpha}$ and $\delta\hat{\beta}$. We shall call $|\alpha|$ and $|\beta|$ the DC components, while $\delta\hat{\alpha}$ and $\delta\hat{\beta}$ are alternating current (AC) components [114]. They represent the noise fluctuations at the sideband of interest. Assuming the noise fluctuations to be small, we keep them only to the first order and obtain

$$\hat{i}_c - \hat{i}_d \propto 2|\beta||\alpha|\cos(\phi) + |\beta|(\delta\hat{\alpha}^\dagger e^{i\phi} + \delta\hat{\alpha}e^{-i\phi}) + |\alpha|(\delta\hat{\beta}^\dagger e^{-i\phi} + \delta\hat{\beta}e^{i\phi}) \; , \tag{3.7.9}$$

$$\Updownarrow$$

$$\hat{i}_c - \hat{i}_d \propto 2|\beta||\alpha|\cos(\phi) + |\beta|\hat{X}_{\delta\hat{\alpha}}(\phi) + |\alpha|\hat{X}_{\delta\hat{\beta}}(\phi) \; , \tag{3.7.10}$$

where the last line has introduced a generalized quadrature operator,

$$\hat{X}_{\hat{a}}(\phi) = \hat{a}e^{-i\phi} + \hat{a}^\dagger e^{i\phi} \; , \tag{3.7.11}$$

such that for $\phi = 0$, $\hat{X}_{\hat{a}}(\phi) = \hat{Q}$, and for $\phi = \frac{\pi}{2}$, $\hat{X}_{\hat{a}}(\phi) = \hat{P}$.

The first term in Equation (3.7.10) shows how the DC output from the photocurrent subtraction depends on the relative phase between the inputs. In practice this relative phase is controlled by a mirror attached to a piezo electric transducer. This transducer reacts to an applied voltage, typically of some hundreds of volts, and expands or contracts accordingly, by a distance on the order of the wavelength. This allows for very precise control of the interference between the beams. Keeping this phase stable is important, as any deviation means that a different marginal distribution of the state in question is measured. Keeping the relative phase at $\phi = \frac{\pi}{2}$ to measure $\hat{P}$ is fairly straightforward, in that the first term in Equation (3.7.10) should be zero. In this way, measuring the DC output from the subtracted photocurrents exactly provides an error signal for a locking circuit. Measuring $\hat{Q}$ is slightly more involved, in that it usually requires some auxiliary modulation to generate the error signal. If an auxiliary phase modulation is applied and the subtraction of the two AC components forces them to cancel exactly, then the homodyne detector must be measuring a marginal distribution exactly orthogonal to the phase, i.e the amplitude.

The last two terms in Equation (3.7.10) show that the operator for the fluctuations in the signal mode is amplified by $|\beta|$, and the fluctuations in the local oscillator mode are amplified by $|\alpha|$. We say that the sidebands generate a beat pattern with the carrier, in analogy with the terminology originally developed for radio technology [114]. Since we are not interested in measuring the noise contribution from the local oscillator, we arrive at the conclusion that the requirement $|\beta| \gg |\alpha|$ is necessary if we wish to resolve the quantum noise properties of the signal mode. This approximation is sometimes called the brightness approximation.

A technical benefit of the subtraction of the photocurrents is that it allows for a very high common mode rejection, upwards of 40 dB depending on the balancing of the beam splitter. This means that any noise that is common to both detectors will be cancelled out, because it appears in both photocurrents and cancels itself out, which to some degree dispenses with the requirement that the laser source be shot noise limited. Of course, the electronic noise arising from the photodetector circuit itself must still be kept low, and cannot be eliminated through this particular technique.

Heterodyne detection

A heterodyne detection scheme, see Figure 3.13, is one where the signal beam is superimposed with a vacuum mode on a balanced beam splitter. The two output modes are sent to two separate homodyne detectors, that measure P and Q respectively, with the technique described in Section 3.7.1. However, there is a more compact way of implementing this technique, provided that certain conditions are satisfied. Suppose that we implement a homodyne detector as described in Section 3.7.1, and that in addition to subtracting the photocurrents, we also add them,

$$\hat{i}_c + \hat{i}_d \propto \hat{b}^\dagger \hat{b} + \hat{a}^\dagger \hat{a} \ . \tag{3.7.12}$$

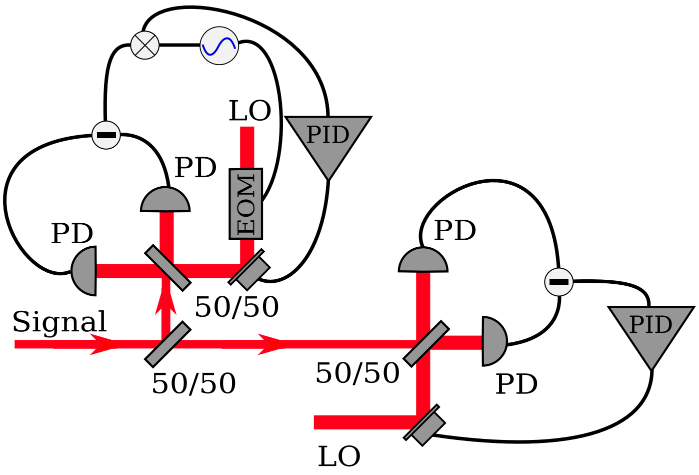


Figure 3.13: A scheme illustrating a heterodyne detection of the quadratures of a signal beam. The signal beam is split on a 50/50 beam splitter, and the two outputs are detected using two independent homodyne detectors. Two strong local oscillators are interfered with comparatively weak signal beams on 50/50 beam splitters and the relative phases controlled by phase shifters. In one homodyne detector, the relative phase is locked to $\frac{\pi}{2}$ using the subtracted DC output. The other is locked through the measurement of a phase modulated sideband. PS: Phase shifter, PD: Photo detector, PID: Servo controller, LO: Local oscillator, EOM: Electro-optical modulator.

Performing the linearization as before, we get,

$$\hat{i}_c + \hat{i}_d \propto |\beta|^2 + |\alpha|^2 + |\beta|\hat{Q}_{\delta\hat{\beta}} + |\alpha|\hat{Q}_{\delta\hat{\alpha}} \ . \tag{3.7.13}$$

Here, the photocurrents are a combination of the added DC outputs, the noise fluctuations of the local oscillator amplified by the local oscillator strength, and the noise fluctuations of the signal amplified by the signal strength. We see therefore, that for this to work we require $|\alpha|$ to be sufficiently large in order to amplify the signal oscillations. On the other hand, we saw from Equation (3.7.10) that it requires $|\beta| \gg |\alpha|$. Let us instead consider the case where $|\alpha| = |\beta|$,

$$\hat{i}_c - \hat{i}_d \propto 2|\alpha|^2 \cos(\phi) + |\alpha|(\hat{X}_{\delta\hat{\alpha}}(\phi) + \hat{X}_{\delta\hat{\beta}}(\phi)) \ , \tag{3.7.14}$$

$$\hat{i}_c + \hat{i}_d \propto 2|\alpha|^2 + |\alpha|(\hat{Q}_{\delta\hat{\beta}} + \hat{Q}_{\delta\hat{\alpha}}) \ . \tag{3.7.15}$$

We see that for both addition and subtraction, we get the signal fluctuations, but at the cost of the local oscillator noise not being cancelled. However, at the sideband of interest, and assuming a shot noise limited laser source, $\hat{X}_{\delta\hat{\beta}}$ will be the vacuum fluctuations, and so performing a heterodyne detection in this manner, the extra unit of vacuum enters through the vacuum fluctuations of the local oscillator rather than through a physical beam splitter, but otherwise performs as expected. This also requires that both carriers are sufficiently powerful to amplify the sideband fluctuations.

We may also consider the case where we wish to perform a generalized heterodyne detection, a Bell detection as described in Section 2.12. Here, the operator $\hat{X}_{\delta\hat{\beta}}$ also contains a signal, in addition to the vacuum noise. If both carriers are bright and the source is shot noise limited, adding and subtracting the photocurrents once again offers a compact alternative to a conventional Bell detection scheme, in the same way as for heterodyne detection.

Data acquisition

As we saw in Sections 3.7.1 and 3.7.2, homodyne and heterodyne measurements return photocurrents with a frequency spectrum corresponding to the sideband noise spectrum. This may be seen by, for example, measuring the voltage converted signal with a spectrum analyzer that shows the strength of the individual frequency components. Another way to record the outcome of a measurement is by digitizing it with a high speed digitizer, since we, according to Nyquists theorem [5], need to sample with at least twice the frequency of the fastest sideband we wish to investigate.

We are often only interested in one specific sideband. The solution is then to mix the voltage converted photocurrent with a sinusoidal signal at the frequency of interest. This sinusoidal signal is called the electronic local oscillator (ELO). This will cause a beat between the different frequency components. Specifically, the spectrum of the mixer output will contain the voltage converted photocurrent sideband of interest moved to DC, and the voltage converted photocurrent sideband moved up by the ELO frequency because of the identity,

$$\sin(\Omega)\sin(\Omega_{\mathrm{ELO}}) = \frac{1}{2}(\cos(\Omega - \Omega_{\mathrm{ELO}}) - \cos(\Omega + \Omega_{\mathrm{ELO}}) \ , \qquad (3.7.16)$$

where Ω is the sideband frequency and Ω_{ELO} is the ELO frequency. We here wish to measure the component with the frequency $\Omega - \Omega_{\mathrm{ELO}}$, since this enables the analog-to-digital converter to sample near DC. To attenuate the component at frequency $\Omega + \Omega_{\mathrm{ELO}}$, and also to avoid the aliasing effects predicted by Nyquist's theorem, a low-pass filter is inserted before the analog-to-digital conversion.

A low-pass filter in this position determines the measurement bandwidth, typically in the hundreds of kHz, but to completely avoid the aliasing a sampling frequency higher than twice the measurement bandwidth should be selected, such that the filter is able to properly suppress the high-frequency components in the spectrum. This choice of frequency depends primarily on the slope of the filter and the bit depth of the analog-to-digital converter.

Tomographic reconstruction of Wigner functions

This section introduces the concept of state reconstruction through the use of marginal quadrature probability distributions. These techniques were initially developed for medical imaging, but were then applied by Smithey *et al.* to measurements of squeezed states [93, 121].

Inverse Radon transformation

Suppose that we have measured a number of marginal distributions of some state through the use of homodyne detection. We have seen in Section 3.7.1 that this can be accomplished by changing the relative phase between the signal and local oscillator beams. For each phase angle we may define a new marginal distribution, and we collect these probability distributions to get the two dimensional probability $\mathrm{pr}(X,\theta)$. Thus, for a given angle θ, $\mathrm{pr}(X,\theta)$ quantifies the probability of the outcome X. We note that Wigner functions have the important property [82],

$$\mathrm{pr}(X,\theta) = \int_{-\infty}^{\infty} W(X\cos(\theta) - P\sin(\theta), X\sin(\theta) + P\cos(\theta))\mathrm{d}P \ . \tag{3.8.1}$$

To put this in words, the marginal distributions obtained through our homodyne detection with varied relative phase are given by the integral over P of a Wigner function at an angle θ to the conventional coordinate system.

Since quantum mechanical measurements in general, and homodyne measurements in particular, only ever produce marginal distributions, Equation (3.8.1) provides a convenient relation between the experimentally obtained marginal distributions and the Wigner function that uniquely describes the state. Inverting this integral is the objective of the so called inverse Radon transform. The inversion has the form [82],

$$W(Q,P) = \frac{1}{2\pi^2}\int_0^{\pi}\int_{-\infty}^{\infty} \mathrm{pr}(X,\theta)K(Q\cos(\theta) + P\sin(\theta) - X)\mathrm{d}X\mathrm{d}\theta \ , \tag{3.8.2}$$

where $K(x)$ is the integration kernel,

$$K(x) = \frac{1}{2}\int_{-\infty}^{\infty} |\xi| e^{i\xi x}\,\mathrm{d}\xi \ . \tag{3.8.3}$$

The filtered back projection algorithm is a straightforward method for implementing this inversion [82]. Given a histogram containing the obtained marginals one sets a cutoff frequency in the kernel integral, such that it becomes

$$K(x) = \frac{1}{2}\int_{-k_c}^{k_c} |\xi| e^{i\xi x}\,\mathrm{d}\xi = \frac{1}{x^2}(\cos(k_c x) + k_c x\sin(k_c x) - 1) \ . \tag{3.8.4}$$

Because this function is not well behaved around $x = 0$ one introduces a threshold $|k_c x| = 0.1$ such that,

$$K(x) = \begin{cases} \frac{1}{x^2}(\cos(k_c x) + k_c x\sin(k_c x) - 1) & \text{when } |k_c x| > 0.1 \\ \frac{k_c^2}{2}\left(1 - \frac{k_c^2 x^2}{4} + \frac{k_c^4 x^4}{72}\right) & \text{when } |k_c x| \leq 0.1 \end{cases} . \tag{3.8.5}$$

k_c is a free parameter in the sense that there is no value that works for every state one wishes to reconstruct. One may regard it as a frequency filter, such that it determines the minimum size of the features in the Wigner function that will be resolved. If the value is too high the reconstruction will contain characteristic ripples. If the value is too low the reconstruction will turn into a featureless lump.

Maximum likelihood

The maximum likelihood algorithm is fundamentally different from the inverse Radon transform. Instead of getting the Wigner function as output, the maximum likelihood algorithm generates the density matrix most likely to be responsible for the observed marginal distributions. This density matrix is represented in the Fock basis. Since a harmonic oscillator is unbounded in photon number, it is necessary to truncate the density matrix. As long as this is done at a point where the photon distribution of the state to be reconstructed is sufficiently attenuated, this is not a problem.

This condition of suitably small photon numbers is rather easily achieved for squeezed vacuum states and small displacements, since the mean photon number is low for these states. However, for a thermal state with high variance the photon number decays slowly and so maximum likelihood will likely be too slow to solve the problem. The maximum likelihood algorithm is however preferable to the inverse radon transform for low photon numbers because it is more likely to be numerically stable, and has no free parameter that must be chosen rather arbitrarily by the user [122].

The problem one wishes to solve is the same as for the inverse Radon transform, but it must be stated slightly differently. Suppose again, that we have a marginal probability distribution for some angle θ in the Q, P phase space. This probability distribution is described by the trace formula,

$$\mathrm{pr}(\theta) = \mathrm{Tr}(\hat{\mathcal{M}}_\theta \hat{\rho}) \ , \tag{3.8.6}$$

of the state $\hat{\rho}$ one wishes to reconstruct with the POVM $\hat{\mathcal{M}}$ for the angle θ [122, 123]. In this way $\hat{\mathcal{M}}$ represents the measurement that produces the relevant marginal distribution. We define the iteration operator

$$\hat{R}(\hat{\rho}) = \sum_i \frac{\hat{\mathcal{M}}_\theta(X_i, \theta_i)}{\mathrm{pr}(X_i, \theta_i)} \ , \tag{3.8.7}$$

which is applied with the recursion

$$\hat{\rho}^{(k+1)} = \hat{R}(\hat{\rho}^{(k)})\hat{\rho}^{(k)}\hat{R}(\hat{\rho}^{(k)}) \ , \tag{3.8.8}$$

and normalization in each step, to guarantee that $\mathrm{Tr}\hat{\rho}^{(k+1)} = 1$. It can be shown, using variational calculus, that the likelihood functional,

$$\mathcal{L} = \prod_i \mathrm{pr}_{\hat{\rho}}(X_i, \theta_i) \ , \tag{3.8.9}$$

is maximized by this choice of iteration in most cases [122, 124]. The essence of the algorithm is that one sets up an initial $\hat{\rho}$, either a vacuum state or a maximally mixed state, or something of the sort. Then one constructs a projection operator $\hat{R}(\hat{\rho})$ from Equation (3.8.7), which depends on the observed marginals and the wavefunctions of the relevant Fock states. These are proportional to the well known Hermite polynomials, which can be generated recursively rather easily.

For each iteration the projection operator is applied to the density matrix, a new projection operator is constructed based on the outcome of this, and this process continues either until a certain convergence threshold has been reached or a particular number of iterations have been performed, such that one is reasonably certain that $\hat{\rho}$ has converged towards the correct answer. Figure 3.14 shows a comparison between inverse Radon and maximum likelihood reconstruction of a squeezed vacuum state.

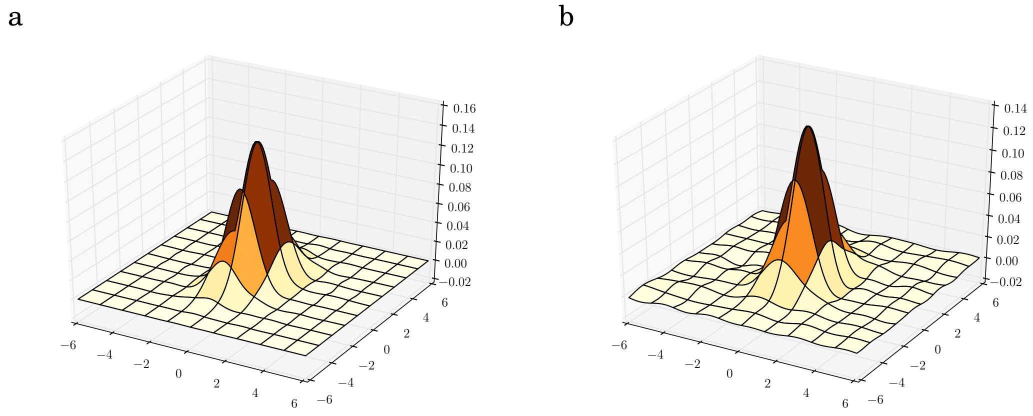


Figure 3.14: Comparison of the reconstructed Wigner functions of a squeezed state, with (a) maximum likelihood and (b) inverse Radon transformation. The inverse Radon reconstruction has distinct ripples that are not present when using maximum likelihood.

High-rate measurement device independent quantum cryptography

Introduction

In the discussion of secure quantum communication between two honest parties, we usually have a simple scenario where Alice wishes to communicate with Bob and Eve is eavesdropping on the quantum channel between them that facilitates the conversation. This is the configuration considered for the development of the BB84 protocol [7], and many subsequent developments [18, 42, 43, 44, 47, 48]. However, an important component in the development of modern information theory is the idea of the relay.

The simplest useful configuration we can imagine without falling back to simple point-to-point protocols consists of three parties. Two of these are the actual users, Alice and Bob, and the third party is Charlie, who is charged with relaying information between Alice and Bob. In quantum information theory this construction occurs in a variety of protocols, where different levels of trust and signalling assumptions are distributed across the different parties, creating many interesting scenarios [15, 16, 20, 35, 125, 126]. A collection of such relays could form the first iteration of the so-called quantum internet [127].

Of particular interest is the idea of measurement device independent quantum key distribution (MDIQKD) [34, 35]. This is, in a sense, a weaker version of the powerful idea of device independent quantum key distribution [32, 33], where the breaking of a Bell like inequality certifies the security of the scheme independently of the sources and the detection. This is useful if one is not willing to trust the manufacturer, but the nature of the scheme makes it incredibly hard to realize in a practical way. Point-to-point protocols generally assume that both sources and measurement devices can be trusted, which is not necessarily justifiable in in-field implementations [40, 41, 128, 129]. Failure to align the implementation with the assumptions made in the security proof lead to side channels that can be exploited by quantum hackers [130, 131, 132, 133]. These attacks are by their very nature highly dependent on the implementation, but they underline the fact that it is necessary to be aware of the assumptions made. Therefore, the fewer assumptions one has to make, the stronger the system is.

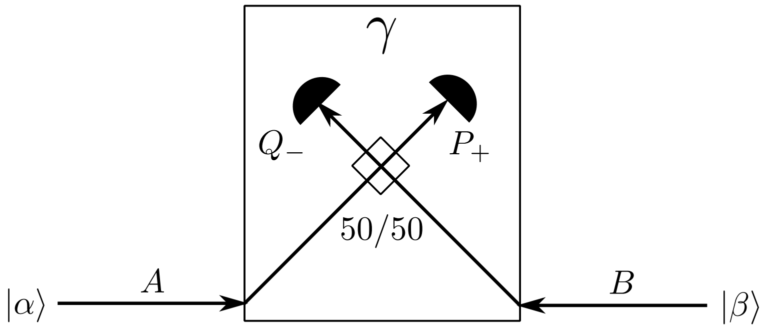


Figure 4.1: Basic relay configuration with a continuous variable Bell detection and coherent state inputs from Alice and Bob.

Measurement device independence is a concept that allows for dispensing with the trust assumptions on the detection hardware, though the state production must remain trusted. In this way it strikes the balance between standard point-to-point protocols and the completely device independent protocols that utilize entanglement. Despite this being a weaker property than full device independence, it is also fundamentally easier to achieve [134, 135, 136], and consequently can be more readily applied in practical scenarios. One further advantage of measurement device independence is that it allows for the construction of a more convenient network structure, and in particular to dispense with the end-to-end networking principle [137, 138].

What we demonstrate here is the theoretical development and experimental test of the first measurement device independent protocol in continuous variables (CVMDIQKD). The protocol for CVMDIQKD is roughly this:

1. Alice and Bob prepare random coherent states $|\alpha\rangle$ and $|\beta\rangle$.
2. Alice and Bob forward their states to a relay.
3. The relay performs a Bell-like detection on the input states and broadcasts the outcome γ publicly.
4. With the knowledge of γ Alice can infer $|\beta\rangle$ and vice versa.

The scheme is illustrated in Figure 4.1. What is interesting about this protocol is that without making any assumptions on the detection, it can be shown that Eve can not in any way manipulate the measurement of the relay or the announcement of γ to give herself an advantage. She can of course refuse to announce γ or announce a wrong value, but this is a trivial denial-of-service attack that is always available, even in point-to-point protocols.

In practice it turns out that a spatially symmetric configuration is not optimal. What is indeed optimal is that one party is closer to the relay. This allows the other party to be quite far away, and the total range between the parties can be much greater than is the case for a symmetric configuration. The theory for this protocol was developed by Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel Braunstein and Seth Lloyd, while the experiment was implemented by this author and colleagues. This work was published in [139].

Theory

To make the above discussion more concrete let us derive the properties of the protocol. As mentioned, Alice and Bob prepare coherent states $|\alpha\rangle$ and $|\beta\rangle$ respectively. Now, as argued in Section 2.8, we may regard this as Alice and Bob preparing EPR states of some magnitude, with each of them sending one mode toward the relay and keeping the other for conditioning. We therefore have an initial covariance matrix of the form,

$$\mathbf{\Gamma}_{aAbB} = \begin{bmatrix} \mu\mathbb{I}_2 & \sqrt{\mu^2-1}\boldsymbol{Z} & \mathbf{0}_2 & \mathbf{0}_2 \\ \sqrt{\mu^2-1}\boldsymbol{Z} & \mu\mathbb{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{0}_2 & \mu\mathbb{I}_2 & \sqrt{\mu^2-1}\boldsymbol{Z} \\ \mathbf{0}_2 & \mathbf{0}_2 & \sqrt{\mu^2-1}\boldsymbol{Z} & \mu\mathbb{I}_2 \end{bmatrix} . \tag{4.2.1}$$

The lower case modes a and b are the modes kept locally by Alice and Bob, respectively. The upper case modes A and B are sent towards the relay. We choose both EPR states to have size μ. There is no reason for Alice and Bob to pick different values, and they can easily agree on this choice beforehand. In the density matrix formalism this overall system is described by the state $\hat{\rho}_{aAbBE}$, when we include the modes of the eavesdropper. This global state containing all relevant modes is pure. Now we allow Eve to implement some unitary operator $\hat{U}$ on all the modes except a and b, as seen in Figure 4.2. This will leave the overall state pure, but there is no requirement that this operation preserve Gaussianity. We recall that local operations always commute because they take place in different modes. This means that we may consider the effects of Eve's measurement before we consider the conditioning measurements of Alice and Bob. We then use the fact that [71] any Gaussian operation may be represented as a sequence of Gaussian channels with unitary operations and subsequent homodyne detections. We assume that the eavesdropper implements a Gaussian detection operation, because this will maximize her information content as argued in Section 2.13.

By extension, we simply assume that Eve implements homodyne detection, since the transformation that takes the actual detection method into homodyne detection may be absorbed into the unitary $\hat{U}$. Let us call the overall state conditioned on this measurement outcome $|\Phi_{abE|\gamma}\rangle$, where γ is the measurement outcome. Since Eve implemented homodyne detection, the state $|\Phi_{abE|\gamma}\rangle$ is pure. It is composed of the reduced states $\hat{\rho}_{ab|\gamma}$ and $\hat{\rho}_{E|\gamma}$. Using the self-duality property of the von Neumann entropy from Section 2.14 we therefore conclude that,

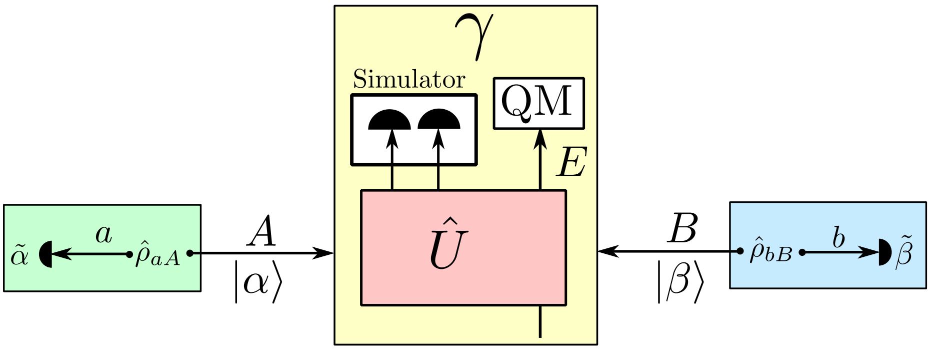


Figure 4.2: Generalized joint attack on the MDIQKD protocol. The modes A and B from Alice and Bob respectively are inputs to a unitary operation $\hat{U}$, which interferes these modes with ancillary vacuum modes controlled by Eve. $\hat{U}$ outputs two modes that simulate the effect of the relay measurement, and the rest of the outputs labelled E go to a quantum memory (QM), which Eve measures once the protocol is over in order to implement a collective attack.

$$S(\rho_{ab|\gamma}) = S(\rho_{E|\gamma}) \ , \tag{4.2.2}$$

since Eve is able to purify the post-measurement state of Alice and Bob. We now let Alice encode her outgoing state by having her perform a heterodyne measurement on mode a. Producing the outcome $\tilde{\alpha}$, we get the overall state pure state $|\Phi_{bE|\gamma\tilde{\alpha}}\rangle$. We therefore have the relation,

$$S(\hat{\rho}_{b|\gamma\tilde{\alpha}}) = S(\hat{\rho}_{E|\gamma\tilde{\alpha}}) \ , \tag{4.2.3}$$

which means that Eve is limited in her information gain by the Holevo quantity from Equation (2.14.30) expressed through the von Neumann entropies,

$$\chi(E|\gamma) = S(E|\gamma) - S(E|\gamma\tilde{\alpha}) = S(\hat{\rho}_{ab|\gamma}) - S(\hat{\rho}_{b|\gamma\tilde{\alpha}}) \ . \tag{4.2.4}$$

This is a remarkable result because it depends only on the state $\hat{\rho}_{ab|\gamma}$. Next, we let Bob perform his conditioning measurement, with the outcome $\tilde{\beta}$. The classical mutual information shared by Alice and Bob is thus determined by,

$$I(AB|\gamma) = I(\tilde{\alpha}, \tilde{\beta}|\gamma) = I(\alpha, \beta|\gamma) \ . \tag{4.2.5}$$

This quantity is also completely determined by the state $\hat{\rho}_{ab|\gamma}$. The secret key rate of the protocol is therefore given by an average over the relay measurement outcomes such that,

$$R = \int_{\mathbb{C}} P(\gamma) R_{|\gamma} \, \mathrm{d}^2\gamma \ , \tag{4.2.6}$$

with $R_{|\gamma} = I(\alpha, \beta|\gamma) - \chi(E|\gamma)$ from the standard Devetak-Winter bound [109] and where $P(\gamma)$ is the probability distribution of the relay outcomes.

We now wish to show that $\hat{U}$ can not be chosen in such a way as to compromise the security of the protocol. To do this, consider the probability distribution $P(\alpha, \beta, \gamma) = P(\alpha, \beta|\gamma)P(\gamma)$ of the measurement outcomes, available to Alice and Bob from observation. Given this probability distribution it is possible for Alice and Bob to infer an optimal joint attack on their links and for them to infer the state $\hat{\rho}_{ab|\gamma}$ that results from this. Since $\hat{\rho}_{ab|\gamma}$ can be inferred in this way and $P(\gamma)$ is known, the rate R is completely determined. Consequently, as long as we change $\hat{U}$ in such a way that $P(\alpha, \beta, \gamma)$ stays the same, the rate is unchanged. We consider the unitary operator representing Bell detection, which naturally fulfils the identity $\mathbb{I} = \hat{U}^{\dagger}_{\text{Bell}}\hat{U}_{\text{Bell}}$. We may use this unitary to change Eve's homodyne detections into a Bell detection, as we originally intended the relay to do. This is done by changing our arbitrary unitary $\hat{U}$ such that $\hat{U} = \hat{U}\hat{U}^{\dagger}_{\text{Bell}}\hat{U}_{\text{Bell}}$, and define a new arbitrary unitary $\hat{U}' = \hat{U}\hat{U}^{\dagger}_{\text{Bell}}$.

From this argument we see that there is no difference between a properly working relay performing Bell detection, with Eve performing a joint attack on the links described by the unitary $\hat{U}'$, and Eve appropriating the relay and performing homodyne detections directly. One may be changed into the other without changing the observed probability distribution, and consequently without affecting the secret key rate. We may therefore consider the relay as performing as intended and focus on the possible attacks on the links. This is the power of measurement device independence. We now recall, from Section 2.13, that Gaussian attacks on Gaussian protocols are optimal [81], because they maximize Eve's information gain. We may therefore construct an upper bound on Eve's information gain if we assume that her attack on the relay links is of a Gaussian nature, since the Gaussian states permit the use of the covariance matrix framework

Consider the post-relay covariance matrix, $\mathbf{\Gamma}_{ab|\gamma}$, which may acquired from Equation (4.2.1) through the proper symplectic operations which will be elaborated on later. This state is invariant to changes in γ [140]. However, $I_{AB|\gamma}$ and $\chi_{E|\gamma}$ are determined solely by $\mathbf{\Gamma}_{ab|\gamma}$ so we may write,

$$I(AB|\gamma) = I(A:B) \qquad , \qquad \chi(E|\gamma) = \chi(E) \ . \tag{4.2.7}$$

It then immediately follows that,

$$R = R_{|\gamma} = I(A:B) - \chi(E) \ , \tag{4.2.8}$$

where we have assumed an ideal post processing efficiency, as this does not change any of our further results substantially. From this, the rate is determined only by $\mathbf{\Gamma}_{ab|\gamma}$, which is not surprising since we know that there exists an equivalence between $\hat{\rho}_{ab|\gamma}$ and $\mathbf{\Gamma}_{ab|\gamma}$ when the states are Gaussian.

We now consider a particular attack, namely a two-mode version of the entangling cloner attack [71, 141, 97]. This attack is illustrated in Figure 4.3. Consider a beam splitter in each link, with transmissions T_A and T_B respectively. Eve controls a number

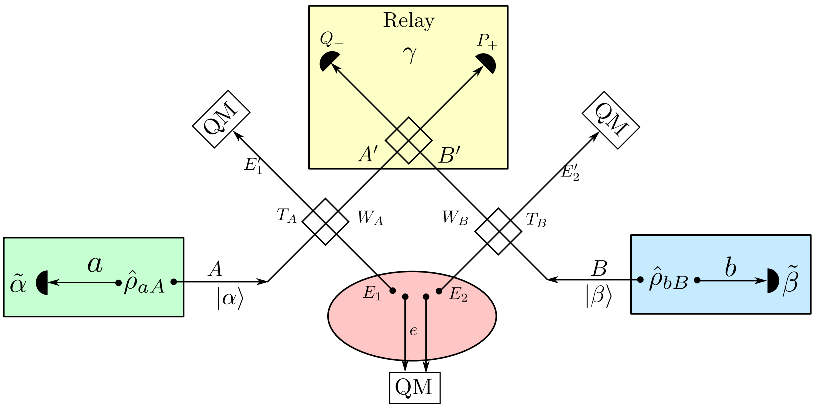


Figure 4.3: An illustration of the generalized entangling cloner attack. The user output modes towards the relay, A and B, are interfered on two beam splitters with two auxiliary modes, E_1 and E_2, controlled by the eavesdropper. The beam splitters have the ratios T_A and T_B, and the ancillary modes introduce excess noise contributions of W_A and W_B in the respective modes. The eavesdropper ancillary modes are part of a larger reservoir E_1, $\mathbf{e}$, E_2, which defines an overall pure Gaussian state. Eve's output modes of this attack, E_1' and E_2', are stored in quantum memories that are collectively measured once the state transfer stage of the protocol terminates.

of auxiliary modes, and in particular she has two modes, E_1 and E_2, which are injected into the links via the beam splitters. The modes E_1 and E_2 have the general covariance matrix,

$$\mathbf{\Gamma}_{E_1E_2} = \begin{bmatrix} W_A & 0 & g & 0 \\ 0 & W_A & 0 & g' \\ g & 0 & W_B & 0 \\ 0 & g\prime & 0 & W_B \end{bmatrix} . \tag{4.2.9}$$

We see that for each link W_A or W_B of thermal noise is injected, and these noise injections are correlated with each other according to the coefficients g and g'. How well correlated the modes are allowed to be is determined by the Heisenberg inequality from Equation (2.7.3). The global covariance matrix is then,

$$\mathbf{\Gamma}_{aAbBE_1E_2} = \mathbf{\Gamma}_{aAbB} \otimes \mathbf{\Gamma}_{E_1E_2} , \tag{4.2.10}$$

where $\mathbf{\Gamma}_{aAbB}$ is defined in Equation (4.2.1). After applying the beam splitter transformations of transmissions T_A and T_B with a subsequent reordering of the modes we obtain,

$$\mathbf{\Gamma}_{aA'bE_1'E_2'B'} = \begin{bmatrix} \mathbf{\Gamma}_{ab} & \boldsymbol{C}_{abA'E_1'} & \boldsymbol{C}_{abE_2'B'} \\ \boldsymbol{C}^T_{abA'E_1'} & \mathbf{\Gamma}_{A'E_1'} & \boldsymbol{C}_{A'E_1'E_2'B'} \\ \boldsymbol{C}^T_{abE_2'B'} & \boldsymbol{C}^T_{A'E_1'E_2'B'} & \mathbf{\Gamma}_{E_2'B'} \end{bmatrix} , \tag{4.2.11}$$

where we have the diagonal submatrices,

$$\boldsymbol{\Gamma}_{ab} = \mu(\mathbb{I}_2 \otimes \mathbb{I}_2) \ , \tag{4.2.12}$$

$$\boldsymbol{\Gamma}_{A'E'_1} = \begin{bmatrix} x_A\mathbb{I}_2 & x''_A\mathbb{I}_2 \\ x''_A\mathbb{I}_2 & x'_A\mathbb{I}_2 \end{bmatrix} \ , \tag{4.2.13}$$

$$\boldsymbol{\Gamma}_{E'_2B'} = \begin{bmatrix} x'_B\mathbb{I}_2 & x''_B\mathbb{I}_2 \\ x''_B\mathbb{I}_2 & x_B\mathbb{I}_2 \end{bmatrix} \ , \tag{4.2.14}$$

with

$$x_k = T_k\mu + (1 - T_k)W_k \ , \tag{4.2.15}$$

$$x'_k = T_kW_k + (1 - T_k)\mu \ , \tag{4.2.16}$$

$$x''_k = \sqrt{T_k(1 - T_k)}(W_k - \mu) \ . \tag{4.2.17}$$

The off-diagonal submatrices, which contain the correlations are given by,

$$\boldsymbol{C}_{abA'E'_1} = \begin{bmatrix} \sqrt{\tilde{\varphi}T_A}\boldsymbol{Z} & -\sqrt{\tilde{\mu}(1 - T_A)}\boldsymbol{Z} \\ \mathbf{0}_2 & \mathbf{0}_2 \end{bmatrix} \ , \tag{4.2.18}$$

$$\boldsymbol{C}_{abE'_2B'} = \begin{bmatrix} \mathbf{0}_2 & \mathbf{0}_2 \\ -\sqrt{\tilde{\varphi}(1 - T_B)}\boldsymbol{Z} & \sqrt{\tilde{\mu}T_B}\boldsymbol{Z} \end{bmatrix} \ , \tag{4.2.19}$$

$$\boldsymbol{C}_{A'E'_1E'_2B'} = \begin{bmatrix} \sqrt{(1 - T_A)T_B}\boldsymbol{G} & \sqrt{(1 - T_A)(1 - T_B)}\boldsymbol{G} \\ \sqrt{T_AT_B}\boldsymbol{G} & \sqrt{(1 - T_B)T_A}\boldsymbol{G} \end{bmatrix} \ , \tag{4.2.20}$$

with,

$$\boldsymbol{G} = \begin{bmatrix} g & 0 \\ 0 & g' \end{bmatrix} \ . \tag{4.2.21}$$

However, since we know that Eve can purify the conditioning modes, we are not interested in Eve's ancilla modes. We therefore truncate the global covariance matrix to get

$$\boldsymbol{\Gamma}_{abA'B'} = \begin{bmatrix} \mu\mathbb{I}_4 & \boldsymbol{C}_{abA'} & \boldsymbol{C}_{abB'} \\ \boldsymbol{C}^T_{abA'} & \boldsymbol{\Gamma}_{A'} & \boldsymbol{C}_{A'B'} \\ \boldsymbol{C}^T_{abB'} & \boldsymbol{C}^T_{A'B'} & \boldsymbol{\Gamma}_{B'} \end{bmatrix} \ , \tag{4.2.22}$$

where we have the blocks

$$\boldsymbol{\Gamma}_{A'} = x_A\mathbb{I}_2 \qquad , \qquad \boldsymbol{\Gamma}_{B'} = x_B\mathbb{I}_2 \ , \tag{4.2.23}$$

and the correlations

$$\boldsymbol{C}_{abA'} = \begin{bmatrix} \sqrt{\tilde{\mu}T_A}\boldsymbol{Z} \\ \mathbf{0}_2 \end{bmatrix} \qquad , \qquad \boldsymbol{C}_{abB'} = \begin{bmatrix} \mathbf{0}_2 \\ \sqrt{\tilde{\mu}T_B}\boldsymbol{Z} \end{bmatrix} \ , \tag{4.2.24}$$

$$\boldsymbol{C}_{A'B'} = \sqrt{(1-T_A)(1-T_B)}\boldsymbol{G} \ . \tag{4.2.25}$$

To obtain the conditional covariance matrix $\boldsymbol{\Gamma}_{ab|\gamma}$, we need to condition $\boldsymbol{\Gamma}_{abA'B'}$ on the Bell detection performed by the relay. We do this according to the recipe given in Section 2.12. We first construct,

$$\boldsymbol{\Theta} = \frac{1}{2}(\boldsymbol{Z}\boldsymbol{\Gamma}_{A'}\boldsymbol{Z} + \boldsymbol{\Gamma}_{B'} - \boldsymbol{Z}\boldsymbol{C}_{A'B'} - \boldsymbol{C}^T_{A'B'}\boldsymbol{Z}) = \frac{1}{2}\begin{bmatrix}\theta & 0 \\ 0 & \theta'\end{bmatrix} \ , \tag{4.2.26}$$

where $\theta = (T_A + T_B)\mu + \lambda$ and $\theta' = (T_A + T_B)\mu + \lambda'$. In addition, $\lambda = \kappa - ug > 0$ and $\lambda' = \kappa + ug' > 0$, with parameters $\kappa = (1-T_A)W_A + (1-T_B)W_B$ and $u = 2\sqrt{(1-T_A)(1-T_B)}$. With this matrix defined, we apply Equation (2.12.4) to get,

$$\boldsymbol{\Gamma}_{ab|\gamma} = \mu\mathbb{I}_4 - (\mu^2 - 1) \times \begin{bmatrix} \frac{T_A}{\theta} & 0 & -\frac{\sqrt{T_A T_B}}{\theta} & 0 \\ 0 & \frac{T_A}{\theta'} & 0 & -\frac{\sqrt{T_A T_B}}{\theta'} \\ -\frac{\sqrt{T_A T_B}}{\theta} & 0 & \frac{T_B}{\theta} & 0 \\ 0 & -\frac{\sqrt{T_A T_B}}{\theta'} & 0 & \frac{T_B}{\theta'} \end{bmatrix} \ . \tag{4.2.27}$$

For two mode states we may express the symplectic spectrum in terms of the determinants of the sub blocks of the covariance matrix, also called the symplectic invariants [90]. Using this, in conjunction with the definition of Equation (2.13.13), we can conveniently express the mutual information as,

$$I(A:B) = \frac{1}{2}\log_2\left(\frac{1 + \det\boldsymbol{\Gamma}_{b|\gamma} + \mathrm{Tr}\boldsymbol{\Gamma}_{b|\gamma}}{1 + \det\boldsymbol{\Gamma}_{b|\gamma\tilde{\alpha}} + \mathrm{Tr}\boldsymbol{\Gamma}_{b|\gamma\tilde{\alpha}}}\right) \ . \tag{4.2.28}$$

The Holevo bound is again expressed through the von Neumann entropies,

$$\chi(E) = S(\hat{\rho}_{ab|\gamma}) - S(\hat{\rho}_{b|\gamma\tilde{\alpha}}) \ . \tag{4.2.29}$$

Calculating the symplectic spectrum in the case of ideal EPR states with $\mu \gg 1$ we may write,

$$\chi(E) = S(\nu_{ab|\gamma,1}) + S(\nu_{ab|\gamma,2}) - S\left(\sqrt{\det\boldsymbol{\Gamma}_{b|\gamma\tilde{\alpha}}}\right) \ . \tag{4.2.30}$$

In the ideal EPR state limit and for $T_A \neq T_B$, the symplectic eigenvalues of the state $\hat{\rho}_{ab|\gamma}$ are given by the expressions,

$$\nu_{ab|\gamma,1} = \frac{|T_A - T_B|}{T_A + T_B}\mu \qquad , \qquad \nu_{ab|\gamma,2} = \frac{\lambda\lambda'}{|T_A - T_B|} \ . \tag{4.2.31}$$

For the particular case where $T_A = T_B$ the symplectic eigenvalues are,

$$\nu_{ab|\gamma,1} = \sqrt{\frac{\lambda\mu}{2T_B}} \qquad , \qquad \nu_{ab|\gamma,2} = \sqrt{\frac{\lambda'\mu}{2T_B}} \ . \tag{4.2.32}$$

Combining these expressions with Equation (4.2.8) we arrive at the secure key rate,

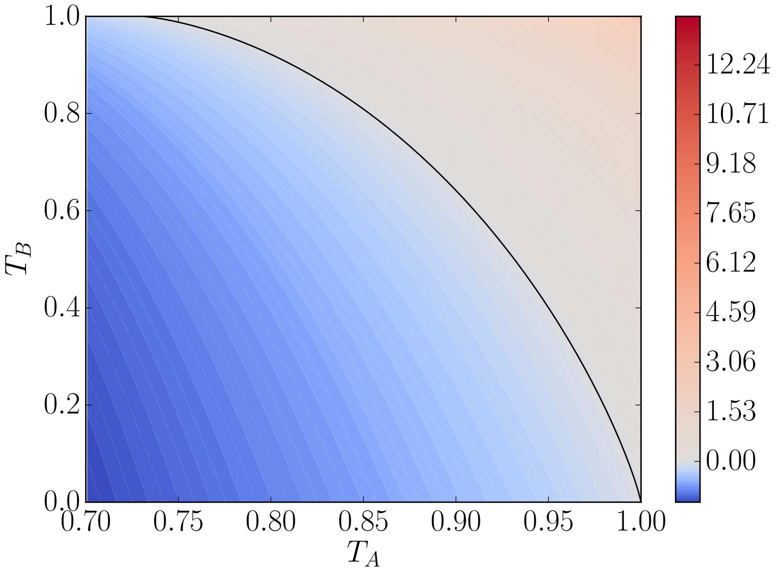


Figure 4.4: Security region for the MDI protocol in terms of the two transmissions in the joint quantum channel. The solid black line indicates where the secure key rate is exactly zero. From this plot it is clear that an asymmetric configuration is preferred with Alice being much closer to the relay. This plot has zero excess noise, such that the joint quantum channel is characterized purely by the transmissions T_A and T_B.

$$\begin{aligned} R(T_A, T_B, \epsilon) = \log_2 \left(\frac{2(T_A + T_B)}{e|T_A - T_B|\varepsilon} \right) + g\left(\frac{T_A \varepsilon}{T_A + T_B} - 1 \right) \\ - g\left(\frac{T_A T_B \varepsilon - (T_A + T_B)^2}{|T_A - T_B|(T_A + T_B)} \right) \,, \end{aligned} \tag{4.2.33}$$

with $\varepsilon = \frac{2(T_A+T_B)}{T_A T_B} + \epsilon$, and $g(x)$ is the bosonic information function given in Equation (2.14.21). ε quantifies the protocol noise, and separates it into a term caused by the introduction of quantum shot noise, and a term of size ϵ introduced by the eavesdropper, which we refer to as the excess noise. Further, the correlation parameters are chosen such that $g = -g'$, which turns out to be the worst case scenario for the correlations in the injected noise. This also confirms the intuition that a joint attack on the links is superior to two separate entangling cloner attacks, where Eve prepares two independent EPR states and injects a mode from each into the links [71].

We investigate the secure region of the protocol by plotting the rate against T_A and T_B in Figure 4.4. Any location in this transmission plane where $R > 0$ is deemed secure. The preference for transmission asymmetry is very apparent from this plot, and we will focus our experimental investigation on the scenario where Alice is in close proximity to the relay and the distance between Bob and the relay is varied.

Experiment

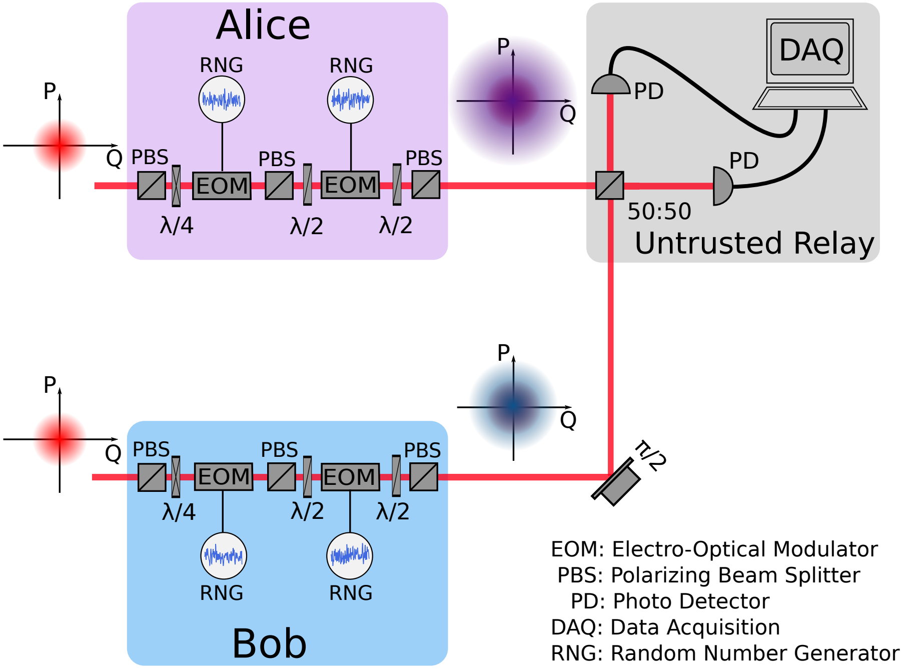


Figure 4.5: Experimental setup for the MDIQKD experiment. Alice and Bob have bright separate carrier beams with shot-noise limited sidebands at 10.5 MHz. The brightness of the carrier serves as the local oscillator. These sidebands are modulated by independent amplitude and phase modulators controlled by random number generators. From run to run, the net effect of this is to displace both input vacuum states into random displaced states picked from a 2D Gaussian distribution that determines the size of the continuous alphabet. Attenuation from the channel is simulated by a reduction of Bob's modulation depth. The displaced states are mixed on a balanced 50/50 beamsplitter and the outputs of this interference are detected by two separate photodiodes. The photocurrents are filtered, digitized and suitably processed to infer the rate of secret key generation. EOM: Electro-optical modulator, PD: Photodiode, PBS: Polarizing beam splitter, DAQ: Data acquisition, RNG: Random number generator.

The experimental setup implemented a prepare-and-measure version of the entanglement based scheme described above. See Figure 4.5 for a sketch of the experiment. A 1064 nm laser beam was split into two equal parts. Each path had a phase modulator and an amplitude modulator, which had their modulations orthogonalized according to the procedure outlined in Section 3.3. These modulators were driven by independent Gaussian noise sources, that were white within the measurement bandwidth of 100 kHz. As explained in Section 3.3, the polarization was kept pure to minimize the cross quadrature correlations. The outputs from the noise generators were also recorded such that the initial modulation could later be correlated with the relay measurements in the post-processing.

The beams were interfered on a balanced 50/50 beam splitter, with about 99 % visibility in order to realize the Bell detection of the relay. The relative phase of the beams was controlled by a piezo mounted mirror. The mirror position was actively adjusted through a servo controller to equalize the power in the beam splitter output ports. These outputs went directly to two high efficiency photo detectors. Locking the mirror position was enabled by the zero crossing of the subtracted carrier power measurements from these detectors, as explained in Section 3.7.1.

The AC outputs of the photo detectors were downmixed from 10.5 MHz. By locking the relative phase in the manner described, subtraction of these outputs allowed us to measure the phase quadrature, while adding the photocurrents gave us the amplitude quadrature. This is the simplified Bell detection scheme described in Section 3.7.2, which is possible because the carrier beam is bright and shot noise limited [142].

Before being digitized, the signals went through a 100 kHz lowpass filter which set the measurement bandwidth. The digitization had a sampling rate of 500 kHz and 14 bit resolution, to enable the proper suppression and avoid aliasing. The effective transmission was varied, not by using a beamsplitter and waveplate combination, but by reducing the effective modulation for the corresponding party. This reduction in modulation is completely equivalent to reducing the carrier power, but this approach was more convenient from an experimental point of view to avoid changing the shot-noise level.

From the data we were able to infer the classical covariance matrix, which contains the modes involved in the practical implementation. We label this matrix as $\mathbf{\Gamma}(Q_A, P_A, Q_B, P_B, X_{-r}, X_{+r})$. Here Q_A ,P_A, Q_B, and P_B are the random variables with Gaussian distributions that Alice and Bob selected their coherent states from. We condition this matrix on the relay outcomes X_{-r} and X_{+r}, which are themselves random variables of Gaussian distributions, to obtain the conditional covariance matrix $\Gamma_{\text{cond}} = \mathbf{\Gamma}(Q_A, P_A, Q_B, P_B|\gamma_r)$. r is a balancing parameter that is not unity due to a mismatch of photo detector gains. This parameter is selected to optimize the rate, in order to simulate a perfectly working relay. As argued from the security proof, we may always assume a perfectly working relay and so this rate maximization is justified.

Neither of these matrices that result from the initial reconstruction make any reference to the entanglement based model. However, it can be shown that the reconstructed conditional matrix is related to the entanglement based covariance matrix by the transformation,

$$\mathbf{\Gamma}_{ab|\gamma_r} = \eta^2 \mathbf{\Gamma}_{\text{cond}} - \mathbb{I}_4 \ , \tag{4.3.1}$$

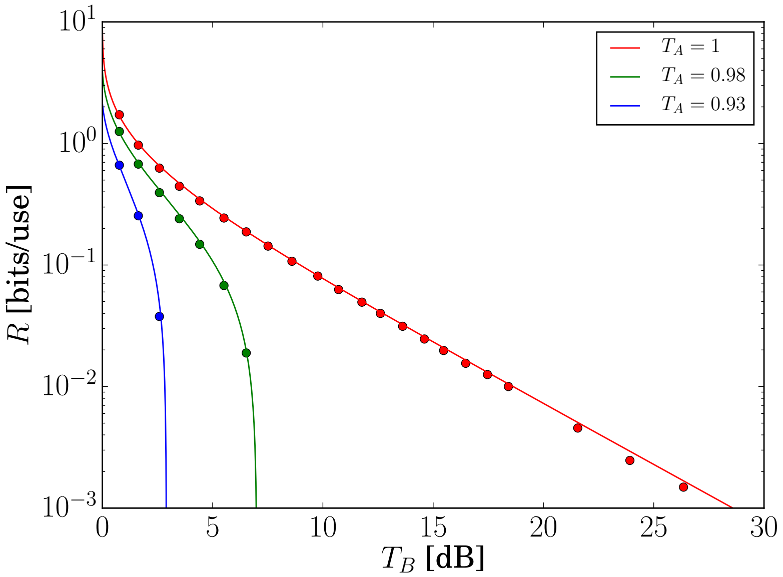


Figure 4.6: The rate of secret key generation R in terms of Bob's transmission loss in dB for $T_A = 0.98$ and $T_A = 0.93$, and $\beta = 1$. The theoretical rate under the coherent Gaussian attack with fitted excess noise is plotted as the solid line, with $\varepsilon = 0.0014$ for $T_A = 0.98$ and $\varepsilon = 0.0055$ for $T_A = 0.93$.

with the rescaling parameter,

$$\eta = \sqrt{(\mu + 1)(\mu^2 - 1)}^{-1} \,. \tag{4.3.2}$$

From this covariance matrix one may calculate a bound on the rate, by following the standard procedure of determining the mutual information and the Holevo bound through the symplectic spectrum.

The results are shown in Figure 4.6, where the secret key rate is calculated in bits per channel use, which is the number of secret bits Alice and Bob share for each coherent state they put into the channel. The plot shows the inferred secret key rate bound for three different values of transmission from Alice to the relay. As predicted in Section 4.2 we see that there is a strong asymmetry in the protocol, which favours Alice being in close proximity to the relay, and the closer she is the farther away Bob is allowed to be. The theory lines corresponding to the points inferred from the reconstructed covariance matrices are calculated using the estimated channel parameters and the use of Equation 4.2.8.

Concluding remarks

In conclusion this project demonstrated the first implementation of measurement device independent quantum key distribution in continuous variables. This result is surprising in the sense that the honest parties can connect to a completely compromised untrusted relay and still maintain security.

While the present experimental implementation was done in free space, an obvious, and indeed necessary, extension is to perform the entire experiment in optical fiber, preferably at a telecom wavelength like 1550 nm. The challenge there is firstly to show that it is indeed possible to implement an efficient relay, where both the interference and the balancing of the relay can be implemented with tolerable accuracy. Secondly, it would be ideal to perform an in-field implementation with separate laser sources to show that synchronization of the sources is feasible without reducing the efficiency of the relay.

Indeed, in the present experimental implementation, Alice and Bob automatically share a local oscillator because their seed beams originate from the same laser source. In an in-field implementation this is not likely to be practical. The local oscillator is thus an obvious entry point for side-channel attacks. Some of these loopholes can be closed by power monitoring [143] and filtering [35]. An additional complication when using separate laser sources is the synchronization between the signal and the local oscillator. These challenges may be surmounted using purely classical techniques such as very precise atom clock synchronization and authenticated classical communication between the parties. In general the issue of side-channel attacks on CVQKD protocols through the local oscillator remains unresolved, though progress is being made [144].

Another exciting prospect is that of increasing the modulation frequency. As mentioned, the equation for the secret key rate calculates how many secret key bits are exchanged per use of the channel, and so by increasing the modulation frequency and corresponding detection rate, the number of channel uses per unit of time will go up, giving a linear increase in the rate. Going to GHz sideband frequencies would therefore allow for very fast key generation.

An interesting perspective for measurement device independent QKD in general is the construction of more conventional network-like structure, such as an efficient star network, where many users connecto to public access points which function like the relays described here. One might also consider the possibility of investigating lower optical frequency carriers, such as the infrared or microwave regime, where shot noise limited sources are difficult to achieve. However, other work indicates that this might indeed not be as detrimental as expected [141, 145, 146]. This might prove useful for more localized network structures in the spirit of wireless internet connections. Our protocol is also a step towards a network repeater structure, where only every other node needs to be trusted, as opposed to a repeater structure constructed from point-to-point protocols.

Non-Markovian Reactivation of Quantum Relays

Introduction

This chapter deals with a special case of the protocol for measurement device independent quantum key distribution with continuous variables. As established in Chapter 4, relays are fundamental devices within information theory, and specifically network information theory. We consider again the typical three party relay configuration, and in particular the following protocols:

1. Entanglement swapping [125, 140, 147, 148]
2. Quantum teleportation [20, 149, 150, 151]
3. Entanglement distillation [126]
4. Quantum key distribution [35]. See also Chapter 4.

Entanglement distillation is known to require non-Gaussian operations [78, 79, 80], and so the details of its implementation are outside the scope of this thesis. However, we shall discuss the idea briefly, as far as our Gaussian framework permits, because distillation relates to the entanglement based model of relay based quantum key distribution. Since we have a well established equivalence between prepare-and-measure QKD and the entanglement model, that we shall elaborate on below, we are able to make statements about entanglement swapping, distillation and teleportation through investigations of prepare-and-measure MDIQKD.

The quantum channels that couple the user to the relay are generally considered to be lossy and noisy. However, the noise is typically assumed to be Markovian in nature. This means that the errors introduced by the noise are independently and identically distributed. This is the assumption of independent and identically distributed outcomes critical to much of classical and quantum information theory, as discussed in Section 2.14. The objective of this work is to investigate the behaviour of quantum relays under non-Markovian noise injection in the relay links, where the quantum information is transferred using continuous variables. Specifically, we consider the effects of correlated Gaussian noise injected into the links. The relay performs the conditioning continuous variable Bell detection described in Section 2.12. Alice and Bob can then implement the previously mentioned protocols, which are all based on the usage of bipartite entanglement, virtual or otherwise.

The relay configuration can be implemented in many different physical systems, for example as quantum chips [152, 153] or superconducting circuits [154]. However, as the quantum systems are scaled down, correlated errors become increasingly likely [155], and in this limit having a model for non-Markovian noise becomes crucial. In larger scale relay configurations, either in free space or in optical fibre, correlated noise and channel memory effects arise naturally, either in high-speed communication [156], from atmospheric turbulence [157, 158, 159] or the diffraction limit [160, 161]. As discussed in Chapter 4, correlated errors can also occur in relay based QKD, when Eve attacks by injecting correlated states into the quantum channels that link Alice and Bob to the relay.

The effect of the injection of this correlated noise is to make the links entanglement breaking [162, 163], such that none of the above protocols can work under Markovian conditions. The noise is then made non-Markovian by increasing the correlations between the injected modes, while keeping them separable. The presence of these correlations can not reactivate bipartite or tripartite entanglement. There is however, a correlation threshold for which quadripartite entanglement does become reactivated, where the four modes involved are the modes sent towards the relay and the modes kept locally by Alice and Bob. The measurement of the relay then conditions this quadripartite entanglement into bipartite entanglement of the remote modes between Alice and Bob, which can then be used for the various protocols.

Indeed, all four protocols can be reactivated, and this reactivation proceeds from swapping and teleportation, to distillation and finally to QKD, in terms of the amount of correlations in the noise. This is experimentally demonstrated by investigating the MDIQKD protocol under this noise injection, as it is the most nested of the four. We shall use this treatment of reactivation of relay based entanglement distribution protocols under thermal noise, as developed by Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri and Samuel Braunstein, to motivate the experimental work of this author and colleagues on an MDIQKD protocol with correlated noise. We therefore devote a large part of this chapter to stating the main results of these theoretical considerations. This work, with theoretical developments and the experimental implementation, was published in pre-print [164].

Theory

To investigate the scenario where thermal noise is injected into the relay links, we go back to the generalized entangling cloner attack on the MDIQKD protocol in Chapter 4. See Figure 5.1. We recall the global covariance matrix before the action

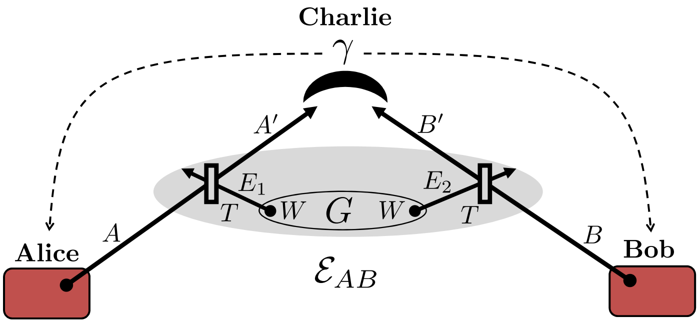


Figure 5.1: Alice and Bob are both in possession of quantum state generation devices that generate Gaussian continuous variable quantum states of some form. These devices send one output each towards Charlie who administers the quantum relay that implements a CV protocol. The relay itself performs a CV Bell detection with the outcome γ, which is broadcast to both users. The links between the users and the relay constitute a joint Gaussian channel called $\mathcal{E}_{AB}$, that may or may not introduce correlations between the links before the relay. This channel is implemented with the use of two beam splitters with the same transmission T for both links. The beam splitters couple modes A and B to two ancillary modes, E_1 and E_2. In addition to the loss introduced by the beam splitters, these modes inject thermal noise with variance W into both links, which is correlated according to $\boldsymbol{G}$. This overall injected state is described by $\hat{\rho}_{E_1E_2}$, which remains separable.

of the channel, where Alice and Bob prepare EPR states and Eve controls the joint quantum channel $\mathcal{E}_{AB}$,

$$\boldsymbol{\Gamma}_{abAE_1E_2B} = \begin{bmatrix} \mu\mathbb{I}_2 & \mathbf{0}_2 & \sqrt{\tilde{\mu}}\boldsymbol{Z} & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & \mu\mathbb{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \sqrt{\tilde{\mu}}\boldsymbol{Z} \\ \sqrt{\tilde{\mu}}\boldsymbol{Z} & \mathbf{0}_2 & \mu\mathbb{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & W\mathbb{I}_2 & \boldsymbol{G} & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{G} & W\mathbb{I}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & \sqrt{\tilde{\mu}}\boldsymbol{Z} & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mu\mathbb{I}_2 \end{bmatrix} . \tag{5.2.1}$$

Again, like in Chapter 4, we consider symmetric inputs such that we have the parameter μ for the variance of the EPR states, and the definition $\tilde{\mu} = \mu^2 - 1$. We maintain the mode labelling convention from Chapter 4, which means that a and b are the EPR state modes kept locally by Alice and Bob respectively and the other modes are shown in Figure 5.1. After the channel with transmissions T_A and T_B we obtain the global state,

$$\boldsymbol{\Gamma}_{aA'bE'_1E'_2B'} = \begin{bmatrix} \boldsymbol{\Gamma}_{ab} & \boldsymbol{C}_{abA'E'_1} & \boldsymbol{C}_{abE'_2B'} \\ \boldsymbol{C}^T_{abA'E'_1} & \boldsymbol{\Gamma}_{A'E'_1} & \boldsymbol{C}_{A'E'_1E'_2B'} \\ \boldsymbol{C}^T_{abE'_2B'} & \boldsymbol{C}^T_{A'E'_1E'_2B'} & \boldsymbol{\Gamma}_{E'_2B'} \end{bmatrix} , \tag{5.2.2}$$

where we have the diagonal submatrices,

$$\mathbf{\Gamma}_{ab} = \mu(\mathbb{I}_2 \otimes \mathbb{I}_2) \ , \tag{5.2.3}$$

$$\mathbf{\Gamma}_{A'E'_1} = \begin{bmatrix} x_A\mathbb{I}_2 & x''_A\mathbb{I}_2 \\ x''_A\mathbb{I}_2 & x'_A\mathbb{I}_2 \end{bmatrix} \ , \tag{5.2.4}$$

$$\mathbf{\Gamma}_{E'_2B'} = \begin{bmatrix} x'_B\mathbb{I}_2 & x''_B\mathbb{I}_2 \\ x''_B\mathbb{I}_2 & x_B\mathbb{I}_2 \end{bmatrix} \ , \tag{5.2.5}$$

with

$$x_k = T_k\mu + (1-T_k)W_k \ , \tag{5.2.6}$$

$$x'_k = T_kW_k + (1-T_k)\mu \ , \tag{5.2.7}$$

$$x''_k = \sqrt{T_k(1-T_k)}(W_k-\mu) \ . \tag{5.2.8}$$

The off-diagonal submatrices, which contain the correlations are given by,

$$\boldsymbol{C}_{abA'E'_1} = \begin{bmatrix} \sqrt{\tilde{\mu}T_A}\boldsymbol{Z} & -\sqrt{\tilde{\mu}(1-T_A)}\boldsymbol{Z} \\ \mathbf{0}_2 & \mathbf{0}_2 \end{bmatrix} \ , \tag{5.2.9}$$

$$\boldsymbol{C}_{abE'_2B'} = \begin{bmatrix} \mathbf{0}_2 & \mathbf{0}_2 \\ -\sqrt{\tilde{\mu}(1-T_B)}\boldsymbol{Z} & \sqrt{\tilde{\mu}T_B}\boldsymbol{Z} \end{bmatrix} \ , \tag{5.2.10}$$

$$\boldsymbol{C}_{A'E'_1E'_2B'} = \begin{bmatrix} \sqrt{(1-T_A)T_B}\boldsymbol{G} & \sqrt{(1-T_A)(1-T_B)}\boldsymbol{G} \\ \sqrt{T_AT_B}\boldsymbol{G} & \sqrt{(1-T_B)T_A}\boldsymbol{G} \end{bmatrix} \ , \tag{5.2.11}$$

with,

$$\boldsymbol{G} = \begin{bmatrix} g & 0 \\ 0 & g' \end{bmatrix} \ . \tag{5.2.12}$$

When $\boldsymbol{G} = \mathbf{0}_2$, that is the injected noise modes are completely uncorrelated, the behaviour of the noise is indeed Markovian and the links can be described as two independent Gaussian lossy and noisy channels [140, 147, 148]. However, when $\boldsymbol{G} \neq \mathbf{0}_2$, the noise is non-Markovian and the links are connected through this noise injection.

For this purpose we are not interested in true entangling cloner attacks, as the examples of correlated noise states mentioned in the introduction still maintain separability. We therefore derive a number of conditions that ensure this. Firstly, we require physicality of the state prepared by the environment, or Eve, such that,

$$\mathbf{\Gamma}_{E_1E_2} + i\mathbf{\Omega}_2 \geq 0, \tag{5.2.13}$$

which is exactly the Heisenberg inequality from Equation (2.7.3). By checking the eigenvalues for the symmetrized global post channel state, where $T_A = T_B = T$, and $W_A = W_B = W$ we arrive at the conditions,

$$|g| < W \quad , \quad |g'| < W \quad , \quad W|g + g'| \leq W^2 + gg' - 1 \ . \tag{5.2.14}$$

Since we also wish to ensure separability of the injected noise, the environment noise modes must also obey the PPT criterion,

$$\tilde{\mathbf{\Gamma}}_{E_1E_2} + i\mathbf{\Omega}_2 \geq 0, \tag{5.2.15}$$

where $\tilde{\mathbf{\Gamma}}_{E_1E_2}$ is the partially transposed of the covariance matrix $\mathbf{\Gamma}_{E_1E_2}$, obtained by the transformation,

$$\tilde{\mathbf{\Gamma}}_{E_1E_2} = \mathbf{\Lambda}_{\text{PPT}}\mathbf{\Gamma}_{E_1E_2}\mathbf{\Lambda}_{\text{PPT}} \ . \tag{5.2.16}$$

In this simple two-mode case of Equation (2.9.3) we have that,

$$\mathbf{\Lambda}_{\text{PPT}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \ . \tag{5.2.17}$$

From the eigenvalues of $\tilde{\mathbf{\Gamma}}_{E_1E_2}$, we arrive at the separability condition [165],

$$W|g - g'| \leq W^2 - gg' - 1 \ . \tag{5.2.18}$$

These conditions limit the values that g and g' may take, such that we have a constrained area in the correlation plane, as seen in Figure 5.2.

With this in mind we wish to investigate the separability of the system described by $\mathbf{\Gamma}_{aA'bB'}$, in other words the system that consists of the modes of the honest parties after the joint quantum channel. We obtain this state by tracing out the modes E_1' and E_2' from the global state $\mathbf{\Gamma}_{aA'bE_1'E_2'B'}$.

For this state there is a threshold beyond which the modes a and A' are no longer entangled. We find this threshold by investigating under which conditions the logarithmic negativity goes to zero. Since we are considering a state of two modes, the logarithmic negativity of the reduced state $\mathbf{\Gamma}_{aA'}$ is determined by the smallest symplectic eigenvalue of the partially transposed state $\tilde{\mathbf{\Gamma}}_{aA'}$ [71]. For an ideal EPR state where $\mu \gg 1$ we find that this eigenvalue is given by,

$$\tilde{\nu}^-_{aA'} = \frac{1+T}{(1-T)W} \ . \tag{5.2.19}$$

The state becomes separable when $\tilde{\nu}^-_{aA'} = 1$, which gives the threshold,

$$W_{EB} = \frac{1+T}{1-T} \ . \tag{5.2.20}$$

If the thermal noise lies beyond this threshold, such that $W > W_{EB}$, and in addition if $\mathbf{G} = \mathbf{0}$, all entanglement between any number of parties is gone [102, 166]. In this

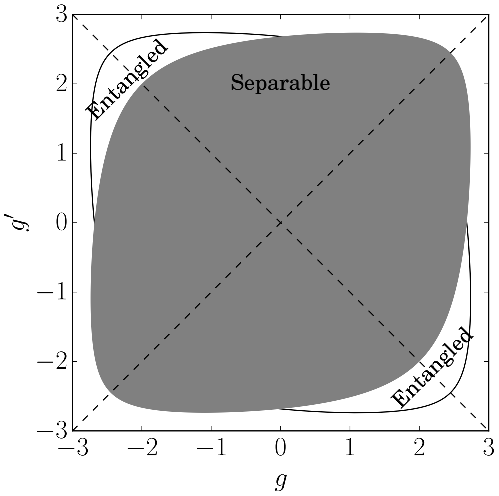


Figure 5.2: Separability of the noise injected by the eavesdropper. In the gray region the thermal noise injected in both relay links forms a separable state, while the two wings bordered by solid black lines have correlations strong enough that the injected noise is entangled. In the white area beyond this, the correlations are so strong as to become unphysical. The injected thermal state is asymmetric such that $W_A = 2$ SNU and $W_B = 5$ SNU.

limit, none of the four protocols described previously will function, because the noise injected into the links degrades the correlations between the parties, such that the EPR states distributed by Alice and Bob are no longer entangled.

Now, if the thermal noise is beyond the threshold and $\mathbf{G} \neq \mathbf{0}$, separable correlations are not strong enough to restore either bipartite or tripartite entanglement. However, there exists a threshold where the separable correlations may reactivate 1×3 quadripartite entanglement [102]. We will in particular be focused on reactivating this type of entanglement between mode a and the set of modes $bA'B'$, which is an example of a $1 \times M$ mode partition described in Section 2.9. See also Figure 5.3.

In what follows we will go through the protocols that can be reactivated and investigate the conditions that allow for this.

Entanglement swapping

We consider the situation where Alice and Bob have two identical EPR states, $\hat{\rho}_{aA}$ and $\hat{\rho}_{bB}$, such that the global state of four modes is $\hat{\rho}_{aA} \otimes \hat{\rho}_{bB}$ and of these four modes a and A belong to Alice and b and B belong to Bob. See Figure 5.4 for an illustration of this configuration.

The idea is now that the parties each keep a and b and send A and B, respectively, to Charlie at the relay, through the relay links that may or may not be correlated as

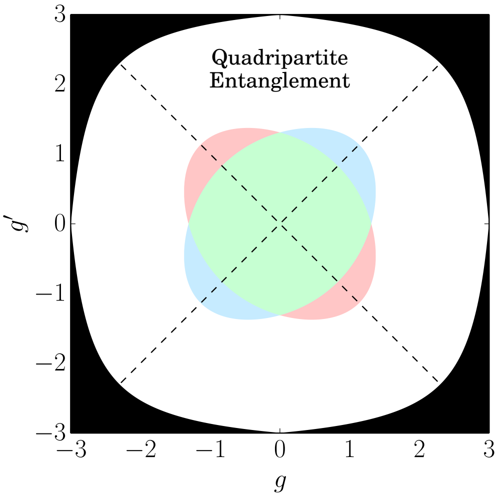


Figure 5.3: Correlation plane for the presence of 1×3 partitioned quadripartite entanglement past the bipartite entanglement breaking threshold $W > W_{EB}$, with $T = 0.5$ and $W = 1.1 \times W_{\mathrm{EB}} = 3.3$. The region with the red shading shows quadripartite entanglement between the mode partitions A' and abB'. The region with the blue shading shows quadripartite entanglement between a and $bA'B'$. The green region has no entanglement for any mode partitions. The white region has entanglement in both mode partitions, and the black region denotes entangled or unphysical noise injection.

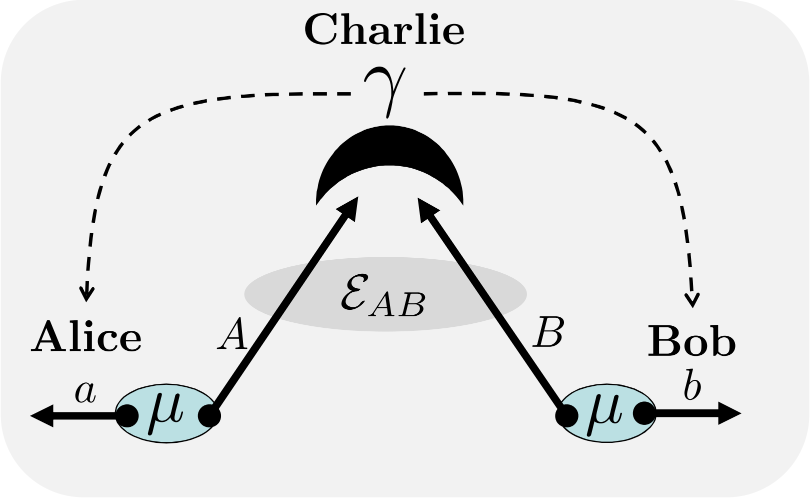


Figure 5.4: Entanglement swapping using a relay based Bell detection. Alice and Bob each have an EPR state of size μ. They send their modes A and B through the joint Gaussian channel $\mathcal{E}_{AB}$. Charlie, acting as the relay, receives these modes, after they have been transformed by the channel. The outcome of the relay measurement γ, is announced publicly. The remote modes, a and b, kept by Alice and Bob will be projected into the state $\hat{\rho}_{ab|\gamma}$ by the conditioning of the relay measurement.

described above. Charlie measures γ, and in announcing this outcome to Alice and Bob, conditions the modes they kept into the Gaussian state $\hat{\rho}_{ab|\gamma}$, with mean-value $\mathbf{x} = \mathbf{x}(\gamma)$ and conditional covariance matrix $\Gamma_{ab|\gamma}$. By applying Equation (2.12.4) to the reduced global state $\mathbf{\Gamma}_{aA'bB'}$ we find that,

$$\mathbf{\Gamma}_{ab|\gamma} = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{C} \\ \boldsymbol{C}^T & \boldsymbol{B} \end{bmatrix} , \tag{5.2.21}$$

and the 2×2 blocks are given by,

$$\boldsymbol{A} = \boldsymbol{B} = \begin{bmatrix} \mu - \frac{\mu^2-1}{2(\mu+\kappa)} & 0 \\ 0 & \mu - \frac{\mu^2-1}{2(\mu+\kappa')} \end{bmatrix} \tag{5.2.22}$$

$$\boldsymbol{C} = \begin{bmatrix} \frac{\mu^2-1}{2(\mu+\kappa)} & 0 \\ 0 & -\frac{\mu^2-1}{2(\mu+\kappa')} \end{bmatrix} . \tag{5.2.23}$$

Rewritten in this way κ and κ' contain all the environmental parameters that are introduced through the beam splitters in the links,

$$\kappa = (T^{-1} - 1)(\omega - g) \qquad , \qquad \kappa' = (T^{-1} - 1)(\omega + g') . \tag{5.2.24}$$

From this conditional state we compute the logarithmic negativity as described in Section 2.9. Since this state has two modes, we may once again express the logarithmic negativity purely in terms of the smallest partially transposed symplectic eigenvalue $\tilde{\nu}^-_{ab|\gamma}$. Using some standard results from the analysis of general Gaussian two-mode states we can show that [90],

$$\tilde{\nu}^-_{ab|\gamma} = \sqrt{\frac{(1+\mu\kappa)(1+\mu\kappa')}{(\mu+\kappa)(\mu+\kappa')}}. \tag{5.2.25}$$

How much entanglement is swapped expressed in terms of the logarithmic negativity $\mathcal{N}$ will naturally depend on μ, and this is optimal in the limit of a maximally entangled EPR state where $\mu \gg 1$. In this limit we find that,

$$\tilde{\nu}^-_{ab|\gamma} \simeq \tilde{\nu}^-_{ab|\gamma,\text{opt}} = \sqrt{\kappa\kappa'} . \tag{5.2.26}$$

We say that the swapping is successful when $\tilde{\nu}^-_{ab|\gamma} < 1$, since this implies non-zero logarithmic negativity between the conditioned local modes of Alice and Bob. For maximally entangled EPR states this leads us to the conclusion that reactivation of entanglement swapping through environmental correlations can only occur when $\kappa\kappa' < 1$.

Quantum teleportation

For this protocol, we view Charlie as a teleporter, transferring a coherent state $|\alpha\rangle$ from Alice to Bob. See Figure 5.5 for a sketch of this scheme. The state Alice wishes to

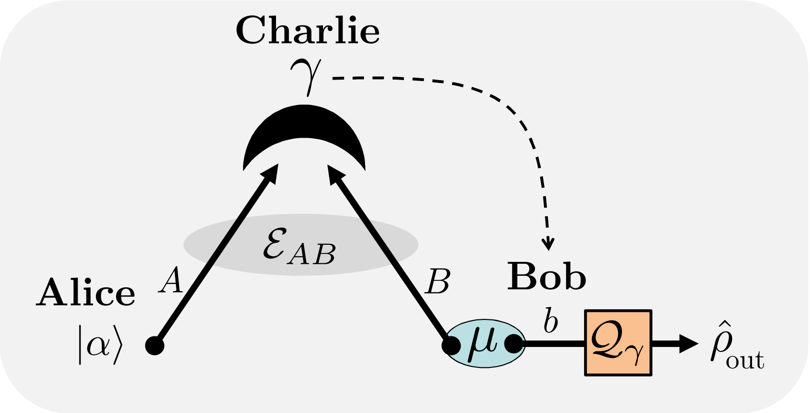


Figure 5.5: Quantum state teleportation using a relay based Bell detection. Bob has an EPR state of size μ, and Alice has a coherent state $|\alpha\rangle$, which she wants to teleport to Bob. Alice forwards this coherent state to Charlie, and Bob sends the mode B to Charlie, while keeping b. Both of the modes sent towards the relay go through the joint Gaussian channel $\mathcal{E}_{AB}$. Charlie performs a Bell detection, and announces γ to Bob. This allows Bob to perform the conditional quantum operation $\hat{\mathcal{Q}}_\gamma$, such that the state $|\alpha\rangle$ is teleported into the output state ρ_{out}, which is in the mode Bob has kept for himself. This allows Bob to recover α with fidelity $\mathcal{F}$.

teleport and one mode of Bob's EPR state are both sent to Charlie through the relay links. Charlie communicates the measurement outcome γ to Bob, who then conditionally prepares his remaining mode [12] to retrieve the teleported state $\hat{\rho}_{\text{out}} \simeq |\alpha\rangle\langle\alpha|$.

If the μ of Bob's EPR state is chosen such that $\mu \gg 1$, we can use the covariance matrix framework to show that the fidelity of this teleportation is given by the optimal fidelity,

$$\mathcal{F} \simeq \mathcal{F}_{\text{opt}} = \sqrt{(1+\kappa)(1+\kappa')}^{-1} \leq (1+\tilde{\nu}^{-}_{ab|\gamma,\text{opt}})^{-1} \ . \tag{5.2.27}$$

We see now that there is a clear connection between the performance of teleportation and swapping, as the efficacy of both protocols can be expressed in terms of the minimal symplectic eigenvalue of the partially transposed matrix. As noted earlier, swapping fails when $\tilde{\nu}^{-}_{ab|\gamma,\text{opt}} \geq 1$, and in this case teleportation is classical, such that the fidelity becomes $\mathcal{F}_{\text{opt}} \leq 1/2$ [71].

Entanglement distillation

We now consider the distillation of entanglement, as illustrated in Figure 5.6. We imagine that Alice and Bob use Charlie to run the swapping protocol N times. After each run they store their entangled modes in quantum memories. At the end of this they will have a set of entanglement swapped states $\hat{\rho}^{\otimes N}_{ab|\gamma}$. The purpose of the distillation is now to perform some operation that takes these N states into a single two-mode state with more entanglement than any of the individual states.

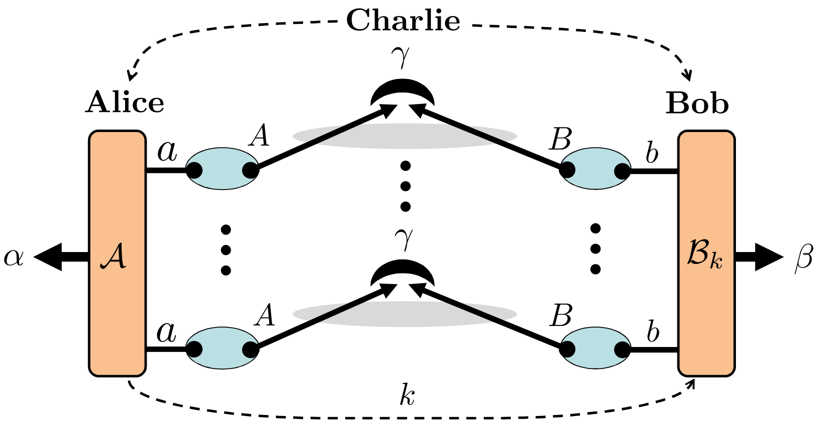


Figure 5.6: Entanglement distillation using relay based Bell detection. After N uses of the entanglement swapping relay protocol, with the outcomes stored in quantum memories, Alice and Bob can now distill their many entangled states into a single state with improved entanglement. Alice performs the collective operation $\hat{\mathcal{A}}$ on the set of modes a. She forwards the classical outcome k of this operation to Bob, allowing him to perform a conditional operation $\hat{\mathcal{B}}_k$ on his set of modes b. This implements optimal one-way distillation, but requires $\hat{\mathcal{B}}_k$ to be non-Gaussian.

To do this, Alice applies a local optimal operator [109] $\hat{\mathcal{A}}$ on her N a modes. The quantum outcome of this operation, $\boldsymbol{\alpha}$, is a distilled system, and the classical measurement outcomes k are broadcast to Bob. When Bob receives k, he performs an operation conditioned on these outcomes, called $\hat{\mathcal{B}}_k$, which will transform his set of b modes into the distilled system $\boldsymbol{\beta}$. The operations $\hat{\mathcal{A}}$ and $\hat{\mathcal{B}}_k$ can not both be Gaussian if distillation is to be achieved [78, 79, 80], and as such they are outside the scope of this thesis.

It is possible to choose these operations such that the distilled system become Bell state pairs [12]. The efficiency of the distillation is determined by how much entanglement is generated per relay use. To quantify the amount of entanglement that results from this is cumbersome, but it is possible to set up a lower bound. This bound is known as the coherent quantum information, and is related to the quantum mutual information defined in Section 2.14 [109, 167, 168]. It further has an analogue in the classical channel capacity, which quantifies how many bits can be transferred per channel use without introducing errors [5]. For a bipartite state it is defined as,

$$I_{\mathcal{C}}(\hat{\rho}_{ab}) = S(\hat{\rho}_b) - S(\hat{\rho}_{ab}) \tag{5.2.28}$$

Because the non-Gaussian operations are local to Alice and Bob, we may postpone their application and simply quantify the coherent quantum information fully in the covariance matrix framework. The von Neumann entropies in Equation (5.2.28) are therefore easily evaluated through the symplectic spectrum of the conditional covariance matrix $\mathbf{\Gamma}_{ab|\gamma}$. When the distributed EPR states are ideal, $\mu \gg 1$, it can be shown that,

$$I_{\mathcal{C}} = -\log_2(e\tilde{\nu}^{-}_{ab|\gamma}) \ , \tag{5.2.29}$$

which relates the performance of the distillation protocol to both teleportation and swapping, since we may conclude that entanglement distillation is possible when $\tilde{\nu}^{-}_{ab|\gamma} < e^{-1} \simeq 0.367$.

Secret key distillation

Lastly, we consider the relay based QKD scheme of Chapter 4. To reiterate, the relay controlled by Charlie is responsible for distributing the correlations between Alice and Bob through the swapping of their entanglement. These correlations are not visible to Charlie, who may also be regarded as Eve. The Gaussian, and possibly correlated, noise in the links is in this case considered to be injected by the eavesdropper. To obtain the key material, Alice and Bob perform an entanglement distillation, where the quantum operation $\hat{\mathcal{A}}$ performed by Alice is a heterodyne measurement with the classical outputs $\boldsymbol{\alpha}$, which constitutes the first stage of the protocol for generating the secret key material. Her measurements also give the results k, which Bob needs for conditioning.

Bob then performs a measurement operation $\hat{\mathcal{B}}_k$ that depends on k, which gives him the output $\boldsymbol{\beta}$, allowing him to estimate the key rate. If we assume that the reconciliation is perfect, the rate R increases monotonically with an increase in μ. The rate further depends solely on μ and the environmental parameters κ and κ'. Ideally, we have that the rate generation from the MDIQKD protocol is lower bounded by the coherent quantum information from the distillation protocol, i.e. $R \geq I_{\mathcal{C}}$. We may symmetrize the expression for the secret key rate from Chapter 4 to obtain,

$$\begin{aligned} R = {} & \frac{1}{2}\log_2\left(\frac{(1+\mu+2\kappa)^2(1+\mu+2\kappa')^2}{16(1+\kappa)(1+\kappa')(\mu+\kappa)(\mu+\kappa')}\right) - g\left(\sqrt{\frac{\mu(1+\mu\kappa)}{\mu+\kappa}}\right) \\ & - g\left(\sqrt{\frac{\mu(1+\mu\kappa')}{\mu+\kappa'}}\right) + g\left(\sqrt{\frac{(1+\mu+2\mu\kappa)(1+\mu+2\mu\kappa')}{(1+\mu+2\kappa)(1+\mu+2\kappa')}}\right) \ . \end{aligned} \tag{5.2.30}$$

If we assume an ideal EPR state generation in the entanglement model we get the simpler expression,

$$R_{\text{opt}} \gtrsim \log_2\left(\frac{\mathcal{F}_{\text{opt}}}{e^2\tilde{\nu}^{-}_{ab|\gamma,\text{opt}}}\right) + g(1+2\tilde{\nu}^{-}_{ab|\gamma,\text{opt}}) \ , \tag{5.2.31}$$

which is written in terms of the minimal PPT symplectic eigenvalue. From this it is apparent that the rate can only be positive when $\tilde{\nu}^{-}_{ab|\gamma,\text{opt}} \lesssim 0.192$. We therefore conclude that our practical QKD protocol is most sensitive to noise out of the four protocols presented here, and thus requires the highest degree of non-Markovian behaviour from the noise to be reactivated. This is also clear from the presentation of the protocols, since we have seen that QKD can be regarded as a stepwise implementation of entanglement swapping and subsequent distillation. Illustrated in Figure 5.7 is the correlation plane, where one can see in which regions the individual protocols activate.

In Figure 5.7 there is a clear asymmetry in the plane which is caused by the chosen Bell detection. The other obvious choice where Charlie projects the state onto the variables $\hat{Q}_+$ and $\hat{P}_-$ would mirror the correlation plane with respect to the origin. We also see that entanglement swapping reactivates well after quadripartite entanglement is reactivated. This indicates that Bell detection might not be optimal for generating the quadripartite entanglement or reactivating these protocols in general. Lastly, one observes that an increase in correlations simply increases protocol performance, and reactivates them in the order previously mentioned.

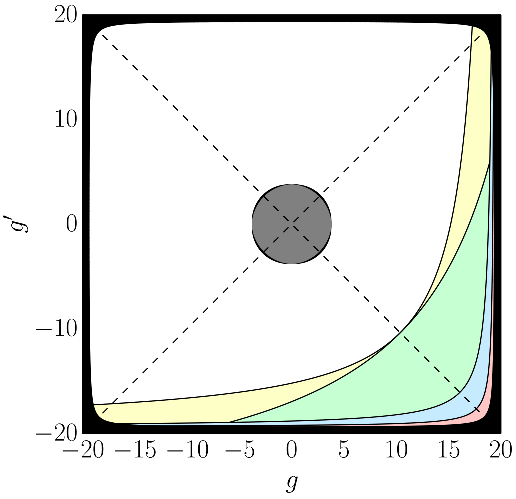


Figure 5.7: Hierarchy of protocol reactivation in terms of correlation parameters. Parameters chosen for this plot are $T = 0.9$, $\omega = 1.02 \times \omega_{\text{EB}} = 19.38$ and ideal EPR states. The values outside the black region correspond to values of g and g' where the thermal noise contains separable correlations. The inner grey region has no entanglement for any number of parties. The white region has symmetric quadripartite entanglement but no protocol reactivation. Entanglement swapping activates in the yellow area and beyond, while teleportation activates in the green area and beyond. The blue area denotes activation of entanglement distillation, while the red region indicates reactivation of the practical QKD scheme.

Correlated additive noise

Of course, entanglement distribution is complicated in practice, and indeed as mentioned before, the distillation itself requires non-Gaussian operations. We therefore wish to consider a closer to classical non-Markovian Gaussian environment. In the following we therefore make use of the equivalence between the prepare-and-measure

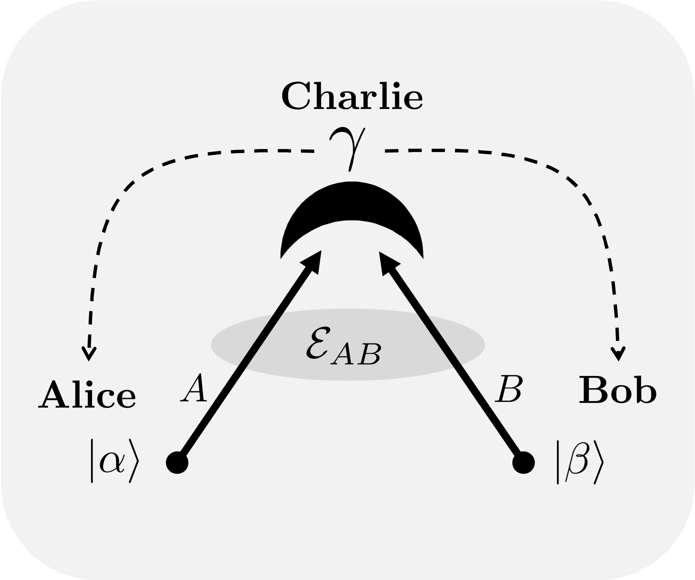


Figure 5.8: Practical QKD using a relay based Bell detection. Alice and Bob prepare coherent states in the modes A and B, chosen from a Gaussian distribution of mean values. These coherent states are sent to Charlie who performs the relay detection. This creates classical correlations between Alice and Bob, which enables the generation of a secret key. As in the standard MDIQKD, Eve could replace Charlie without compromising the security of the relay.

schemes and the entanglement model. To do this, we first discard the idea of storing the swapped states in quantum memories, and instead use heterodyne detections for the conditioning by Alice and Bob. As we have established previously, this is the same as drawing a single coherent state per channel use from a Gaussian distribution of coherent state mean values, with variance $\mu - 1$ for both parties, though of course Alice and Bob must select their states independently of each other. These prepared states are sent through the relay links to Charlie who performs a Bell detection and broadcasts the result $\gamma \simeq \alpha - \beta^*$. See Figure 5.8 for this simplified scheme, also described in Chapter 4.

In the limit where $T \to 1$ and $\omega \to \infty$, we define the constant parameters $n = (1-T)\omega$, $c = g(\omega - 1)^{-1}$ and, $c' = g'(\omega - 1)^{-1}$. The effect of taking this limit is that the modes A and B receive correlated classical noise, such that their quadrature operators transform according to the rule,

$$\left(\hat{Q}_A, \hat{Q}_A, \hat{Q}_B, \hat{Q}_B\right) \to \left(\hat{Q}_A, \hat{Q}_A, \hat{Q}_B, \hat{Q}_B\right) + (\xi_1, \xi_2, \xi_3, \xi_4) \ . \tag{5.2.32}$$

Here, ξ_i is a Gaussian variable of zero mean and is otherwise specified by the classical noise covariance matrix,

$$\mathbf{\Gamma}_{\mathrm{CN}} = n \begin{bmatrix} 1 & 0 & c & 0 \\ 0 & 1 & 0 & c' \\ c & 0 & 1 & 0 \\ 0 & c' & 0 & 1 \end{bmatrix} . \tag{5.2.33}$$

$n \geq 0$ is the variance of the additive noise and the coefficients $-1 \leq c, c' \leq 1$ quantify the correlations in the classical noise. In these parameters the entanglement threshold becomes $n > n_{EB} = 2$. The results for reactivation of the above protocols can be expressed in these new parameters by taking the limits $T \to 1$ and $\omega \to \infty$ in the relevant expressions. The experiment described below will focus on the reactivation of the practical MDIQKD protocol, as it remains the most difficult protocol to reactivate.

Experimental results

To show what one can achieve with non-Markovian effects, we investigate the most nested protocol, i.e. practical relay based QKD with classical additive noise. In particular we investigate the behaviour of the secret key rate $R(\mu, n, c, c')$ in terms of n in the regime where the classical noise is correlated such that $c = c' = 1$ and $\mu = 52$.

The setup for the experiment is depicted in Figure 5.9. Alice and Bob generate random coherent states, chosen from independent Gaussian distributions of the same size. They generate these states by inputting classical Gaussian noise into pairs of electro-optical modulators, that are fed by a common 1064 nm laser source that is split evenly to their stations. This pair of modulators in total realizes the Weyl operator of Equation (2.4.1), since the individual modulations have been orthogonalized according to the procedure described in Section 3.3. The generators which produce the classical Gaussian noise also have their outputs recorded such that they may be correlated with the relay measurements during the post-processing. This allows for a proper estimation of the channel parameters and of the correlations between the parties.

In addition to these signal modulations, these modulators are compromised by a side-channel attack where Eve injects her own classical separable correlated noise into the two pairs of modulators. She does this using two classical noise generators which both have two highly correlated outputs. From run to run, the net effect is that Eve displaces Alice's input state by some unknown amount, and also displaces Bob's input state by the same amount. From this construction we arrive at a correlated-additive Gaussian environment, with $c \simeq 1$ and $c' \simeq 1$ as described above, where n is determined by the amplitude of Eve's side-channel noise generators. On average each mode will therefore contain a thermal state representing the coherent state alphabets of Alice and Bob, respectively, each with an extra contribution to their variance from the side-channel attack of the eavesdropper. The signal modulation is chosen such that it corresponds to $\mu = 52$ SNU, corresponding to around 17 dB of modulation

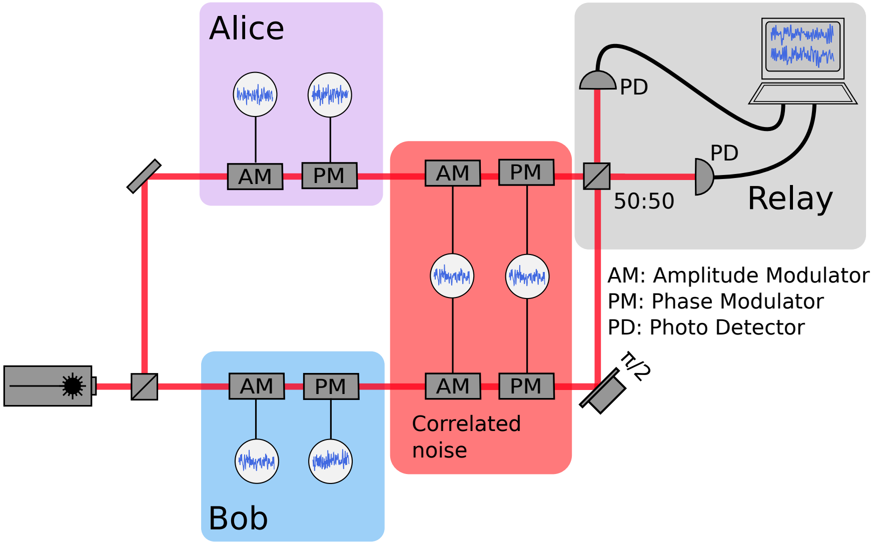


Figure 5.9: Alice and Bob prepare their quadrature symmetric coherent state alphabets on two 2.8 mW laser beams, that originate from the same 1064 nm laser source. The states are generated by pairs of electro-optical modulators fed by classical noise signals from uncorrelated noise generators. In addition to these signals, Eve adds correlated noise in the stations from two noise generators that each have two highly correlated outputs. The noise injected by Eve is thus the same for both stations and is also symmetric in the quadratures. The relay is implemented with a simplified Bell detection that interferes the two inputs beams on a balanced beam splitter, with addition and subtraction of the down-mixed photocurrents in post-processing. The relay has an overall efficiency of 98 %. AM: Amplitude modulator, PM: Phase modulator, PD: Photodetector.

relative to the shot noise, with the variance n added onto this from the side-channel attack.

The prepared states propagate to the relay operated by Eve. The first operation the relay performs is a balanced beam splitter operation that interferes the two input modes. The outputs of this operation are detected by a pair of photo detectors, and the outcome of this determines the parameter γ, completing the conditional Bell detection. As such the relay functions as in Chapter 4 and it implements the simplified version of the Bell detection described in Section 3.7.2. The relay is not perfect and so we attribute $\simeq 2\%$ of loss to it, which may benefit Eve, though the additive noise model does not explicitly account for this loss. Experimentally, the loss primarily comes from the limited visibility of the interference and the quantum efficiency of the photo detectors. These losses are the same as for the MDIQKD implementation described in Chapter 4.

We consider the combined effect of Eve's side-channel attack and the relay loss as a global coherent Gaussian attack, recognizing that this is not the optimal version of

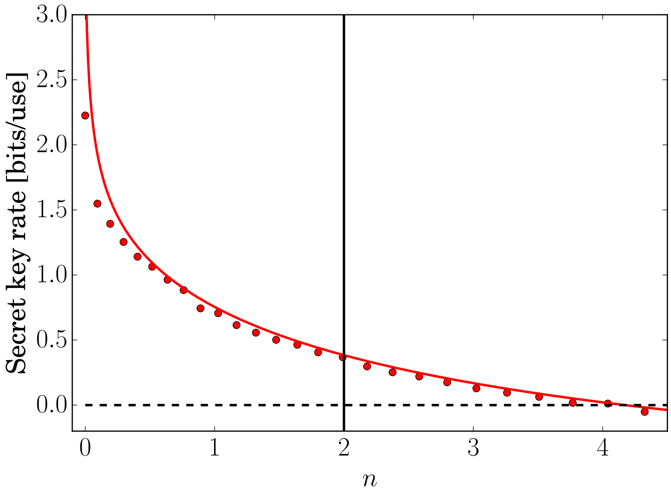


Figure 5.10: The secret key rate, measured in bits per channel use, in terms of the injected correlated noise n. The solid line represents the theoretical estimate of the rate with the noise coefficients $c = c' = 1$ and a signal modulation of $\mu \simeq 52$, while the points refer to the rate calculated from experimental data. We observe a positive secret key rate after the entanglement breaking threshold at $n = 2$, represented by the solid black line. $\beta = 1$ for this calculation. Inefficiencies at the relay directly translate into transmission loss, which the theory line does not account for in the additive noise limit.

the attack that was considered in Chapter 4. In fact the injected noise is correlated in such a way as to be optimal for the secret key rate generation. We compute the secret key rate in a manner similar to for MDIQKD, by first of all inferring the corresponding classical covariance matrix, which is related to the entanglement based version of the protocol, and then assuming that Eve is able to purify the state shared by Alice and Bob. From the generated covariance matrix the von Neumann entropies and the mutual information between Alice and Bob may be calculated, which in turn gives an estimate on the extractable rate.

In Figure 5.10 we plot the calculated secret key rate against the classical additive noise n. The rate decreases with increasing n, and is strictly positive when $2 < n \leq 4$. Beyond this point the links become entanglement breaking, and the rate remains positive due to of the presence of the separable correlations. This behaviour occurs in spite of experimental imperfections, though we do see that the theoretically predicted rate of Equation (5.2.30) is slightly higher than what is observed, as the relay inefficiency is not included in the model. This efficiency mainly arises from the relay detection loss. In spite of this inefficiency we confirm the non-Markovian reactivation of the QKD protocol experimentally.

Concluding remarks

In conclusion, we have shown that the most nested of the four entanglement based protocols in a standard three party relay configuration can be reactivated by non-Markovian effects in the Gaussian noise injected into the links.

In the limit where strong Gaussian noise is injected into the links, one enters a regime where all possible forms of entanglement between the modes are broken. However, if the injected noise is sufficiently correlated, but separable, it reactivates 1×3 quadripartite entanglement, which can then by localized into ordinary bipartite entanglement by the relay measurement. In this bipartite form, Alice and Bob can perform their protocols as normal.

We confirm these results experimentally through a test of the corresponding relay based prepare-and-measure quantum key distribution protocol, where we observe that the secret key rate stays positive past the threshold of virtual entanglement breaking when the injected thermal noise is highly correlated.

These results are interesting from the perspective of investigating non-Markovian dynamics. Indeed, non-Markovian noise may be regarded as a resource that can be exploitable in certain quantum networks. As previously mentioned, it is known that these dynamics occur in both short and long distance architectures, and so these results might be useful within a broad range of systems.

Continuous Variable Quantum Key Distribution with a Noisy Laser

Introduction

This work is based on a theoretical proposal from Weedbrook *et al.* [141, 145], which describes how quantum key distribution with thermal, rather than coherent, states is feasible under certain conditions, provided that direct reconciliation is applied. A similar result exists for reverse reconciliation [169], where it was demonstrated that a certain amount of detection noise benefits the honest parties.

The prediction made in [145] is then that preparation noise is detrimental to security, even if it is trusted, if reverse reconciliation is used. However, if direct reconciliation is used instead, security can be established in a parameter range where reverse reconciliation does not allow it. Consequently, a direct reconciliation scheme is more vulnerable to detection noise, and so relaxing the requirements on the source ensures that the detection has to be shot noise limited.

The implication is that shot noise limited continuous variable sources are not strictly required to achieve quantum security. Relaxing this requirement of a shot noise limited source could lead to cheaper short range continuous variable quantum key distribution implementations. This is particularly relevant because conventional optical telecom equipment is typically not able to resolve the quantum nature of light, since this is not a requirement for classical communication. This work was published in [170].

Theory

We first restate the main result of Weedbrook *et al.* [141, 145]. Consider the case where Alice prepares a noisy EPR state,

$$\mathbf{\Gamma}_{\text{in}} = \begin{bmatrix} \mu\mathbb{I}_2 & \sqrt{\mu^2-1}\boldsymbol{Z} \\ \sqrt{\mu^2-1}\boldsymbol{Z} & (\mu+\kappa)\mathbb{I}_2 \end{bmatrix} . \tag{6.2.1}$$

This EPR state has extra uncorrelated noise in the mode that is to be transmitted, which signifies the preparation noise. In a prepare-and-measure protocol this noise is equivalent to the noise on the displaced states, which can be seen rather easily by performing a measurement conditioning the noisy mode on the outcome of Alice's local mode. In a pure EPR state this would yield the identity matrix as the covariance matrix, in units of shot noise, while for this noisy state it would scale the identity by κ. When $\kappa = 0$ we recover the usual EPR state prepared by Alice. However, this additional noise will make sure that the global state is not pure, which naturally prohibits the use of the self-duality properties of the von Neumann entropy. We therefore do not have access to identities of the form $S(E) = S(AB)$ with this input state.

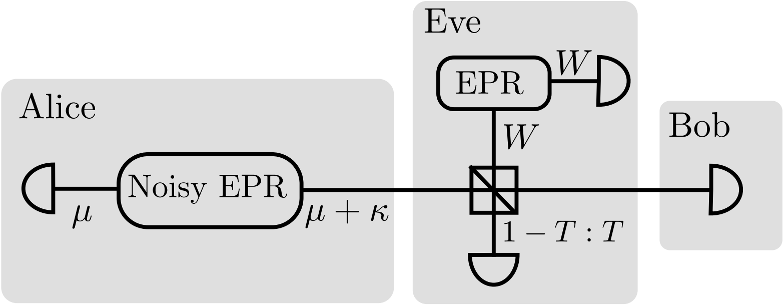


Figure 6.1: Entanglement based model, information theoretically equivalent to the prepare-and-measure scheme. Alice prepares an EPR state, where the outgoing mode has an additional κ of noise. Eve controls the quantum channel where she implements an entangling cloner attack, with loss $1 - T$ and noise W.

We now wish to investigate the effects of this preparation noise in the event of an entangling cloner attack, to see how the parameters influence each other. See Figure 6.1 for an overview of the modes involved. To implement this particular attack, the eavesdropper prepares a pure EPR state for her entangling cloner.

$$\mathbf{\Gamma}_{\boldsymbol{E}} = \begin{bmatrix} W\mathbb{I}_2 & \sqrt{W^2-1}\boldsymbol{Z} \\ \sqrt{W^2-1}\boldsymbol{Z} & W\mathbb{I}_2 \end{bmatrix} . \tag{6.2.2}$$

Letting these two EPR states interact through a beam splitter with a transmission T yields a global covariance matrix,

$$\mathbf{\Gamma}_{ABE} = \begin{bmatrix} \mu\mathbb{I}_2 & \sqrt{T\tilde{\mu}}\boldsymbol{Z} & -\sqrt{\tilde{T}\tilde{\mu}}\boldsymbol{Z} & \mathbf{0}_2 \\ \sqrt{T\tilde{\mu}}\boldsymbol{Z} & (T\mu_\kappa + \tilde{T}W)\mathbb{I}_2 & \sqrt{T\tilde{T}}(W-\mu_\kappa)\mathbb{I}_2 & \sqrt{\tilde{T}\tilde{W}}\boldsymbol{Z} \\ -\sqrt{\tilde{T}\tilde{\mu}}\boldsymbol{Z} & \sqrt{T\tilde{T}}(W-\mu_\kappa)\mathbb{I}_2 & (\tilde{T}\mu_\kappa + TW)\mathbb{I}_2 & \sqrt{T\tilde{W}}\boldsymbol{Z} \\ \mathbf{0}_2 & \sqrt{\tilde{T}\tilde{W}}\boldsymbol{Z} & \sqrt{T\tilde{W}}\boldsymbol{Z} & W\mathbb{I}_2 \end{bmatrix} , \tag{6.2.3}$$

with the renamed parameters $\tilde{T} = 1 - T$, $\tilde{\mu} = \mu^2 - 1$, $\mu_\kappa = \mu + \kappa$, and $\tilde{W} = W^2 - 1$, and we have the corresponding prepare-and-measure parameter $V_{\text{sig}} = \mu - 1$ for the size of the continuous alphabet. This matrix completely characterizes the global state of the system. To determine the mutual information between the honest parties, we use the definition of mutual information via the Shannon entropy as given in Equation (2.13.13) to obtain, in the case of heterodyne detection,

$$I(A:B) = \log_2 \left(\frac{(1-T)W + T(\mu+\kappa) + 1}{(1-T)W + T(1+\kappa) + 1} \right) . \tag{6.2.4}$$

We calculate the Holevo bound from Equation (2.14.32), without the use of purification identities. We therefore have,

$$\chi(E:B) = S(E) - S(E|B) , \tag{6.2.5}$$

for reverse reconciliation and,

$$\chi(E:A) = S(E) - S(E|A) , \tag{6.2.6}$$

for direct reconciliation. We recover the results of [141] and [145] through the use of symplectic invariants [90], and so we have the expression,

$$\chi(E:X) = g(\nu_{E+}) + g(\nu_{E-}) - g(\nu_{E|X+}) - g(\nu_{E|X-}) , \tag{6.2.7}$$

where X may be either A for Alice or B for Bob, depending on the method of reconciliation. The symplectic eigenvalues are given by,

$$\nu_{E\pm} = \frac{1}{2} \left(\sqrt{(e_V + W)^2 - 4T(W^2-1)} \pm (e_V - W) \right) , \tag{6.2.8}$$

and the parameter $e_V = (1-T)V + TW$, with $V = \mu + \kappa + 1$. Additionally, we have the conditional symplectic eigenvalues for reverse reconciliation,

$$\nu_{E|B\pm} = \frac{1}{2} \left(\sqrt{\sigma_T} \pm (\sigma_1 - \sigma_2) \right) , \tag{6.2.9}$$

expressed through the symplectic invariants,

$$\sigma_1 = \frac{(1-T)V + W(T+V)}{1 + TV + (1-T)W} , \tag{6.2.10}$$

$$\sigma_2 = \frac{1 - T + W(1+TV)}{1 + TV + (1-T)W} , \tag{6.2.11}$$

$$\sigma_3 = \sqrt{W^2-1} \left(\frac{1+V}{1 + TV + W(1-T)} \right) , \tag{6.2.12}$$

$$\sigma_T = (\sigma_1 + \sigma_2)^2 - 4\sigma_3^2 T . \tag{6.2.13}$$

These invariants are found through the determinants of the sub-blocks in the global covariance matrix. For direct reconciliation, the symplectic eigenvalues are,

$$\nu_{E|A\pm} = \frac{1}{2} \left(\sqrt{(e_\kappa + W)^2 - 4T(W^2-1)} \pm (e_\kappa - W) \right) , \tag{6.2.14}$$

with the parameter $e_\kappa = (1-T)(1+\kappa) + TW$. We then have the overall secret key rate,

$$R = \beta I(A:B) - \chi(E:X) \ , \tag{6.2.15}$$

where β is the reconciliation efficiency. The security region for the protocol is shown in Figure 6.2, comparing reverse and direct reconciliation security for varying levels of preparation noise. From this one can clearly see that direct reconciliation actually is superior to reverse reconciliation if the level of preparation noise is sufficiently high. A main conclusion of the work done by Weedbrook *et al.* [141, 145] was that direct reconciliation could in principle withstand asymptotic amounts of preparation noise. From Figure 6.2(b) we see that this conclusion does not apply when the reconciliation efficiency is below unity, such that there is in fact an optimal but non-zero amount of preparation noise. This is a clear parallel to the results of García-Patrón and Cerf [169].

In general, the conclusion that direct reconciliation outperforms reverse reconciliation is rather surprising because reverse reconciliation is generally regarded as being superior to direct reconciliation [47, 48].

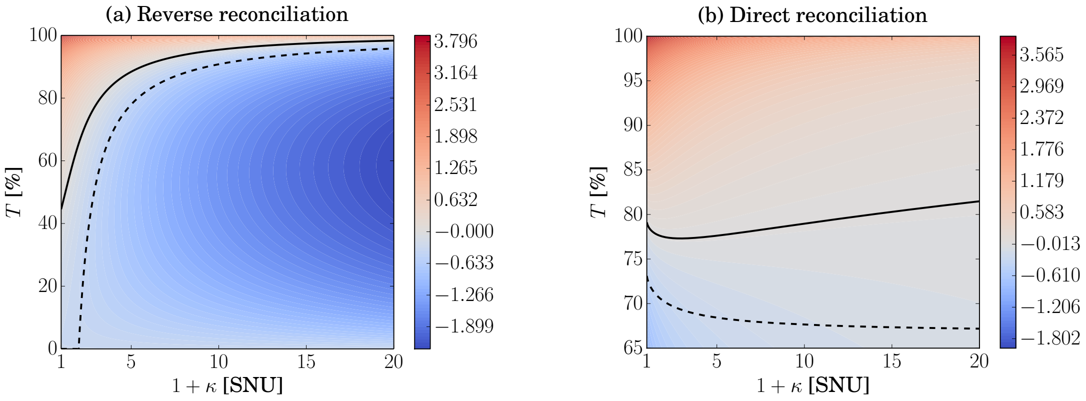


Figure 6.2: Security region for the protocol in terms of transmission T and preparation noise κ, for (**a**) reverse reconciliation and (**b**) direct reconciliation. Error reconciliation efficiency was $\beta = 95\%$, with modulation variance 32 SNU, and thermal noise injection $W = 1.11$. The solid line represents the zero crossing of the secret key rate for these parameters. The dashed lines in both plots represent the edge of the security region in the ideal case where $\beta = 1$, excess noise is zero and modulation is high. For the case of reverse reconciliation, when $\kappa = 0$, the rate goes to zero asymptotically with transmission loss. However, when κ increases the security region shrinks rapidly. For the case of direct reconciliation, the rate goes to zero near 73 % transmission because Bob uses heterodyne detection, and this introduces an extra unit of vacuum. These plots directly illustrate how direct reconciliation is more robust against preparation noise.

Experiments

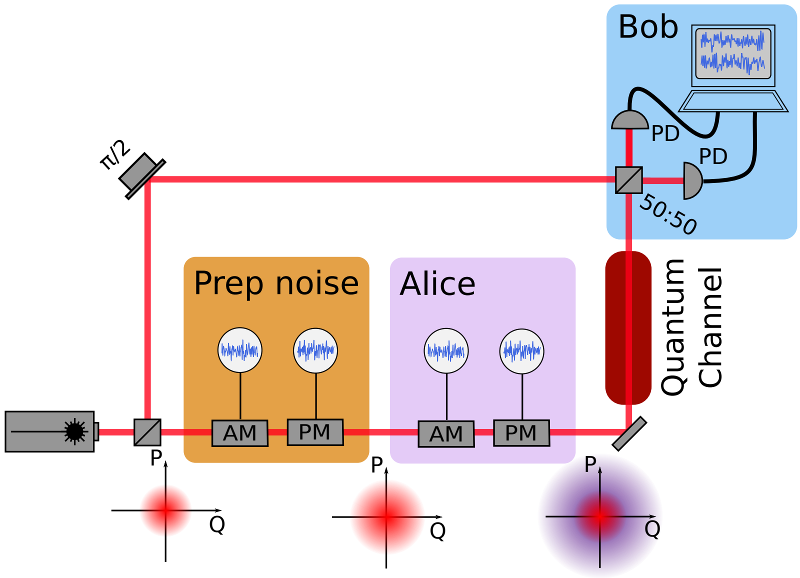


Figure 6.3: Sketch of the experimental setup. The first pair of modulators are used to simulate a noisy laser, since the source is shot noise limited. This allows free control of the quality of the source. The second pair of modulators generate the continuous alphabet. Transmission is controlled by reducing the modulation variance relative to the calibration variance. Bob performs heterodyne detection. AM: Amplitude modulator. PM: Phase modulator. PD: Photo detector.

We experimentally test the predicted superiority of direct reconciliation with different levels of preparation noise. The experimental setup is depicted in Figure 6.3. Alice prepared a quadrature symmetric continuous alphabet of coherent states, with a pair of electro-optical modulators coupled to two independent white noise generators. The modulators were orthogonalized according to the procedure outlined in Section 3.3, and in this way they realize the Weyl operator from Equation (2.4.1). The alphabet thus consists of a Gaussian distribution of coherent states, which in total results in a thermal state with the signal variance $V_S = \mu - 1$, relating this prepare-and-measure implementation to the entanglement equivalent model.

The generator outputs that realized this Gaussian distribution were also recorded with an analog-to-digital converter to be correlated with Bob's measurements in the post-processing stage. The determination of these correlations allowed for precise determination of the channel parameters. In addition to these signal modulations, the modulators received added inputs from two uncorrelated noise generators. These outputs were not recorded and served as the preparation noise, since they effectively reduce the correlations between the Alice's signal and the measurements of Bob. From this additional modulation we realized a total quadrature symmetric thermal input state with the variance $V_S + 1 + \kappa$, where we have separated the shot noise from the classical preparation noise.

A lossy quantum channel of transmission T was implemented by reducing the input modulation relative to the calibration measurement, as was also the case for Chapter 4. The transmitted quantum states were detected with the simplified heterodyne described in Section 3.7.2, where the signal and LO beams each had 2.8 mW of optical power. The benefit of reducing the relative modulation strength was that it allowed the optical power to be kept constant, since with this simplified heterodyne detection, the shot noise level is determined by the combined power of the carriers.

The photocurrents were mixed down from the 10.5 MHz sideband, recorded by the analog-to-digital converter, and were then added and subtracted in the post processing to generate the datasets for the respective quadrature measurement outcomes. These measurements were correlated with the phase matched recording of the input modulation, which was then used to determine the channel parameters. All noise in this implementation is regarded as originating from the trusted preparation noise modulation, and the channel excess noise is assumed to be zero.

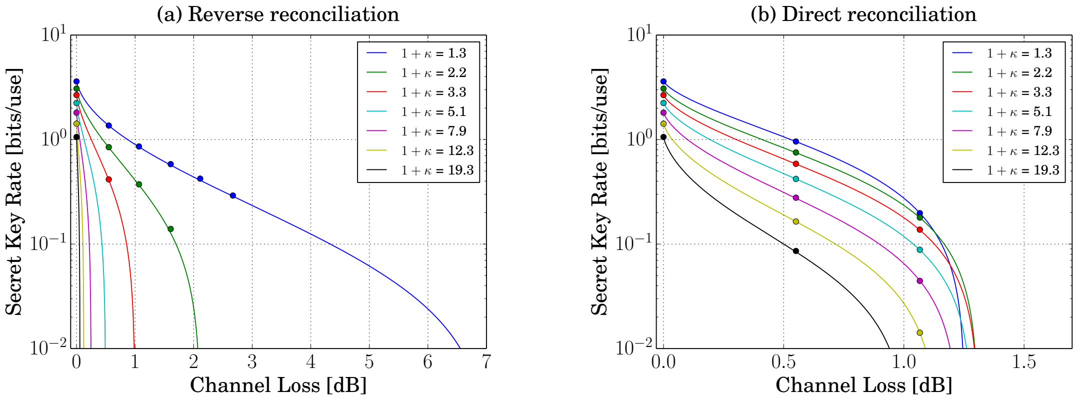


Figure 6.4: Data points and corresponding theory curves, with varying values for κ. (**a**) is for reverse reconciliation, while (**b**) uses direct reconciliation. The efficiency of the reconciliation is set to $\beta = 0.95\,\%$. Statistical error bars are smaller than the point size, due to the high number of data points.

The rates for the found channel parameters are calculated, with the corresponding theory lines as shown in Figure 6.4, plotted against the channel loss in units of dB. Figure 6.4(a) shows the estimated rates for reverse reconciliation, while Figure 6.4(b) shows the rates for direct reconciliation. The seven different traces represent varying values of preparation noise. The corresponding points to these traces do not fit the theoretical predictions exactly. This is caused by overall fluctuations in the channel parameters. The statistical errors are comparatively tiny because of the number of data points, while the fluctuations in the noise parameters are the result of locking instabilities in the local oscillator phase relative to the signal beam, which are not statistically independent errors.

The mismatch of the correlations between the recording of the coherent Gaussian alphabet and the actual alphabet measured at Bob was the principal source of excess preparation noise in this setup, which caused the preparation noise to drop slower than what would be expected from a lossy quantum channel. This mismatch in noise levels was transmission dependent because of the way the transmission loss was implemented. A reduction of the modulation depth in the signal at Alice put her recorded signal closer to the electronic noise of the amplifier and analog-to-digital converter, which degraded the correlations. Choosing to regard this as initial preparation noise, we see from the results that direct reconciliation is superior to reverse reconciliation. While the security of reverse reconciliation quickly degrades for increased preparation noise, the secret key rate stays relatively constant using direct reconciliation.

Concluding remarks

As predicted in [141, 145], these experimental results confirm that direct reconciliation is indeed superior to reverse reconciliation if large amounts of preparation noise are present. One possible application of this is QKD in regimes where shot noise limited sources are too expensive or impractical, for example using microwaves as was also suggested in [141].

An interesting prospect is also implementing this protocol with a cheap diode laser, preferably at a telecom wavelength, where the preparation noise is not artificial.

Single Quadrature Continuous Variable Quantum Key Distribution

Introduction

In general, QKD schemes use that the states prepared by Alice are in conjugate bases, such that the states that encode the information are not orthogonal. This is particularly obvious for QKD with discrete variables [7, 17, 37, 171]. This non-orthogonality ensures that the no-cloning theorem applies [27]. Gaussian states are automatically non-orthogonal no matter what the alphabet is, and so the security provided by the no-cloning theorem extends to the scenario of exchanged Gaussian states no matter the quadrature in which they are distributed. This is the basis of the security of continuous variable QKD [69, 70, 71].

Encoding the alphabet into a single quadrature has been investigated with a coherent state protocol using only two states [49, 50]. We present this idea with a continuous alphabet in a single quadrature. The security analysis considers the specific attack of an asymmetric entangling cloner and preparation noise. We experimentally test both homodyne and heterodyne configurations. It turns out that this single quadrature protocol has an additional complication in terms of hidden correlations exploitable only by the eavesdropper. This was initially discussed by Usenko and Grosshans [172].

From a practical point of view CVQKD in a single quadrature is interesting because it simplifies the state generation for Alice, since she will only need one modulator. The cost of this reduced complexity is that the generated secret key rate decreases faster with noise. This work was published in [173].

Theory

The prepare-and-measure protocol developed here follows that developed in Chapter 6, with one major change being that of a simplified modulation. Here, we let Alice encode a one-dimensional Gaussian alphabet onto her phase quadrature P, which on average generates an asymmetric thermal state in phase space. This is the essential difference between this protocol and the standard dual quadrature continuous

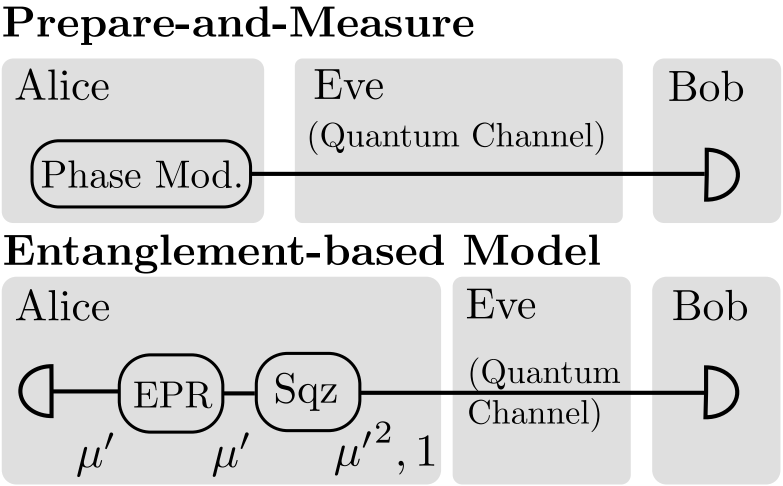


Figure 7.1: Prepare-and-measure scheme and the equivalent entanglement based model. Alice encodes a continuous Gaussian distribution of coherent states onto her phase quadrature and sends these states through the quantum channel. In the entanglement scheme she prepares an EPR state and squeezes the outgoing mode by the proper amount, before using the quantum channel. EPR: Einstein-Podolsky-Rosen source, Sqz: Squeezing operation.

alphabet CVQKD protocol, where the prepared thermal state is typically symmetric. The prepared coherent states go through the quantum channel, and arrive at Bob who implements a coherent quadrature detection, either with heterodyne detection or switched homodyne detection such that he monitors both quadratures on average, to make sure that Eve does not inject probe states into the quadrature that is not encoded. The P quadrature measurement outcomes recorded by Bob are correlated with Alice's input states. These correlations form the basis of the secret key generation after error reconciliation and privacy amplification.

We address the security of the scheme using the techniques described in Section 2.14. The equivalent entanglement based scheme is shown in Figure 7.1. Here, Alice prepares an EPR state, and keeps one mode for conditioning. The outgoing mode is squeezed through a local squeezing operation, before the mode is sent through the quantum channel. As argued in Section 2.8, Alice performing a heterodyne measurement on the conditioning mode will form a 2D Gaussian distribution of coherent states at Bob. On the other hand, performing homodyne detection will generate a 1D distribution of squeezed states. Therefore, if the outgoing EPR mode is squeezed with the proper squeezing parameter, homodyne conditioning will prepare a 1D distribution of coherent states, securing equivalence with the prepare-and-measure scheme. In the entanglement equivalent model, Alice prepares an EPR state of the form,

$$\mathbf{\Gamma}'_{\mathrm{EPR}} = \begin{bmatrix} \mu'\mathbb{I}_2 & \sqrt{\mu'^2 - 1}\boldsymbol{Z} \\ \sqrt{\mu'^2 - 1}\boldsymbol{Z} & \mu'\mathbb{I}_2 \end{bmatrix} . \tag{7.2.1}$$

Performing a local squeezing operation with the variance μ' on the outgoing state we obtain,

$$\mathbf{\Gamma}'_{\text{out}} = \begin{bmatrix} \mu' & 0 & \sqrt{\frac{\mu'^2-1}{\mu'}} & 0 \\ 0 & \mu' & 0 & -\sqrt{\mu'(\mu'^2-1)} \\ \sqrt{\frac{\mu'^2-1}{\mu'}} & 0 & 1 & 0 \\ 0 & -\sqrt{\mu'(\mu'^2-1)} & 0 & \mu'^2 \end{bmatrix} . \tag{7.2.2}$$

The second mode of this state is propagated through the quantum channel. In this channel, Eve is allowed to apply any unitary operator allowed by quantum mechanics. In the asymptotic limit, the Holevo bound then quantifies the maximum amount of information Eve can extract from this operation, as defined in Equation (2.14.32),

$$\chi(E:X) = S(E) - S(E|X) . \tag{7.2.3}$$

X is Alice or Bob, depending on the reconciliation technique used. The asymptotic rate is given by the usual Devetak-Winter bound,

$$R = \beta I(A:B) - \chi(E:X) , \tag{7.2.4}$$

where $I(A:B)$ is defined in Equation (2.13.13) and $\beta \in [0,1]$ quantifying the efficiency of the reconciliation procedure. Assuming that Eve is able to purify the global state, we have the relations $S(E) = S(AB)$, $S(E|B) = S(A|B)$ and $S(E|A) = S(B|A)$, due to the self-duality of von Neumann entropy as described in Section 2.14. From this we get the following equations for the rate with different reconciliation techniques,

$$R_{RR} = \beta(H(A) - H(A|B)) - S(AB) + S(A|B) , \tag{7.2.5}$$

for reverse reconciliation and,

$$R_{DR} = \beta(H(A) - H(A|B)) - S(AB) + S(B|A) , \tag{7.2.6}$$

for direct reconciliation.

These relations are useful in the data processing of the experimental data, as we only have access to the reconstructed modes of Alice and Bob. One difference from the dual quadrature protocol is that the correlations between Alice and Bob in the Q quadrature remain undetermined, because Alice does not encode in this quadrature. This leaves us with a free correlation parameter that must be chosen in a pessimistic fashion, because Eve can implement an attack that realizes the worst possible value. The possible values for this parameter are bounded by Heisenberg's uncertainty principle, which for covariance matrices takes the form given in Equation (2.7.3).

For the specific case of an asymmetric entangling cloner attack, we investigate the behaviour of the protocol parameters, and the dependence on the free correlation parameter. The model for this attack is shown in Figure 7.2. This attack is chosen

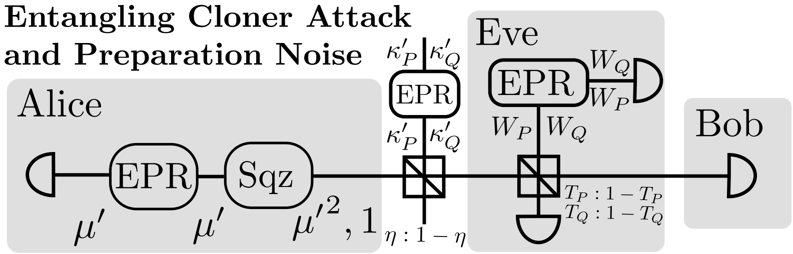


Figure 7.2: Model of the Eve's asymmetric entangling cloner attack on the channel. This model also includes preparation noise, with and without the assumed trust. Trusted modes are not accessible to Eve for purification, while the untrusted modes are. EPR: Einstein-Podolsky-Rosen entanglement, Sqz: Squeezing.

because it is the most practical Gaussian attack Eve can use on the quantum channel, as long as we are in the asymptotic limit [71], where we may make full use of its Gaussian properties. The accessible parameters in this attack are the asymmetric transmissions T_Q and T_P and the asymmetric noise injections W_Q and W_P. The asymmetric preparation noise is described by the parameters κ_Q and κ_P.

Eve implements the attack by preparing a possibly squeezed EPR state, where she injects one mode into the quantum channel through an asymmetric beam splitter. The other mode of Eve's EPR state is stored in a quantum memory. The output mode of the beam splitter operation is also stored in a quantum memory, and the states stored in the quantum memories are measured coherently once the state transfer between Alice and Bob is over. The preparation noise is simulated by the environment generating an EPR state that is interfered with Alice's output mode before it enters the quantum channel. It does this on a beam splitter with transmission $\eta \approx 1$. If the environment does not inject preparation noise into the system, the outgoing mode is very slightly mixed with a vacuum mode. This error is largely corrected for by redefining the parameters of the input state. Importantly, this can never overestimate the security of the protocol, since mixing with a vacuum mode can only ever reduce the correlations shared by Alice and Bob. When subjecting the input state to the preparation noise we get the covariance matrix,

$$\boldsymbol{\Gamma}_{A\kappa'} = \begin{bmatrix} \boldsymbol{A}' & \boldsymbol{C}' \\ \boldsymbol{C}'^T & \boldsymbol{K}' \end{bmatrix} , \tag{7.2.7}$$

with the submatrices,

$$\boldsymbol{A}' = \begin{bmatrix} \mu' & 0 & \sqrt{\eta\frac{\mu'^2-1}{\mu'}} & 0 \\ 0 & \mu' & 0 & -\sqrt{\eta\mu'\tilde{\mu}'} \\ \sqrt{\eta\frac{\mu'^2-1}{\mu'}} & 0 & \eta+\tilde{\eta}e^{-2r}\kappa' & 0 \\ 0 & -\sqrt{\eta\mu'\tilde{\mu}'} & 0 & \eta\mu'^2+\tilde{\eta}e^{2r}\kappa' \end{bmatrix} , \tag{7.2.8}$$

$$\boldsymbol{K}' = \begin{bmatrix} \tilde{\eta} + \eta e^{-2r}\kappa' & 0 & e^{-r}\sqrt{\eta\tilde{\kappa}'} & 0 \\ 0 & \tilde{\eta}\mu'^2 + \eta e^{2r}\kappa' & 0 & -e^{r}\sqrt{\eta\tilde{\kappa}'} \\ e^{-r}\sqrt{\eta\tilde{\kappa}'} & 0 & \kappa' & 0 \\ 0 & -e^{r}\sqrt{\eta\tilde{\kappa}'} & 0 & \kappa' \end{bmatrix} , \tag{7.2.9}$$

$$\boldsymbol{C}' = \begin{bmatrix} -\sqrt{\frac{\tilde{\eta}\tilde{\mu}'}{\mu'}} & 0 & 0 & 0 \\ 0 & \sqrt{\tilde{\eta}\mu'\tilde{\mu}'} & 0 & 0 \\ \sqrt{\eta\tilde{\eta}(e^{-2r}\kappa' - 1)} & 0 & e^{-r}\sqrt{\tilde{\eta}\tilde{\kappa}'} & 0 \\ 0 & \sqrt{\eta\tilde{\eta}(e^{2r}\kappa' - \mu'^2)} & 0 & -e^{r}\sqrt{\tilde{\eta}\tilde{\kappa}'} \end{bmatrix} , \tag{7.2.10}$$

where $\tilde{\eta} = 1 - \eta$, $\tilde{\kappa}' = \kappa'^2 - 1$, and $\tilde{\mu}' = \mu'^2 - 1$. μ' and κ' determine the initial EPR states before the mixing operation, while r is a squeezing parameter, that determines how asymmetric the preparation noise is. The parameters κ'_P and κ'_Q from Figure 7.2 are related to κ' such that $\kappa'_P = \kappa' e^{-2r}$ and $\kappa'_Q = \kappa' e^{2r}$. These initial values are governed by the parameters used in the practical protocol, and so they must obey the equations,

$$\eta\mu'^2 + (1 - \eta)e^{2r}\kappa' = \mu^2 + \kappa_P \ , \tag{7.2.11}$$

$$\eta + (1 - \eta)e^{-2r}\kappa' = 1 + \kappa_Q \ , \tag{7.2.12}$$

$$\eta\mu'(\mu'^2 - 1) = \mu(\mu^2 - 1) \ . \tag{7.2.13}$$

These equations relate the entanglement-based model parameters to the parameters in the practical implementation such that we have the variance $\mu^2 + \kappa_P$ in the P quadrature, which is used for signalling. In this way the signal variance is $\mu^2 - 1$, κ_P is the preparation noise in this quadrature and μ is lower bounded at 1, representing the shot noise. κ_P is thus lower bounded at zero. κ_Q is the preparation noise in the Q quadrature, also lower bounded at zero. The last equation introduces a bound on the correlations, such that they are determined purely by μ, since this parameter represents the signal strength. This is a fully determined system of equations with the solutions,

$$\kappa' = \frac{\mu^2 + \kappa_P - \eta\mu'^2}{(1 - \eta)} e^{-2r} \ , \tag{7.2.14}$$

$$r = \frac{1}{4} \ln\left(\frac{\mu^2 + \kappa_P - \eta\mu'^2}{1 + \kappa_Q - \eta}\right) \ , \tag{7.2.15}$$

$$\mu'^2 = \frac{\Delta}{6\eta} + \frac{2\eta}{\Delta} \ , \tag{7.2.16}$$

where Δ is the determinant,

$$\Delta = \sqrt[3]{(12\sqrt{81\mu^6 - 162\mu^4 - 12\eta^2 + 81\mu^2} + 108\mu^3 - 108\mu)\eta^2} \ . \tag{7.2.17}$$

These solutions allow for the expression of the entanglement-based model through the parameters of the practical protocol.

In the quantum channel controlled by Eve, the covariance matrix $\mathbf{\Gamma}_{A\kappa'}$ is transformed by an asymmetric beam splitter operation with the transmissions T_Q and T_P. It may easily be shown that such a beam splitter maintains the structure of the symplectic space by confirming the condition given in Equation (2.2.5). It may also be suitably decomposed into a combination of the symplectic operations listed in Section 2.7. After the quantum channel, the state shared by Alice and Bob is described by the covariance matrix,

$$\mathbf{\Gamma}_{AB} = \begin{bmatrix} \mu' & 0 & \sqrt{\frac{T_Q\eta\tilde{\mu}'}{\mu'}} & 0 \\ 0 & \mu' & 0 & -\sqrt{T_P\eta\mu'\tilde{\mu}'} \\ \sqrt{\frac{T_Q\eta\tilde{\mu}'}{\mu'}} & 0 & T_Q\kappa'' + \tilde{T}_Q W_Q & 0 \\ 0 & -\sqrt{T_P\eta\mu'\tilde{\mu}'} & 0 & T_P\mu'' + \tilde{T}_P W_P \end{bmatrix} , \tag{7.2.18}$$

where $\kappa'' = \eta + e^{-2r}\tilde{\eta}\kappa'$ and $\mu'' = \eta\mu'^2 + e^{2r}\tilde{\eta}\kappa'$. W_Q and W_P are quadrature asymmetric noise injections from Eve's asymmetric entangling cloner. We additionally define the reflection coefficients $\tilde{T}_P = 1 - T_P$ and $\tilde{T}_Q = 1 - T_Q$. We now wish to calculate the information quantities associated with this state, assuming that the eavesdropper is able to purify the state. We remark that in a practical implementation, there is no way for Alice and Bob to estimate the parameter,

$$\mathbf{\Gamma}_{AB,13} = \sqrt{\frac{T_Q\eta\tilde{\mu}'}{\mu'}} , \tag{7.2.19}$$

which depends solely on one channel parameter, namely T_Q. What they can estimate is the parameter,

$$\mathbf{\Gamma}_{AB,33} = T_Q(\eta + e^{-2r}\tilde{\eta}\kappa') + (1 - T_Q)W_Q , \tag{7.2.20}$$

which for the most pessimistic choice of T_Q in turn gives an estimate of W_Q, provided that the honest parties have some knowledge of κ_Q, which Alice may obtain by secretly measuring some of her own output states before the channel. She may do this regardless of the trust assumptions placed on the preparation noise, i.e. it does not matter if the noise is produced by Eve through a side channel attack or inadvertently created by Alice while she is preparing her output states.

The mutual information between Alice and Bob when Bob uses homodyne detection is given by,

$$I_{\text{homo}}(A : B) = \frac{1}{2}\log_2\left(\frac{(1 - T_P)W_P + T_P(\mu + \kappa_P)}{(1 - T_P)W_P + T_P(\eta + (1 - \eta)\kappa'_P)}\right) . \tag{7.2.21}$$

Taking the limits $\kappa_P = 0$ and $\eta = 1$, one recovers half the information content of a dual quadrature protocol from Chapter 6 as expected. If Bob uses heterodyne detection the expression becomes,

$$I_{\text{hete}}(A:B) = \frac{1}{2}\log_2\left(\frac{(1-T_P)W_P + T_P(\mu+\kappa_P)+1}{(1-T_P)W_P + T_P(\eta+(1-\eta)\kappa'_P)+1}\right) , \tag{7.2.22}$$

where the difference to Equation (7.2.21) is exactly the addition a unit of vacuum that arises from the heterodyne detection as discussed in Section 3.7.2. It is worth noting that only the transmission T_P appears in these expressions, because no information is encoded in Q. Also, only the noise injection in P will degrade the information content, since this noise effectively reduces the signal-to-noise ratio for Bob. W_Q will naturally still influence the security, but it does so by indirectly increasing the Holevo bound, since the physicality bound on the global state in Equation (7.2.18) is relaxed when the noise increases.

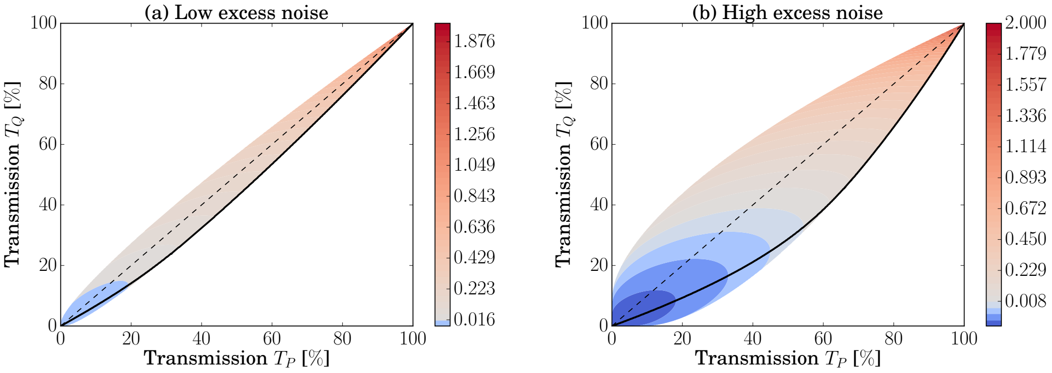


Figure 7.3: Plot of the physicality region in terms of asymmetric transmissions assuming fixed noise injections, with heterodyne detection and reverse reconciliation. The color shows the secret key rate in bits per channel use. The black solid line is the value of T_Q that minimizes the rate for this particular noise injection. The dashed line shows the condition $T_P = T_Q$. For plot (a) parameters are $W_P = W_Q = 1.005\,\text{SNU}$, and for (b) $W_P = W_Q = 1.05\,\text{SNU}$. The parameters $\mu = 31\,\text{SNU}$, $\beta = 1$ and $\kappa_Q = \kappa_P = 0$ are the same for both plots.

The calculation of the Holevo bound will depend on the reconciliation between Alice and Bob, but also on the trust assumption we place on the preparation noise. If the preparation noise is trusted we use the identity $S(E) = S(AB\kappa)$, and if it is not trusted we use $S(E\kappa) = S(AB)$. Both of these are valid due to the self-duality of the von Neumann expression, described in Section 2.14. This added complication of the preparation noise ensures that the expression for the symplectic spectrum of the relevant state is quite complicated. It is however easily calculated numerically. The identities for the conditional entropies relevant to reverse reconciliation are $S(E|B) = S(A\kappa|B)$ and $S(E\kappa|B) = S(A|B)$ for trusted and untrusted preparation noise respectively. For direct reconciliation we have $S(E|A) = S(B\kappa|A)$ and $S(E\kappa|A) = S(B|A)$. These are also calculated numerically. We investigate direct reconciliation, in addition to reverse reconciliation, because we have preparation noise,

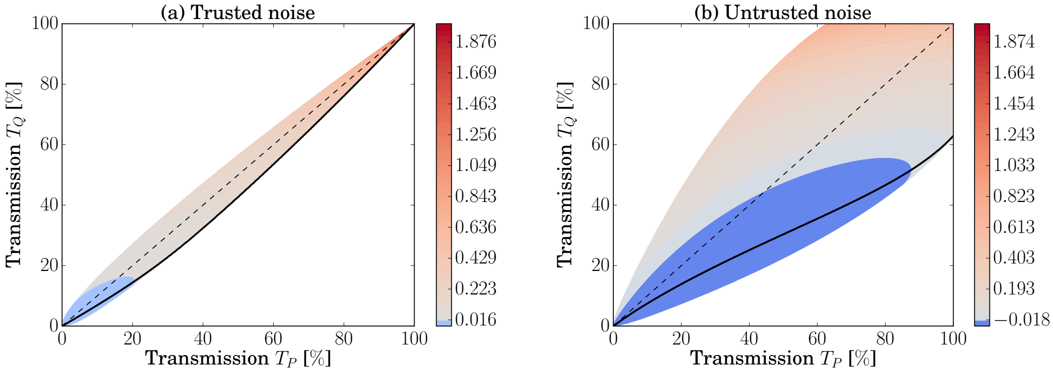


Figure 7.4: Physicality region plotted for fixed injection noise with heterodyne detection and reverse reconciliation, in terms of asymmetric transmissions. Colour indicates secret key rate generation in bits per channel use. The black solid line shows the choice of T_Q that minimizes the rate, dashed line is $T_P = T_Q$. Plot (a) has $\kappa_P = \kappa_Q = 0.1$ SNU, which is assumed to be trusted, while (b) also has $\kappa_P = \kappa_Q = 0.1$ SNU, but the noise is not assumed to be trusted. The parameters $\mu = 31$ SNU, $\beta = 1$ and $W_Q = W_P = 1.005$ are the same for both plots.

otherwise the superiority of reverse reconciliation is well established [31, 48, 66, 70, 71].

For Alice and Bob to estimate the rate of secret key generation they need to estimate the channel parameters. They can readily estimate T_P and W_P, because of their correlations. They also have the variance of Q in Bob's mode available, but this depends on T_Q and W_Q, which still leaves the free parameter $\mathbf{\Gamma}_{AB,13}$. This free parameter is only bounded by the requirement that the state $\mathbf{\Gamma}_{AB}$ remains physical. Knowing the bounds on this parameter, we can plot the security region against the other channel parameters. For example, for fixed noise injection W_P and W_Q, we can investigate how the security region, i.e. the region of positive secret key rate, varies with T_P and T_Q. See Figure 7.3 for this plot, for low and high noise injection. We see very clearly that the physicality region, i.e. the region of physical covariance matrices for variations in $\mathbf{\Gamma}_{AB,13}$, grows when the noise injection goes up. Similar behaviour is observed for the preparation noise, as seen in Figure 7.4. If there is no noise injected, either in the preparation or channel stage, the inequality forces the transmissions to be symmetric such that $T_P = T_Q$. The widening of the physicality for increased noise is what causes the noise sensitivity compared to a dual quadrature protocol. If both quadratures are encoded, there is no ambiguity in determining T_Q and W_Q, as well as T_P and W_P.

Figure 7.5 plots the secret key rate in terms of channel loss in dB. It compares heterodyne and homodyne detection strategies and single and dual quadrature encodings, with reverse reconciliation and no preparation noise. Figure 7.5(a) has no noise injection, and in Figure 7.5(b) $W_Q = W_P = 1.01\,$SNU. The signal variance is optimized

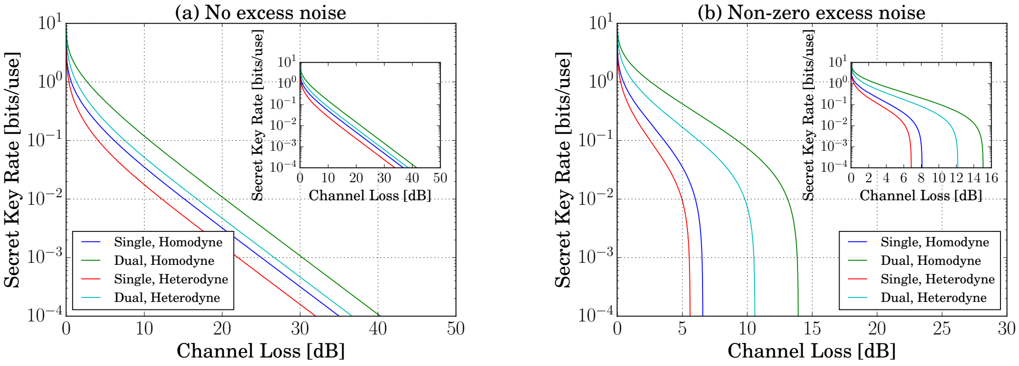


Figure 7.5: Secret key rate plotted against channel loss for four different protocols, combining homodyne and heterodyne detection strategies and dual and single quadrature encoding. Reverse reconciliation is used in both, and there is no preparation noise. Plot (a) has no excess noise injection, and in (b) $W_Q = W_P = 1.01$ SNU. Signal modulation variance was optimized for the protocol parameters, since $\beta = 97\,\%$. $\beta = 100\,\%$ is used in the insets.

for each transmission value, because $\beta = 97\,\%$ in the main figure. $\beta = 100\,\%$ in the insets. When β is not unity, the optimal signal variance depends on the other protocol parameters, and so it is reasonable to find the optimal signal variance for every transmission value to increase the range of the protocol.

Figure 7.6 shows the secure key rate against channel loss, but with different levels of preparation noise. Figure 7.6(a) uses reverse reconciliation and Figure 7.6(b) uses direction reconciliation. As expected from the results of [141] and Chapter 6, direct reconciliation is superior for increased preparation noise.

Combining the plots of Figures 7.3, 7.4, 7.5 and 7.6, the overall conclusion is that encoding coherent states in a single quadrature can indeed provide quantum security, with reduced practical complexity, but a somewhat reduced rate. All the Q quadrature measurements performed by Bob do not give an increase in $I(A:B)$, but they are necessary for estimating the quantum channel, specifically the parameter $\mathbf{\Gamma}_{AB,33}$. There are several ways to implement this in practice, for example every other measurement could be in Q, or Bob could use random switching between the quadratures. This switching need not be symmetric between the quadratures, as long as it is faster than the time scale on which the channel parameters might change. Having the switching be random ensures that Eve can not expect to rely on changing the channel parameters while Bob is not looking.

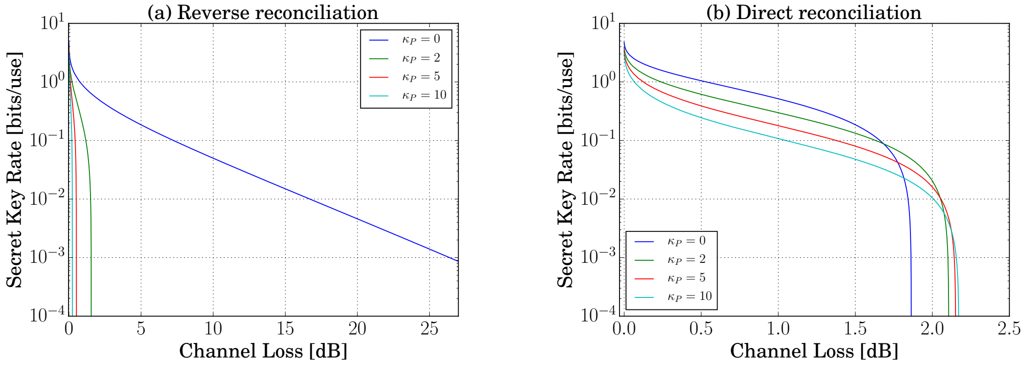


Figure 7.6: Secret key rate plotted against channel loss, with different levels of preparation noise. Reverse reconciliation is used in (a), and it is indeed quite sensitive to increases in κ as expected. Plot (b) uses direct reconciliation. Other parameters are $\beta = 1$, $\mu = 1000$ and $W_Q = W_P = 1$.

Experiments

We implemented the single quadrature protocol with both heterodyne and homodyne detection strategies, in free space. We restrict ourselves to reverse reconciliation techniques as the projected preparation noise values are so minute as to preserve the superiority of this reconciliation technique. The schematic is shown in Figure 7.7. Adjusting the power distribution of the signal beam relative to the local oscillator allows the same setup to realize both detection schemes as as described in Section 3.7.2.

To implement the heterodyne detection scheme, the continuous wave beam was split evenly between signal and LO, so both beams had a power of 2.8 mW. To implement the homodyne detection, the signal was chosen to be 0.1 mW, and the LO was set to 2.8 mW. In both cases the signal beam had the phase quadrature modulated by an electro-optical modulator. Contrary to the protocols described in the previous chapters, there was no need to ensure orthogonalization of the modulations according to the procedure described in Section 3.3. The electro-optical modulator received a Gaussian distribution from a white noise generator at the measured sideband. This generated a coherent state alphabet in a single quadrature, with the variance $V_S = \mu^2 - 1$. The noise generator outputs were also recorded locally at Alice, which allowed these data points to be correlated with the measurements performed by Bob.

Bob performed the heterodyne detection by interfering the two beams and keeping their relative phase locked at $\pi/2$. For the homodyne detection scheme, P and Q were measured separately by changing the relative phase between the beams to $\pi/2$ and 0 respectively. The switching was in this case not on-line, but rather an offline switch after sufficient data from one quadrature had been obtained.

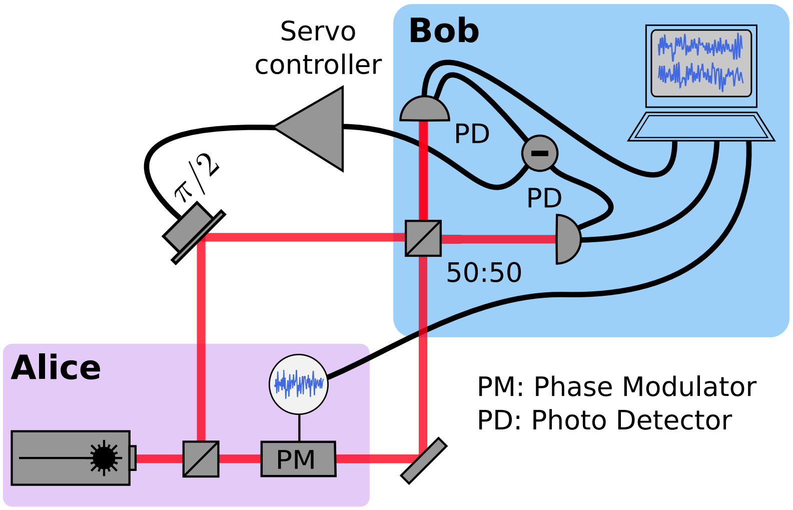


Figure 7.7: Experimental setup sketch. Alice splits her beam, and forwards one mode directly as a bright local oscillator. The signal beam is modulated by a phase modulator fed by a noise generator producing Gaussian white noise within the measurement bandwidth. Bob performed heterodyne detection, while phase locking the local oscillator to have a relative phase to the signal of $\pi/2$. In this case the two beams are equally bright. For homodyne detection the local oscillator was much brighter than the signal beam. For both detection cases the PIN diode currents are digitized, as well as the signal encoding from the noise generator at Alice. PM: Phase modulator, PD: Photo detector.

For both detection schemes, the photocurrents from the detector outputs were demodulated from the 10.5 MHz sideband. The output of the mixer was low-pass filtered at 100 kHz and digitized with a 14 bit data acquisition card, that sampled the signal at 500 kHz. For the heterodyne scheme, the two data streams generated from the above operation were subtracted and added to give the respective quadrature outcomes, as shown in Section 3.7.2. For homodyning, the data streams were subtracted for two separate runs, with different relative phases. The classical signal recorded from Alice's signal generator was scaled in the post-processing to optimize the correlations between the honest parties. Specifically, this was done by minimizing the variance of the subtracted data streams through a gain factor on Alice's measurements.

A modulation variance of 15 dB above shotnoise defines the 100 % transmission value, as a calibration measurement. For the heterodyne measurement, this input modulation was reduced to simulate transmission loss, to avoid changing the shot noise level as in Section 4.3. For the homodyne measurements, the loss was implemented directly via polarization control and a polarizing beam splitter. Each measurement run generated 10^6 samples. From these samples, the post-processing generated the covariance matrix shared by Alice and Bob after the quantum channel in the entanglement-based equivalent model, as shown in Equation (7.2.18). A sample covariance matrix for the entanglement-based equivalent model was generated from this data, and for $T_P = 77\%$ it was found to be,

$$\mathbf{\Gamma}_{\mathrm{AB}} = \begin{bmatrix} 3.172 & 0 & ? & 0 \\ 0 & 3.172 & 0 & -3.567 \\ ? & 0 & 1.019 & 0 \\ 0 & -3.567 & 0 & 5.056 \end{bmatrix} . \tag{7.3.1}$$

The question marks in Equation (7.3.1) represent the correlation parameter from Equation (7.2.18), which is undetermined by the data processing. The mutual information between Alice and Bob is calculated using,

$$I(A:B) = \frac{1}{2}\log_2\left(\frac{V_B}{V_B - C_{AB}^2/V_A}\right) , \tag{7.3.2}$$

where V_A is the signal strength as determined by the size of Alice's modulation, V_B is the second moment of Bob's measurements, and C_{AB} determines the correlation between the parties. Calculating the Holevo bound using the purification assumptions and applying Equation (7.2.5), the secret key rate bound using reverse reconciliation was calculated, while the correlation parameter was chosen to minimize this rate. Setting $\beta = 97\,\%$, the results of the data processing are plotted in Figure 7.8 for both detection schemes.

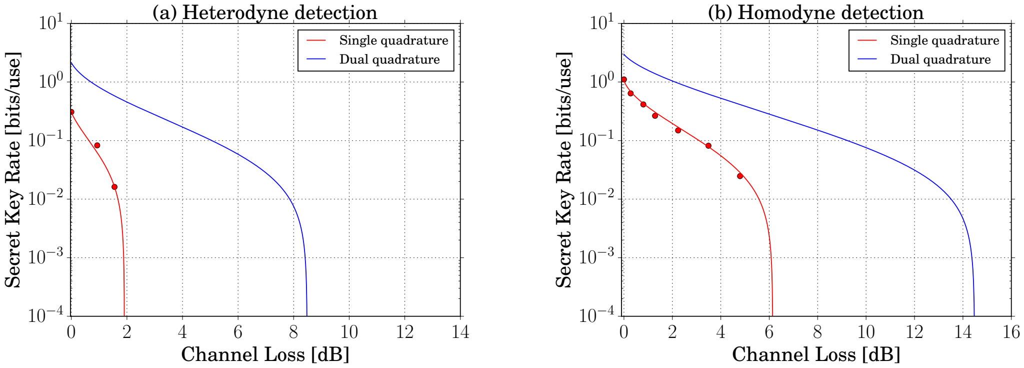


Figure 7.8: Plot of the secret key rate bound obtained from the data versus channel loss in dB, assuming $\beta = 97\,\%$, $\mu = 31.2$ SNU and reverse reconciliation. The measured noise was modelled as a combination of untrusted preparation noise and an entangling cloner attack, and the red solid line is a fit of the theoretical rate equation to find the noise parameters. The blue line is the rate one would obtain from a dual quadrature protocol with the same noise parameters. The statistical error on the data points is smaller than the point size because of the number of points. Plot (a) uses heterodyne detection. The noise parameters are found to be $W_Q = 1.0135$ SNU, $W_P = 1.0000$ SNU, $\kappa_Q = 0.0435$ SNU, $\kappa_P = 0.0422$ SNU. Plot (b) uses homodyne detection. The noise parameters here are $W_Q = 1.0164$ SNU, $W_P = 1.0000$ SNU, $\kappa_Q = 0.0119$ SNU, $\kappa_P = 0.0098$ SNU.

The theoretical model represented by Equation (7.2.5), with untrusted preparation noise, reverse reconciliation and $\beta = 97\,\%$, was used to find suitable values for the noise parameters in the quantum channel by running a fit routine. The results of this fitting are visualized by the red solid lines in both plots. This is compared to the behaviour of a protocol using dual quadrature encoding, with the same noise parameters. The dual quadrature protocol has the advantage of twice the alphabet size, and the ability to certify that $T_P = T_Q$. From these plots and the fitted model we can infer a theoretical maximum range equivalent to just below 10 km in an optical fiber with an attenuation 0.2 dB per km for heterodyne detection and slightly above 30 km for the homodyne detection. The reason for this is that the noise parameters are better for the homodyne detection, especially for the untrusted preparation noise.

The noise contributions in this implementation mainly come from a mismatch between the recorded signal from the noise generator, and the state that is actually produced. In other words these two supposedly identical outputs are limited in how well correlated they are and this results in noise. For the heterodyne detection scheme, when the signal strength is lowered to simulate loss, the clearance to the electronic noise in recording Alice's modulation became smaller, increasing the mismatch to the measured signal, where this decreased clearance was insignificant because of the brightness of the carrier. Further, in Figure 7.5 the modulation variance was optimized for a given channel loss. This was not done in the experimental implementation.

While the statistical error bars on the data points are tiny, due to a sampling of 10^6 points, the inferred rates still deviate from the theoretical prediction. This is caused by channel parameter fluctuations that arise from systematic errors in the setup, such as fringe instability of locking circuit drifts. Thus, from point to point, the channel parameters are slightly different and the theory line represents the choice of parameter values that best fits this trend.

Concluding remarks

We have theoretically and experimentally demonstrated the security of a CVQKD scheme which is considerably simpler to implement than dual quadrature protocols. An important point made here is that encoding in conjugate bases is not a requirement for security. What is a requirement is that the encoded states are not orthogonal, which is trivially the case when the alphabet consists of coherent states, as shown by Equation (2.6.3).

The security of the single quadrature scheme was investigated against a collective asymmetric cloner attack in the asymptotic limit with preparation noise, and the security was demonstrated through purification assumptions on data obtained from implementations of the protocol with heterodyne and homodyne detection schemes. We find that the protocol is more sensitive to excess noise, but does provide security for certain parameter ranges. An outlook for this protocol is a genuine fiber implementation at 1550 nm, to investigate how low the excess noise can become.

Information Leakage in Lossy Quantum Information Channels

Introduction

In this work we consider a conventional point-to-point protocol where Alice and Bob exchange coherent states. When Eve intercepts information from the quantum channel shared by Alice and Bob, she will generate correlations between all parties. These correlations are what reduce the rate of the secret key generation. The purpose of post-processing and privacy amplification is to so to speak filter out the compromised data [62, 63]. It does this by suppressing the correlations between the honest and dishonest parties [31, 70]. This technique only works if the secret key rate, predicted through the Devetak-Winter bound from Equation (2.14.33), is already positive, i.e. $R > 0$. Alternatively the correlations can be suppressed by using entanglement based protocols, where the honest parties distill their entanglement [30, 46, 174]. The quantum channel forces the entangled state ideally shared by Alice and Bob to be a tripartite entangled state between Alice, Eve and Bob. To ensure security the state should be purified to a two-party entangled state shared by Alice and Bob. This will completely eliminate the correlations with Eve, but there exists a no-go theorem stating that non-Gaussian operations are required for this [78, 79, 80].

The purpose of the protocol presented here is to provide a different approach to reducing the correlations with the eavesdropper, without using either post-processing or non-Gaussian operations. While this seems to be as strong as an entanglement distillation operation, it only works for a very specific type of attack, and so there is no conflict with the no-go theorem, since we can not use our approach to reach the same level of security. We achieve this reduction in eavesdropper correlations by designing the input states used by Alice in such a way that Eve is unable to extract any information from the quantum channel. While it has already been established that modulated squeezed state alphabets are superior for certain parameters [53, 97], we show that if Alice prepares a squeezed state and selects her coherent state alphabet in a way constrained by the squeezing she can force the Holevo information of Eve to go to zero if the quantum channel is purely lossy.

The subtleties in the security proof of the single quadrature quantum key distribution of Chapter 7 are largely ignored here. We stress that the purpose of this work is not to demonstrate a fully working, absolutely bulletproof security proof for this variation on squeezing based QKD [42, 43, 44, 45, 53]. Instead we wish to emphasize that, under the specific assumptions made, it is possible to decouple Eve from the quantum channel using simple Gaussian operations, and that this effect seems to have no analogue in the DV regime. The theoretical part of this work is largely the product of the efforts of Vladyslav Usenko and Radim Filip. This work is published in pre-print [175].

Theory

We consider a protocol where the standard Gaussian distributed state alphabet is encoded in the Q quadrature, exactly like the single quadrature protocol described in Chapter 7. The difference is that the initial state that is being modulated is not a vacuum, but a squeezed vacuum state, which is squeezed in the Q quadrature. Instead of a coherent state alphabet, we therefore rather have a squeezed state alphabet along a single direction in phase space, namely the direction of the squeezing quantum noise reduction. In the EPR based scheme we have the initial state, before the channel,

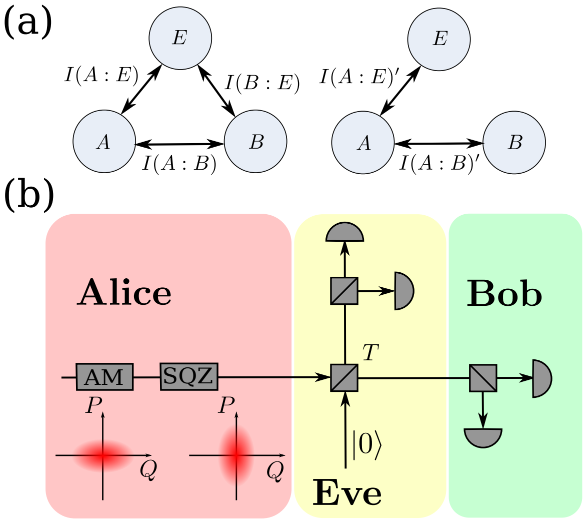


Figure 8.1: (a) Information quantities between the two honest parties and the eavesdropper. The decoupling eliminates the information content between Bob and Eve. (b) Illustration of the zero information leakage scheme. A distribution of squeezed states along the squeezing direction is prepared such that the overall variance is equivalent to the shot noise. Eve controls a purely lossy channel, and Bob performs a homodyne detection. Eve also uses homodyne detection for her measurements. In practice the modulator was before the squeezer to minimize loss on the squeezing. The operations of squeezing and displacement do not commute, but this trivially corrected for through a suitable parameter change.

$$\mathbf{\Gamma}_{\text{in}} = \begin{bmatrix} \mu & 0 & \sqrt{V(\mu^2-1)} & 0 \\ 0 & \mu & 0 & -\sqrt{\frac{\mu^2-1}{V}} \\ \sqrt{V(\mu^2-1)} & 0 & V\mu & 0 \\ 0 & -\sqrt{\frac{\mu^2-1}{V}} & 0 & \frac{\mu}{V} + V_\varepsilon \end{bmatrix} , \tag{8.2.1}$$

where μ is the EPR variance, V is the variance of an auxiliary squeezing operation on the outgoing mode, and V_ε is an extra variance contribution that arises from excess anti-squeezing, rendering the global state non-pure. Purification assumptions and the use of self-duality, derived in Section 2.14, are not necessary to show the idea of this protocol, and so this will not be a concern. μ and V are related to the prepare-and-measure parameters such that,

$$V\mu = V_{\text{sqz}} + V_{\text{sig}} \qquad , \qquad \frac{\mu}{V} = \frac{1}{V_{\text{sqz}}} , \tag{8.2.2}$$

where V_{sqz} is the squeezing variance and V_{sig} is the variance of the continuous Gaussian alphabet in the prepare-and-measure scheme. V_ε corresponds directly to the excess anti-squeezing in both frameworks. In this way this input state is equivalent to the prepare and measure protocol where we only encode information in Q, but unlike in Chapter 7, the alphabet consists of a 1D distribution of squeezed states. This distribution of states is transmitted through the quantum channel, and after the channel Bob uses homodyne detection for his measurement. Assuming that Eve implements the usual entangling cloner attack through a lossy and noisy quantum channel, we have the state shared by Alice and Bob after the channel as,

$$\mathbf{\Gamma}_{AB} = \begin{bmatrix} \mu & 0 & \sqrt{TV\tilde{\mu}} & 0 \\ 0 & \mu & 0 & -\sqrt{\frac{T\tilde{\mu}}{V}} \\ \sqrt{TV\tilde{\mu}} & 0 & TV\mu + (1-T)W & 0 \\ 0 & -\sqrt{\frac{T\tilde{\mu}}{V}} & 0 & T\left(\frac{\mu}{V} + V_\varepsilon\right) + (1-T)W \end{bmatrix} , \tag{8.2.3}$$

where we have defined the parameter $\tilde{\mu} = \mu^2 - 1$. The state shared by Eve and Bob is,

$$\mathbf{\Gamma}_{BE} = \begin{bmatrix} \boldsymbol{B} & \boldsymbol{C}_{EB} \\ \boldsymbol{C}_{EB}^T & \boldsymbol{E} \end{bmatrix} , \tag{8.2.4}$$

where we, with $\tilde{W} = W^2 - 1$, have the blocks,

$$\boldsymbol{B} = \begin{bmatrix} TV\mu + (1-T)W & 0 \\ 0 & T\left(\frac{\mu}{V} + V_\varepsilon\right) + (1-T)W \end{bmatrix} \tag{8.2.5}$$

$$\boldsymbol{E} = \begin{bmatrix} (1-T)V\mu + TW & 0 & \sqrt{T\tilde{W}} & 0 \\ 0 & (1-T)\left(\frac{\mu}{V} + V_\varepsilon\right) + TW & 0 & -\sqrt{T\tilde{W}} \\ \sqrt{T\tilde{W}} & 0 & W & 0 \\ 0 & -\sqrt{T\tilde{W}} & 0 & W \end{bmatrix} \tag{8.2.6}$$

$$\boldsymbol{C}_{EB}^T = \begin{bmatrix} -\sqrt{T(1-T)}(V\mu - W) & 0 \\ 0 & -\sqrt{T(1-T)}\left(\frac{\mu}{V} + V_\varepsilon - W\right) \\ \sqrt{(1-T)\tilde{W}} & 0 \\ 0 & -\sqrt{(1-T)\tilde{W}} \end{bmatrix} , \tag{8.2.7}$$

which are 2 × 2, 4 × 4, and 4 × 2 respectively. From this result we find that the correlations between Eve and Bob in the Q quadrature are determined by the expression,

$$\boldsymbol{C}_{EB,11} = -\sqrt{T(1-T)}(V_{\text{sqz}} + V_{\text{sig}} - W) \ , \tag{8.2.8}$$

as expressed in terms of the prepare-and-measure parameters. For a purely lossy channel, we have $W = 1$ and so the correlation parameter becomes,

$$\boldsymbol{C}_{EB,11} = -\sqrt{T(1-T)}(V_{\text{sqz}} + V_{\text{sig}} - 1) \ . \tag{8.2.9}$$

From this we see that the requirement for Eve to be correlated to Bob is that $V_{\text{sqz}} + V_{\text{sig}} = 1$. As in Chapter 7, Bob will have to monitor both quadratures, so he needs to change his measurement to be in the P quadrature for at least some of the channel uses. The reconciliation procedure [67, 71] can, as usual, be either direct or reverse, but for reverse reconciliation the correlation parameter $\boldsymbol{C}_{EB,11}$ is what determines the information leakage to Eve. For direct reconciliation we can not realize a similar condition.

Figure 8.1(a) shows a schematic for the cancellation of the information leakage from the quantum channel. In general, for any protocol, the classical quantities $I(A:B)$, $I(A:E)$ and $I(E:B)$ are non-zero. When Eve is uncorrelated with Bob we achieve $I(E:B)' = 0$, but more surprisingly we also achieve $\chi(E:B)' = 0$. Therefore, using reverse reconciliation Alice and Bob can decouple Eve from the quantum channel if she can only perform the simple pure loss attack as seen in Figure 8.1(b). It should be emphasized that Eve is only decoupled from the classical information encoded onto the states. Her quantum mutual information will be non-zero unless the quantum channel receives a vacuum state from Alice. Further, for a direct reconciliation scheme, Eve can never be completely decoupled from the classical information unless there is no loss or noise. Interestingly, for reverse reconciliation, this phenomenon of decoupling is independent of the transmission loss, which means that the reduction of the rate generation simply follows the reduction of the mutual information between Alice and Bob. We also show that this does not depend on the purity of the squeezed state.

We show the properties of Eve's Holevo information by directly computing it through the formula given in Equation (2.14.32). For a purely lossy channel Eve's auxiliary mode is a vacuum mode and so it may be safely disregarded. Letting Bob perform homodyne detection in Q, we see that the conditional state $\mathbf{\Gamma}_{E|B}$ is given by,

$$\mathbf{\Gamma}_{E|B} = \begin{bmatrix} (1-T)V\mu + T - \frac{T(1-T)(1-V\mu)^2}{TV\mu - T + 1} & 0 \\ 0 & (1-T)\left(\frac{\mu}{V} + V_\varepsilon\right) + T \end{bmatrix} . \qquad (8.2.10)$$

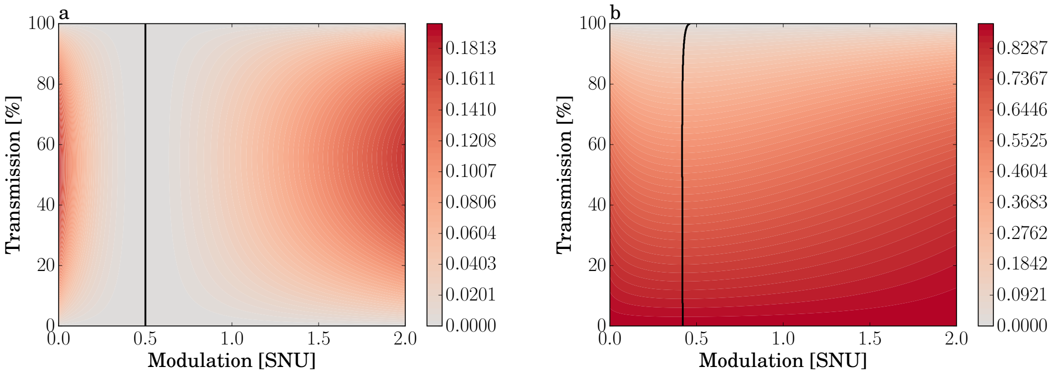


Figure 8.2: (a) Contour plot of Holevo information against transmission and modulation variance, with $V_{\text{sqz}} = 0.5$ SNU. The solid black line indicates where the Holevo quantity is minimized. (b) Contour plot of Holevo information against transmission and modulation variance, with $V_{\text{sqz}} = 0.5$ SNU, but with $W = 1.5$ SNU. The solid black line indicates the minimum value of the Holevo information.

With an expression for this conditional state we can computing the Holevo quantity is relatively straightforward. We see from Equation (2.14.32) that the requirement for $\chi(E : B) = 0$ is equivalent to $S_E = S_{E|B}$. Because the states are Gaussian, we know that these entropies are determined by the symplectic spectra of the respective covariance matrices. Therefore, the covariance matrices need to have the same symplectic eigenvalues to enforce the condition. However, since Bob performs homodyne detection, only the measured quadrature is conditioned. We can therefore simplify the condition to be $\mathbf{\Gamma}_{E,11} = \mathbf{\Gamma}_{E|B,11}$ where the additional subscript indexes the covariance matrix. One way to fulfil this is to introduce detection noise at Bob into the calculation, and let this detection noise go to infinity. This noise contribution will then enter into the conditional entropy. This will have $I(A : B)$ go asymptotically to zero as the noise goes to infinity, though there is known to be an optimal amount of detection noise for reverse reconciliation [169]. Another way to fulfil the condition is to have $V_{\text{sqz}} + V_{\text{sig}} = 1$, which confirms our intuition that eliminating the correlations suffice to decoupling the eavesdropper from the encoded signal. We see from this expression that the alphabet size should be determined by $V_{\text{sig}} = 1 - V_{\text{sqz}}$. This result also confirms the independence on squeezing purity and channel loss, as they

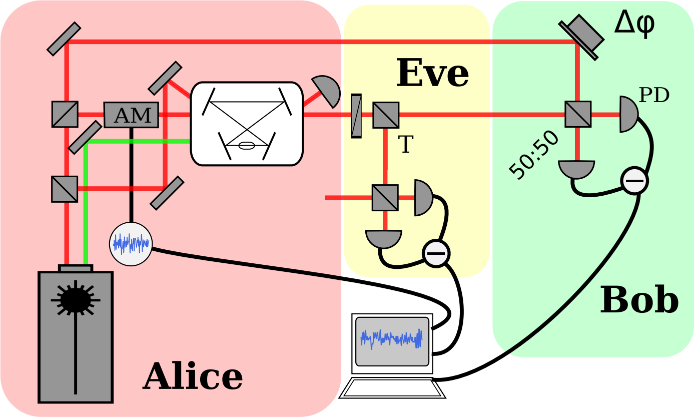


Figure 8.3: Sketch of the setup that implements an alphabet of squeezed states. Alice prepares her asymmetrical thermal state through an amplitude modulator, and squeezes this state. The output is sent through a purely lossy quantum channel of transmission T controlled by Eve who measures the tap-off using quadrature switched homodyne detection. The transmission through the quantum channel is measured by Bob who also uses quadrature switched homodyne detection. The measured signals are correlated with Alice's input alphabet, recorded by an analog-to-digital converter. AM: Amplitude modulator, PD: Photodetector.

are included in Equation (8.2.10).

Figure 8.2 shows contour plots of the Holevo information $\chi(E:B)$ in terms of modulation variance and channel transmission, when $V_{\text{sqz}} = 0.5$ SNU. The solid black line indicates where the Holevo quantity is minimized. In Figure 8.2(a) we see that the minimization condition is independent of transmission and that the Holevo information is exactly zero when $V_{\text{sig}} = 0.5$ SNU. Figure 8.2(b) extends the analysis to the case where Eve injects noise into the quantum channel, such that $W = 1.5$ SNU. Here, the minimization condition is transmission dependent, and indeed also heavily dependent on W. We also see that complete decoupling of the eavesdropper from the quantum channel is not possible in this generalized entangling cloner scenario.

Experiment

We implemented a purely lossy channel and an alphabet of displaced squeezed states. The setup is sketched in Figure 8.3.

Experimentally, Alice prepared her state by squeezing an asymmetric thermal state, where the P quadrature had a variance of 1 shot noise unit (SNU), and Q had a variance varied around the condition $V_{\text{sig}} + V_{\text{sqz}} = 1$. The thermal state was generated by an electro-optical amplitude modulator driven by a noise generator that was white within the measurement bandwidth. The modulator modulated sidebands at 4.9 MHz, with a 90 kHz bandwidth. This thermal state represented an alphabet of coherent states. The generator output was recorded to be correlated with Bob's and Eve's measurements in post-processing to establish correlations between the parties.

The prepared ensemble of coherent states was injected into the bowtie cavity described in Section 3.5.1, with a pumped PPKTP crystal functioning as the non-linear element of an optical parametric amplifier, squeezing the Q quadrature. While this ordering of displacement and squeezing is not equivalent to squeezing before displacement, a suitable change of parameters can make the state production equivalent. The modulation was chosen to be before the squeezing to minimize loss on the squeezed state, since the loss on the modulation induced by the cavity coupling can be rescaled such that the modulation after the squeezer is regarded as the signal. The PPKTP crystal was driven with a 532 nm pump, and we achieved 3 dB of sub shot noise squeezing. The alphabet modulation was varied around this point to test the behaviour of the decoupling. The modulated squeezed state was also exposed to various transmissions before being detected at a homodyne detector by Bob. The tap-off was directed to a quadrature switched homodyne detector that represented Eve.

The modulation depth of the asymmetric thermal state was chosen such that the overall variance corresponded to one unit of shot noise. The transmission loss of the lossy quantum channel was implemented through a wave plate and beam splitter combination. Eve's homodyne detector had an overall efficiency of 95 %, while Bob had an overall efficiency of 85 %, mostly due to limited diode efficiencies. Both Eve and Bob measured both quadratures P and Q, for different combinations of channel loss and alphabet size. The photocurrents generated by the photo detectors were mixed down from their 4.9 MHz sidebands, low-pass filtered at 90 kHz and digitized on a 14 bit depth data acquisition card. The data sets were normalized to shot noise in post-processing. The classical signal recorded for Alice was scaled appropriately in post-processing, to optimize the correlations between Alice and Bob. For each parameter combination this allowed us to reconstruct a 6×6 covariance matrix, that completely characterized the global state. This reconstruction was achieved by calculating the second order moments of the recorded data, and the corresponding covariances between the appropriate parties, essentially calculating the elements of a matrix similar to the one in Equation (2.4.8). From this matrix the Holevo and Shannon information quantities were easily calculated following the recipe outlined in Section 8.2.

Figure 8.4 shows the results for the calculated Holevo information, with corresponding theoretical estimates for the given channel parameters. We clearly see elimination of the Holevo information when $V_{\text{sig}} = -3$ dB, which directly fulfils the condition $V_{\text{sqz}} + V_{\text{sig}} = 1$ SNU, since the squeezer produced 3 dB squeezing. Figure 8.5 shows the data for the secret key rate plotted against modulation variance.

The Holevo information is minimized at $V_{\text{sig}} = -3$ dB, but the rate is not maximized for this modulation depth. This is because the mutual information between Alice and

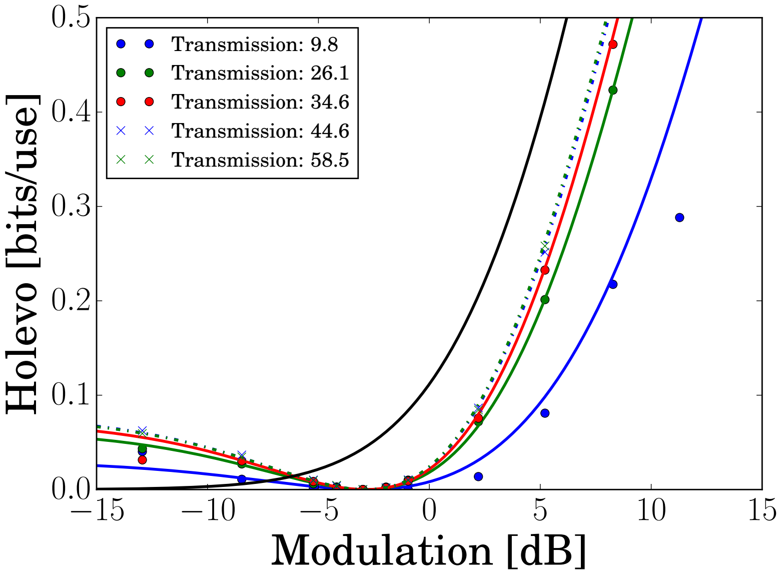


Figure 8.4: Plot of the Holevo information versus modulation, with different lines representing theoretical rates for different transmission values, and their corresponding data points. These results are compared to the expected results from a normal coherent state protocol with 58% transmission, represented by the black solid line. Modulation depth is in units of dB relative to shotnoise.

Bob initially goes up faster for increasing modulation than the Holevo information does. There is therefore an optimal choice for V_{sig} higher than set by the condition $V_{\text{sqz}} + V_{\text{sig}} = 1$, and this value will depend on the reconciliation efficiency β. The lower the value of β, the more the rate favours eliminating $\chi(E:B)$ completely, rather than having a larger alphabet. In general, when the Holevo bound becomes zero, we can ensure that $R > 0$ quite easily because $I(A:B)$ goes to zero asymptotically with channel loss, as long as $\beta \neq 0$. Thus, it should always be possible to extract a secure key under these conditions, provided of course that Eve is limited to the pure loss attack and the asymptotic rate limit assumption can be justified. In this case we do not, however, consider the additional complication of the correlation parameter from Chapter 7, since we assume a purely lossy channel with quadrature symmetric transmissions.

Concluding remarks

This work theoretically and experimentally demonstrated that not only can one achieve security by generating an alphabet of squeezed states, it can outperform a coherent state protocol with identical parameters. Indeed, for purely lossy quantum channels, a properly chosen modulation depth can completely eliminate the information leakage that typically takes place in the quantum channel as it mixes Alice's outgoing mode with the eavesdropper mode.

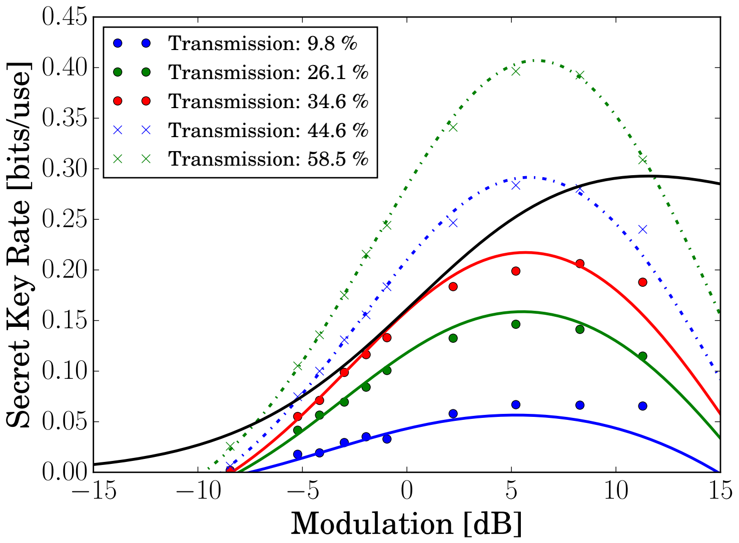


Figure 8.5: Plot of the key rate versus modulation, with different lines representing theoretical rates for different transmission values, and their corresponding data points. These results are compared to the expected results from a normal coherent state protocol with 58% transmission, represented by the black solid line. Modulation depth is in units of dB relative to shotnoise. $\beta = 0.95$.

We confirm these predictions experimentally with a setup producing 3 dB squeezing and homodyne detection at Bob and the eavesdropper. This is the first demonstration of a complete deterministic decoupling of the eavesdropper from the classical encoding in the quantum channel without the use of entanglement distillation, in other words using purely Gaussian operations. The decoupling is independent of channel loss and squeezing purity.

Combining this protocol with a simple Gaussian error correction protocol such as [156] to remove non-Markovian excess noise, could potentially extend the range of the protocol, in the cases where the assumption of a purely lossy channel can not be satisfied.

Practical Quantum Computing on Encrypted Data

Introduction

This work is inspired by the concept of homomorphic encryption from the world of classical information theory [176]. The idea of homomorphic encryption, and what conditions are necessary to achieve it, was first worked out by Rivest et. al. [177]. Homomorphic encryption is concerned with the encryption of sensitive data, where one wants an untrusted party to be able to manipulate the information, for example by indexing, sorting or searching in vast amounts of data, while keeping the data secret from this untrusted party. In other words, the untrusted party, or server, should be able to evaluate a function on the data, without knowing the plaintext of the data. An algorithm for how to achieve this encryption was first developed by Craig Gentry in 2009 [178]. This is useful in the context of cloud computing, where privacy concerns are increasingly prevalent. As an example, it would allow for searching using the Google search engine, without Google knowing the plaintext search term supplied by a client.

Generalizing this homomorphic encryption in the context of quantum information theory is an interesting prospect. It has been shown to be possible to hide a constant fraction of the information, with polynomial overhead in terms of the amount of data, provided that the performed quantum operations are limited to a certain class [179]. On the other hand, deterministic fully homomorphic quantum computing, that offers information theoretical security, has been shown to require exponential overhead [180].

Allowing multiple rounds of communication between the server and the client can relax this requirement. Childs [181] developed the idea of delegated quantum computation, where we consider a server that is able to implement universal quantum computing, and a client who wants access to these capabilities, but who does not trust the server. The idea is to for the client to hide some combination of the input state, the program she wants to run on the quantum computer and the output. The idea of delegated quantum computing has been embraced by IBM in a recent initiative [182].

Using cluster states Broadbent *et al.* [183] developed this idea further, coining the term universal blind quantum computing. This is a protocol that can hide all three of the previously mentioned items. The only requirement put on the client is that she is able to prepare single qubits from a certain simple set. This original idea has since been developed significantly [184, 185, 186, 187, 188, 189, 190].

Intuitively, one would expect to be able relax these requirements if, for example, the program did not need to be hidden from the server. This intuition was confirmed by Fisher *et al.* [191], where it was demonstrated that pre-existing agreement on what program to implement lowers the amount of classical and quantum information to be exchanged during the actual protocol. This relaxed version of universal blind quantum computing is called quantum computing on encrypted data, and this is the protocol that we wish to implement. However, unlike previous work, we are interested in doing this with continuous variable states, which in principle allows for universal quantum computing [192]. However, restricting ourselves to Gaussian operations, we can not achieve universality [193]. The theoretical work presented here is due to the efforts of Kevin Marshall and Christian Weedbrook. The theoretical developments as well as the experimental implementation are published in pre-print [194].

Theory

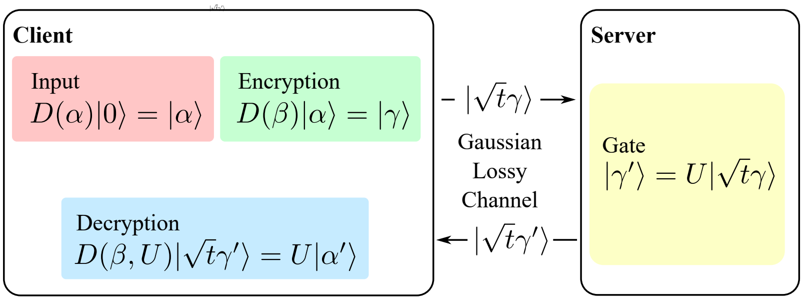

Client
Input
$D(\alpha)|0\rangle = |\alpha\rangle$
Encryption
$D(\beta)|\alpha\rangle = |\gamma\rangle$
Decryption
$D(\beta,U)|\sqrt{t}\gamma'\rangle = U|\alpha'\rangle$
$|\sqrt{t}\gamma\rangle$
Gaussian
Lossy
Channel
$|\sqrt{t}\gamma'\rangle$
Server
Gate
$|\gamma'\rangle = U|\sqrt{t}\gamma\rangle$

Figure 9.1: Scheme illustrating the protocol for quantum computing on encrypted data. The input is an ordinary coherent state. The encryption procedure is a random displacement operator on the initial state. The quantum channel connecting the client and the server is a purely lossy channel. After the channel, the server applies the gate, in this case a displacement gate. The output is sent through the same quantum channel back to the client, who recovers the actual output by performing the decryption operation.

The protocol for quantum computing on encrypted continuous variable states takes place in four stages, see Figure 9.1.

1. **State preparation**. The client prepares her input states that she wishes to put through the quantum computation.

2. **Encryption**. The client encrypts her input state by displacing it in phase space by some random amount. This limits the amount of information available to the server.

3. **Program**. The server receives the encrypted input state from the quantum channel. It performs an operation representing one or several gates from the universal set $\mathcal{G}$, to be defined further in Equation (9.2.2), and sends the output of this back through the quantum channel.

4. **Decryption**. The client applies a decryption operation that depends on the program implemented by the server. This recovers the intended output.

We use the Weyl operator defined in Equation (2.4.1) as the encryption operation. Consider an alphabet of coherent states as an input to the universal quantum computer. Each coherent state represents a letter in this alphabet. Displacing the input state randomly transforms the input into a different letter, and so hides the actual input. On average, these random displacements over the entire phase space will make the input look like a thermal state, since,

$$\frac{1}{\pi}\int_{\mathbb{R}^2} \hat{D}(\boldsymbol{X})|\psi\rangle\langle\psi|\hat{D}^{\dagger}(\boldsymbol{X})\mathrm{d}^2\boldsymbol{X} = \mathbb{I} \ , \tag{9.2.1}$$

where $\boldsymbol{X} = (Q, P)^T$, and the identity holds as long as the input state $|\psi\rangle$ is normalized. This means that on average, the quantity produced by the encryption operation is proportional to the identity, and so is fully mixed. However, such a uniform distribution of displacements over the entire phase space is not possible to realize physically, since we are limited in how large displacements we can make. Instead, we choose a Gaussian distribution, because, as we have seen in Section 2.13, a Gaussian distribution maximizes the entropy out of all the probability distributions with the same covariance matrix, which is equivalent to assuming some physical energy threshold. Intuitively, maximizing the entropy is exactly what is necessary to hide the input state, because higher entropy implies that the server is less correlated with the encrypted input states.

This will limit the security of the scheme in the sense that it will depend on the width of the Gaussian distribution used for the encryption operation. This width should therefore be as high as possible under the technical constraints encountered in the implementation, i.e. we should have as high an energy threshold as is practically feasible. Formalizing this security analysis to show in what sense it offers security and how well it does this in an experimental setting where displacements are finite is an open problem that we will not attempt to solve in the present work.

We now wish to show that this protocol can decrypt outputs resulting from a universal quantum computation. To do this, we consider the universal set of quantum gates in the CV formalism [192],

$$\mathcal{G} = \{\hat{D}_Q(\Sigma), \hat{D}_P(\Sigma), \hat{U}_2(\Sigma), \hat{U}_3(\Sigma), \hat{F}, \hat{C}_Z\} \ , \tag{9.2.2}$$

where Σ is the relevant gate parameter. $\hat{D}_Q(\Sigma)$ and $\hat{D}_P(\Sigma)$ are the displacement gates,

$$\hat{D}_Q(\Sigma) = \exp(i\Sigma\hat{Q}) \qquad , \qquad \hat{D}_P(\Sigma) = \exp(-i\Sigma\hat{P}) \ . \tag{9.2.3}$$

$\hat{U}_k(\Sigma)$ is the k'th order phase gate,

$$\hat{U}_k(\Sigma) = \exp(i\Sigma\hat{Q}^k) \ . \tag{9.2.4}$$

$\hat{F}$ is the Fourier gate,

$$\hat{F} = \exp\left(\frac{i\pi}{4}\left(\hat{Q}^2 + \hat{P}^2\right)\right) \ , \tag{9.2.5}$$

and $\hat{C}_Z$ is the controlled phase gate,

$$\hat{C}_Z = \exp(i\hat{Q}_1 \otimes \hat{Q}_2) \ . \tag{9.2.6}$$

With this set it is possible to implement universal quantum computing in a CV setting [192]. We therefore wish to show that we can reliably decrypt outputs from all these operations. Of this set, only the gate $\hat{U}_3(\Sigma)$ is non-Gaussian [195, 196], and it turns out that one needs at least one non-Gaussian gate to achieve universal quantum computing [193].

Gate	Correction
$\hat{D}_Q(\Sigma)$	$\hat{D}_P(-Q)\hat{D}_Q(-P)$
$\hat{D}_P(\Sigma)$	$\hat{D}_P(-Q)\hat{D}_Q(-P)$
$\hat{U}_2(\Sigma)$	$\hat{D}_P(-Q)\hat{D}_Q(-2Q\Sigma - P)$
$\hat{U}_3(\Sigma)$	$\hat{D}_P(-Q)\hat{D}_Q(3Q^2\Sigma - P)\hat{U}_2(-3Q\Sigma)$
$\hat{F}$	$\hat{D}_P(P)\hat{D}_Q(-Q)$
$\hat{C}_Z$	$\hat{D}_{P,1}(-Q_1)\hat{D}_{Q,1}(-Q_2 - P_1) \otimes \hat{D}_{P,2}(-Q_2)\hat{D}_{Q,2}(-Q_1 - P_2)$

Table 9.1: Corresponding decryption operations for the single mode encryption operator $\hat{D}(\boldsymbol{X})$ and the two-mode encryption operator $\hat{D}_1(\boldsymbol{X}_1)\hat{D}_2(\boldsymbol{X}_2)$ for each gate in $\mathcal{G}$, where $\boldsymbol{X} = (Q, P)^T$.

The corresponding decryption operations for each gate are listed in Table 9.1. For all gates except $\hat{U}_3$, the decryption operation consists purely of displacements. Consider for example the $\hat{D}_Q(\Sigma)$ gate. Encryption for this gate is $\hat{D}(\boldsymbol{X})$, which can be separated into two operations such that $\hat{D}(\boldsymbol{X}) = e^{-\frac{i}{2}QP}\hat{D}_Q(P)\hat{D}_P(Q)$. Decomposed in this way we see that the $\hat{D}_Q(P)$ part obviously commutes with $\hat{D}_Q(\Sigma)$, and $\hat{D}_P(Q)$ commutes up to a phase shift such that

$$\hat{D}_P(Q)\hat{D}_Q(\Sigma) = e^{-iQ\Sigma}\hat{D}_Q(\Sigma)\hat{D}_P(Q) \ . \tag{9.2.7}$$

From this, the decryption $\hat{D}_C(Q,P,\Sigma)$ for the gate $\hat{D}_Q(\Sigma)$ is determined by the requirement that,

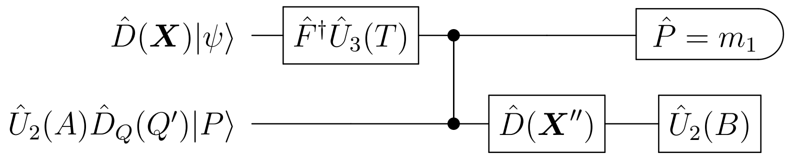
$$\hat{D}_Q(\Sigma)D(\boldsymbol{X}) = \hat{D}_C^\dagger(Q,P,\Sigma)\hat{D}_Q(\Sigma)\ . \tag{9.2.8}$$

Rearranging this we find that,

$$\hat{D}_C(Q,P,\Sigma) = \exp[i(QP/2 - Q\Sigma)]\hat{D}_P(-Q)\hat{D}_Q(-P)\ . \tag{9.2.9}$$

We see that the decryption depends on the encryption parameters Q and P, and that it further depends on the classical gate parameter Σ. We also confirm that this decryption can be realized by displacement alone, such that we do not need to assume that the client has quantum resources at her disposal.

Applying arguments similar to the above we may arrive at the results listed in Table 9.1 and we see that for the Gaussian gates the decryption operations are pure displacements. However, the above approach is not successful for the $\hat{U}_3(\Sigma)$ gate, since the commutation relations are more complicated. This also explains why this is the only gate that requires squeezing resources on the part of the client. If the client wants the server to execute $\hat{U}_3(\Sigma)$ she has to forward two modes, one containing the encrypted input state and the other the squeezed and displaced momentum eigenstate $\hat{U}_2(A)\hat{D}_Q(Q')|P\rangle$, with random parameters A and Q'. The server then implements $\hat{U}_3(\Sigma)$ using the teleportation circuit [10],


$\hat{D}(\boldsymbol{X})|\psi\rangle$
$\hat{F}^\dagger\hat{U}_3(T)$
$\hat{P}=m_1$
$\hat{U}_2(A)\hat{D}_Q(Q')|P\rangle$
$\hat{D}(\boldsymbol{X}'')$
$\hat{U}_2(B)$

The client sends the aforementioned two modes and the value B to the server. The server runs the circuit and measures one of the output modes with the outcome m_1, which needs to be communicated back to the client to allow her to correct for the encryption operation correctly. The correction operator the client needs to implement for the decryption of the $\hat{U}_3(\Sigma)$ gate output is,

$$\hat{D}_{C,\hat{U}_3}(Q,P,\Sigma) = \hat{D}_P(-Q)\hat{D}_Q(3Q^2\Sigma - P)\hat{U}_2(-3Q\Sigma)\ . \tag{9.2.10}$$

Similarly to the simple case of the displacement gates, we see that the decryption depends on the encryption parameters Q and P, and on the gate parameter Σ. However, unlike for the case of the displacement gate, the $\hat{U}_2$ gate now enters into the decryption operation. In addition to this, there is also the requirement that the server communicates the measurement outcome m_1 to the client. This requirement of an extra round of classical communication is essentially what causes this scheme to not be homomorphic. Interestingly, Dulek et al. [197] have considered a similar problem with the Clifford set of DV quantum computing gates and the T gate [198, 199], where the T gate needs special treatment to implement homomorphically encrypted delegated quantum computing. It is possible that the CV scheme described here could be extended in a similar fashion, but this too remains an open problem.

More complicated quantum operations in continuous variable quantum computing can be implemented by generating Hamiltonians that are polynomials of arbitrary order in $\hat{Q}$ and $\hat{P}$. This is possible by proper manipulation of the gates in the universal set [192, 200]. Thus, an arbitrary program can be approximated by a proper composition of gates [192]. The individual decryption operations that arise from the application of the individual gates can be pushed to the end of the composition of gates to form an overall decryption operator for the entire program, such that executing a program in this way does not require multiple uses of the lossy quantum channel, up to an overall change in phase due to the commutation relation between displacements in P and Q. This is possible because of the simple nature of the decryption operations. Many of the gates in the universal set have been realized [201, 202, 203, 204]. Of these the non-Gaussian gates are the most challenging and their implementation is outside the scope of this thesis.

Experiments

Encryption efficiency

We experimentally implement the CV quantum computing gates $\hat{D}_P(\Sigma)$ and $\hat{D}_Q(\Sigma)$. We also implement a squeezing operation on a displaced state which is equivalent to the $\hat{U}_2(\Sigma)$ gate up to a phase shift.

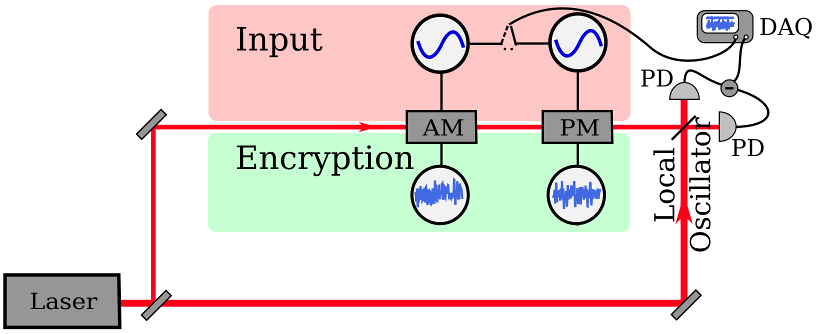


Figure 9.2: Two electro optical modulators are used to modulate the phase and amplitude quadratures. They are driven by two sets of independent Gaussian white noise generators. The modulators output an alphabet of encrypted coherent states at a 10.5 MHz sideband, which is demodulated and digitized by a data acquisition card. PD: Photo Detectors, AM: Amplitude modulator, PM: Phase modulator, DAQ: Data acquisition.

We first investigate the efficiency of the encryption, using the setup sketched in Figure 9.2. The client initially generates a Gaussian distribution of coherent states of light, as defined in Section 2.6, to store quantum information. This is done using electro-optical modulators, and on average it produces the ensemble,

$$\hat{\rho}_{\mathrm{in}} = \int_{\mathbb{R}^2} G_{\mathrm{in}}(\boldsymbol{X})\hat{D}(\boldsymbol{X})|0\rangle\langle 0|\hat{D}^{\dagger}\boldsymbol{X}\mathrm{d}^2\boldsymbol{X} \ , \tag{9.3.1}$$

distributed according to the Gaussian distribution $G(\boldsymbol{X})$ with the variance V_{in} in both quadratures. This distribution is generated by two independent white noise generators. The input states were encrypted by adding another Gaussian distribution of displacements through the same modulators, but with independent Gaussian noise generators, with symmetric variance V_{enc}. The state ensemble after the encryption therefore becomes,

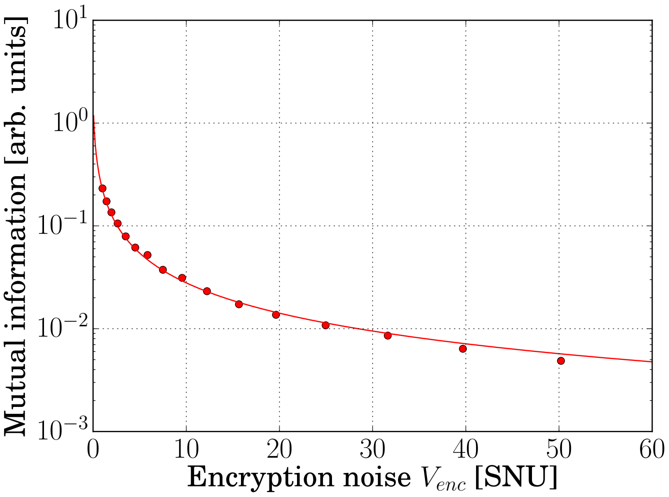


Figure 9.3: A plot of the mutual information $I(\mathrm{server}_{\mathrm{enc}}\!:\!\mathrm{client}_{\mathrm{in}})$ between the server and the client for a Gaussian alphabet of coherent states with variance $V_{\mathrm{in}} = 0.6$ SNU, versus encryption variance V_{enc}. If the alphabet size stays constant, an increase in encryption variance will decrease the information between server and client. The statistical error bars are smaller than the point size.

$$\hat{\rho}_{\mathrm{enc}} = \int_{\mathbb{R}^2} G_{\mathrm{enc}}(\boldsymbol{X})\hat{D}(\boldsymbol{X})|0\rangle\langle 0|\hat{D}^{\dagger}(\boldsymbol{X})\,\mathrm{d}\boldsymbol{X} \ , \tag{9.3.2}$$

which in phase space is described by the Gaussian $G_{\mathrm{enc}}(\boldsymbol{X})$ with the total symmetric variance $V_{\mathrm{in}} + V_{\mathrm{enc}}$. These encrypted quantum state were measured by the server with homodyne detection. The Gaussian distribution generating the input states was recorded, to be correlated with the server measurement outcomes. These correlations determine the classical mutual information, defined in Section 2.13, between the server and the client and the information content available to the server should follow the expression,

$$I(\mathrm{server}_{\mathrm{enc}}\!:\!\mathrm{client}_{\mathrm{in}}) = \frac{1}{2}\log_2\left(1 + \frac{V_{\mathrm{in}}}{V_{\mathrm{enc}}}\right) \ . \tag{9.3.3}$$

The results of this investigation are shown in Figure 9.3. Ideally, $I(\text{server}_{\text{enc}}:\text{client}_{\text{in}})$ should go to zero, which only happens in the limit where $V_{\text{enc}} \to \infty$. In practice, what we require is that the encryption variance is much larger than the alphabet size, $V_{\text{enc}} \gg V_{\text{in}}$.

Displacement gates

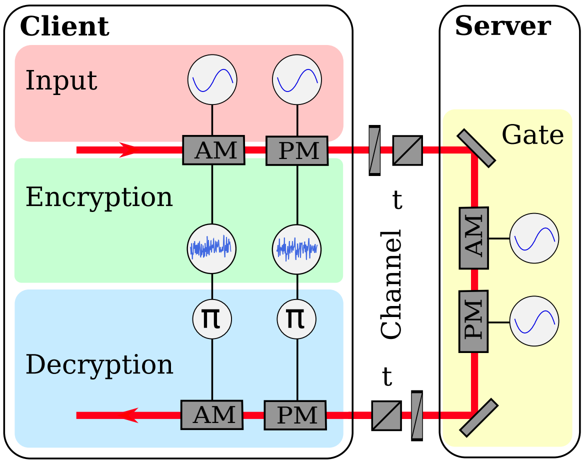


Figure 9.4: Experimental setup for the implementation of encrypted computing with displacement gates. The modulators prepared an ensemble of encrypted input states using two electro-optical modulators each fed by two uncoupled Gaussian white noise generators. The prepared encrypted states were sent to the server through a lossy quantum channel with transmission T, which was implemented through a waveplate and polarising beamsplitter combination. After the channel the server implemented $\hat{D}_Q$ and $\hat{D}_P$ gates. The server implemented an ensemble of displacement gates, using another pair of modulators with uncoupled Gaussian white noise generators. These displaced quantum states were sent back through the lossy quantum channel with transmission T. The client decrypted these returned states using a phase shifted signal from the initial encryption noise generator. AM: Amplitude modulator, PM: Phase modulator.

The setup where the server implements both displacement gates is shown in Figure 9.4. The client split a 1064 nm seed beam into two parts, designated as signal and LO respectively. The LO went immediately to the homodyne detector controlled by the client.

Two electro-optical modulators at the client side prepared the encrypted input states on the signal beam. This was done through a phase and an amplitude modulator, which each received two uncorrelated noise inputs. One of these noise signals represened the continuous alphabet the client uses to encode her quantum information. The other noise signal represented the encryption noise. Both noise signals were white within the measurement bandwidth of 1 MHz around the 10.5 MHz sideband. The input states consisted of a Gaussian alphabet with variance $V_{\text{in}} = 0.3$ SNU, with

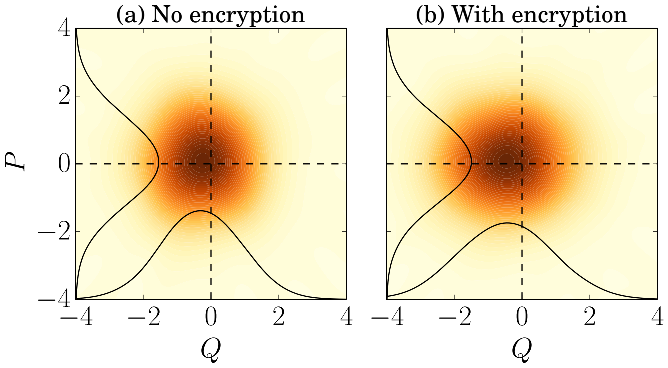


Figure 9.5: Wigner functions for the delegated displacement gate output, (a) without encryption and (b) with an encryption of $V_{\text{enc}} = 31$ SNU and subsequent decryption. The input state ensemble had the variance $V_{\text{in}} = 0.3$ SNU and the gate operation adds an additional distribution with variance $V_{\text{gate}} = 0.6$ SNU.

$V_{\text{enc}} = 31$ SNU of encryption noise on top. With this ratio between input and encryption, we expect the server to be able to recover $I = 0.005\,\text{bits/use}$ of information. Figure 9.6(a) shows the signal-to-noise ratio for each protocol step. The purely lossy quantum channel between the client and the server was implemented through a beam splitter and wave plate combination, which gave an effective transmission T through the channel. Because this experiment only dealt with coherent states, the intrinsic loss at the client and the server was scaled out, and loss was assumed to only occur in the quantum channel.

When the states arrived at the server, another pair of electro-optical modulators implemented $\hat{D}_Q$ and $\hat{D}_P$ gates with the gate parameters chosen by a white noise signal. In this way the experiment tested an ensemble of gate parameters, and so the server also implemented a symmetric Gaussian distribution of displacements with variance $V_{\text{gate}} = 0.6$ SNU. The overall state after the gate operation therefore had the variance $V_{\text{gate}} + V_{\text{in}} + V_{\text{enc}}$ for a lossless channel.

On the return trip to the client, the gate output states were sent through a lossy quantum channel with the transmission T. A last pair of electro-optical modulators was located at the client receiver, where the client applied a phase shifted encryption operation, exactly anti-correlated to the encryption signal, to recover the decrypted output of the server's quantum computation, before this output was measured by a homodyne detector. Ideally, the client should recover the state $\hat{D}_Q(P)\hat{D}_P(Q)|\phi\rangle$. However, imperfections in the decryption procedure in fact gave her an output state with variance $V_{\text{in}} + V_{\text{gate}} + V_{\text{res}}$. The residual noise also followed a Gaussian distribution, and was measured to be $V_{\text{res}} = 0.072$ SNU. This high degree of noise cancellation was enabled by a custom noise generator, where the outputs for the encryption and decryption were highly correlated at the sideband frequency in question. Further, the relative phase between these signals was essential for proper noise cancellation. To control this phase a DB64 Coax Delay Box from Stanford Research Systems was inserted in the connection between the noise generator and the decryption modulator.

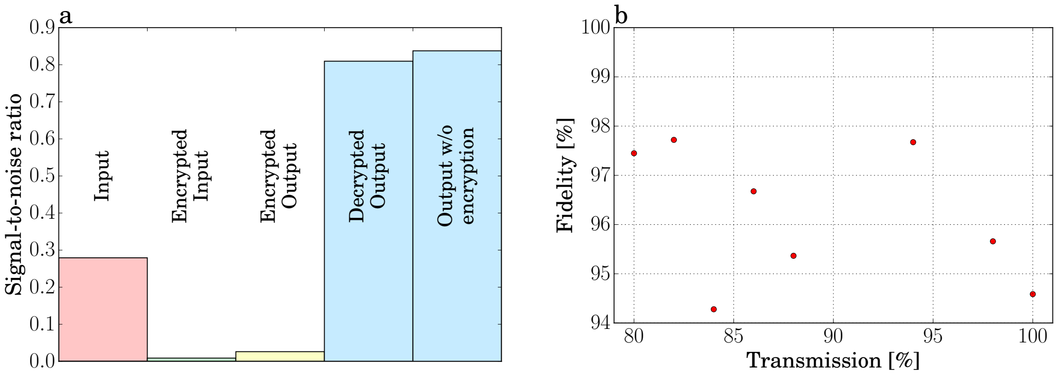


Figure 9.6: (a) Signal-to-noise ratio from the point of view of the server, for each step of the protocol. Each step is measured with homodyne detection. The channel is calibrated such that $T = 1$, and an ensemble of coherent input states was prepared. The green stage shows the reduced SNR for the encrypted input state. The server performs a displacement in the yellow stage, which increases the SNR. This state is returned to client who decrypts it to receive the output with increased SNR in the blue stage. The upper trace in the last step is a measurement without the encryption routine, which has an increased SNR because the decryption operation slightly degrades the output. The input state, which has a small amplitude relative to the encryption is prepared in the red stage. (b) Plot of the fidelity between the output states generated using the encrypted input state and the output states generated from plain-text states, as a function of channel transmission T. Statistical error bars are smaller than the point size. The fidelity variations arise from systematic errors in the tuning of the relative phase between the encryption and decryption operations, which limits the efficiency of the decryption.

After the decryption, the client performed scanned homodyne detection, with a visibility of 92 %. The low visibility was primarily caused by the 6 modulator crystals distorting the beam profile relative to the local oscillator. The homodyne detection output was mixed down from the 10.5 MHz sideband and sent to an analog-to-digital converter after being low-pass filtered at 1 MHz to set the measurement bandwidth. The acquired marginal distributions were then put through the maximum likelihood algorithm described in Section 3.8, in order to reconstruct the respective density matrices.

The Wigner functions from the ensemble states reconstructed with and without encryption are shown in Figure 9.5. In order to better quantify the performance of the decryption, Figure 9.6(a) shows the SNR for the different protocol stages and Figure 9.6(b) shows the fidelity between the output generated by the encrypted ensemble of input states and the unencrypted ensemble of input states. The fidelity was calculated using Equation (2.3.6), where $\hat{\rho}_0$ was the ideal output state without encryption and subsequent decryption and $\hat{\rho}_1$ was the result of the protocol. Thus, the fidelity measure exactly quantifies how well the decryption could be performed, without referencing the performance of the gate or the channel. For the tested channel transmissions, the fidelity stays above 94 %.

Squeezing gate

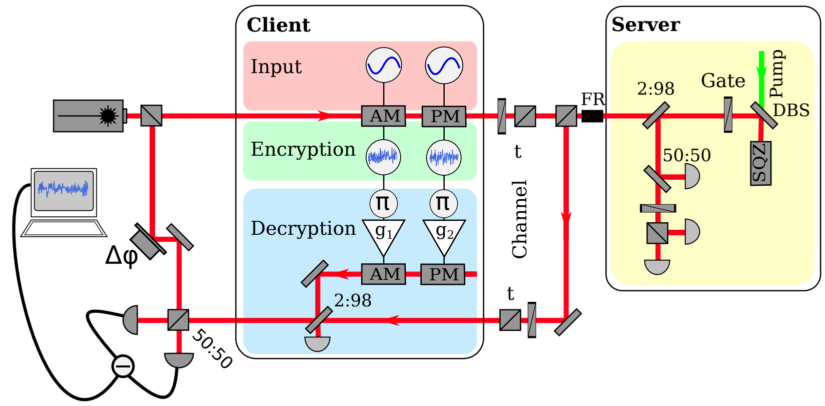


Figure 9.7: The experimental setup where the server implemented a squeezing operation. The encrypted coherent input state was injected into a linear semi-monolithic squeezing cavity. The output of the cavity was redirected by a Faraday rotator, and interfered with a strong coherent beam on an asymmetric beamsplitter to implement the decryption operation. The decryption noise was adjusted with gain factors g_1 and g_2 that depend on the squeezing. AM: Amplitude modulator, PM: Phase modulator.

The experimental setup shown in Figure 9.7 had the server implement the amplitude squeezing operation,

$$\hat{S}(r) = \exp\left(\frac{r}{4}(\hat{a}^2 - \hat{a}^{\dagger 2})\right) , \tag{9.3.4}$$

with squeezing parameter r, which is equivalent to the $\hat{U}_2(T)$ gate up to a phase shift [204]. The experimental setup is shown in Figure 9.7. In this experiment the client prepared a single coherent state as the input, not an ensemble. The encryption operation was still a Gaussian distribution.

The states were prepared by first splitting the 1064 nm seed beam into three parts, designated signal, LO and decryption. The LO went directly to the homodyne detector controlled by the client. The decryption went to the decryption modulators, where a thermal state exactly anti-correlated to the encryption state was prepared.

The signal beam was displaced, such that the input state was a single coherent state, which was then encrypted by a Gaussian noise distribution as was also the case for the displacement gate experiment. This encrypted coherent state was sent through the quantum channel with transmission T. After the channel the input state went through a Faraday rotator and a halfwave-plate in order to ensure that the input polarization was primarily vertical, though a small horizontal polarization component is required for the locking scheme described in Section 3.6.2.

Following the polarization optics the encrypted displaced state was sent into the pumped linear semi-monolithic optical parametric amplifier described in Section 3.5.2, from the non-HR side of the cavity. In this way the encrypted input state was squeezed and returned to the client. This is the first demonstration of squeezing directly on quantum information, so-called in-line squeezing. Until now squeezing transformations have been applied in an off-line manner [204]. The vacuum squeezing generated in this way is plotted in Figure 9.8. From this result we were able to determine the performance of the gate itself and conclude that it encounters a total of 43 % of transmission loss from the generation of the squeezing to the homodyne detection.

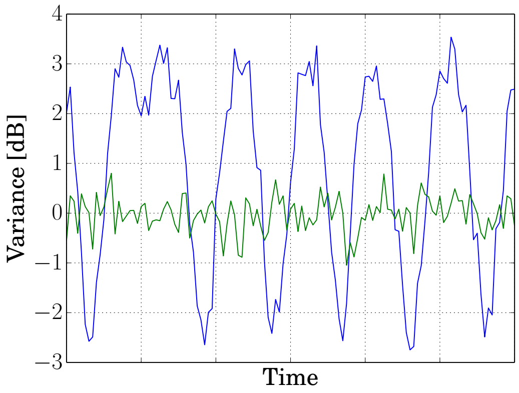


Figure 9.8: Variance of the squeezed state used for the quantum gate, with a scanned local oscillator. The green trace represents shotnoise.

The encrypted squeezed coherent state exited the cavity through the non-HR side. A 2 % tap-off was redirected to a 50/50 beam splitter. One mode of this splitting was detected directly by a photo detector and the AC output of this was mixed down to serve as an error signal for the pump phase lock. The other mode was directed to a wave plate and beam splitter combination with a subsequent photo detector detection on both these split beams, which is then subtracted. This subtraction generates an error signal at DC, which is used to lock the cavity length. The remaining 98 % of the output went back to the wave plate and Faraday rotator combination. Propagating through these components in the reverse direction ensured that the polarization after the rotator was horizontal, meaning that the beam was reflected by the polarizing beam splitter. After this beam splitter, a lossy quantum channel of transmission T

was implemented. Subsequent to this, the output beam was interfered with the aforementioned decryption beam, where the relative phase of these beams was controlled by a piezo actuated mirror. The beams were locked around destructive interference through a measurement of the 36.7 MHz sideband also used for the pump phase lock, which was optimal for the noise cancellation. Controlling the offset of this error signal gave very precise control of the relative phase. In turn, having control of this relative phase allowed for more precise cancellation of the decryption noise than in the experiment with the displacement gates. Similarly to the experiment with the displacement gates, the client used scanned homodyne detection using the LO from before.

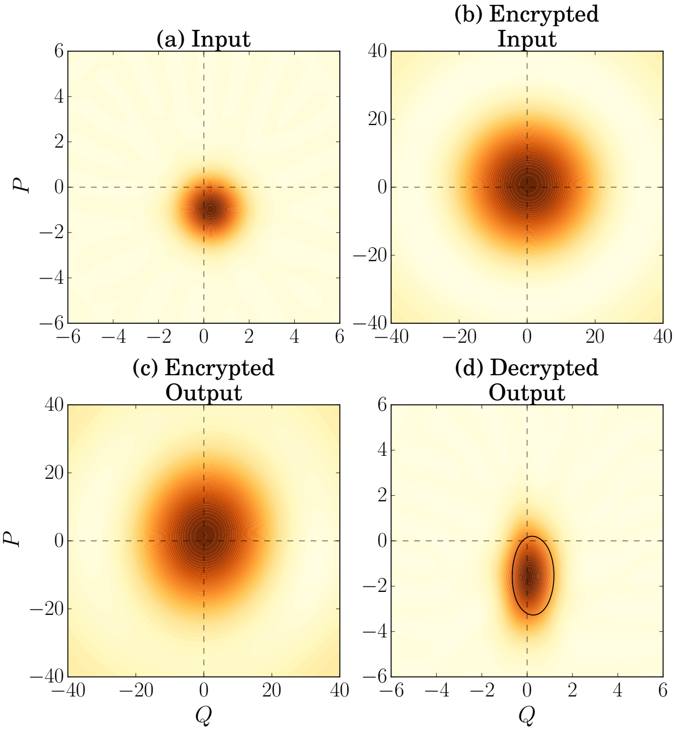


Figure 9.9: For each step of the protocol, the corresponding Wigner function is shown to illustrate the state. For each step, the state is measured with homodyne detection and mixed down from the 10.5 MHz sideband where it resides. In the last step, the black outline denotes the FWHM of the squeezing ellipse that would result from the server acting on a plaintext input state.

The reconstructed Wigner functions for each of the protocol steps are shown in Figure 9.9. The Wigner functions are reconstructed by homodyne detections with scanned relative phase between the signal and local oscillator, to collect marginal distributions as described in Section 3.8. The filtered back projection algorithm was used for the states where the mean photon number was too large to admit reconstruction by maximum likelihood. Figure 9.9(a) shows the initial displaced state prepared by Alice. Figure 9.9(b) shows this state as encrypted by an ensemble of random displacements. In Figure 9.9(c) the encrypted displaced state has been squeezed, such that the second order moments are no longer symmetric in the quadratures. However, none of the variances are below shotnoise because of the encryption. In Figure 9.9(d), the client recovers the displaced squeezed state after decrypting the state received through the quantum channel. The squeezing is now below shot noise.

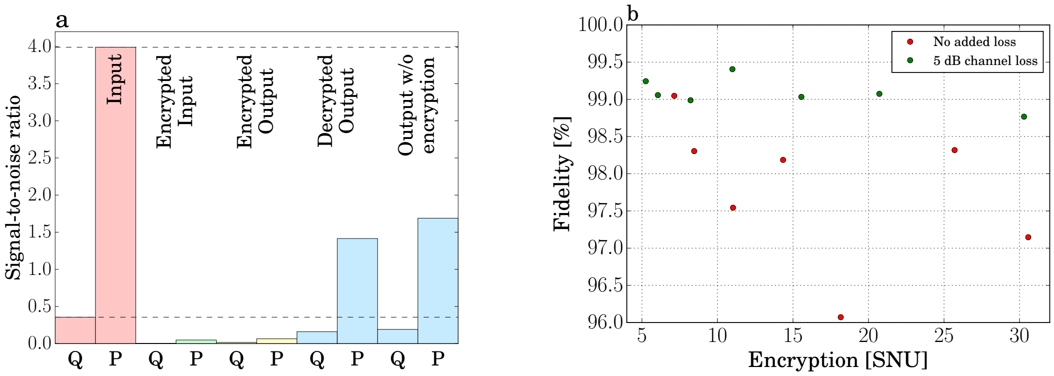


Figure 9.10: (a) The signal-to-noise ratio from the point of view of the server in each quadrature for each step of the protocol. The prepared input state is displaced most in the P quadrature. The next step reduces the SNR in both quadratures, but the signal remains stronger in P. After the squeezing operation, the SNR is slightly increased in both quadratures. The decrypted output features a lower SNR than the plaintext output. Ideally the SNR should correspond to the input state as the gain factor in the squeezing also affects the coherent excitation in the displaced state. Thus, the difference between the levels quantifies the performance of the gate. (b) Plot of fidelity between encrypted and plain-text output states in terms of encryption noise. Plotted with lossless channel and 63 % transmission channel, equivalent to 10 km of optical fiber at 1550 nm. Statistical errors are smaller than the point size, due to the number of data points.

The performance of the squeezing gate and the associated decryption operation are quantified in Figure 9.10. Figure 9.10(b) shows the fidelity between a decrypted output and a plain-text execution of the protocol. This fidelity is plotted in terms of encryption noise, both for a lossless quantum channel and 5 dB $\simeq$ 63 % transmission loss, equivalent to using 10 km of fiber at a telecom wavelength as the channel. The measured fidelities vary against the encryption noise in the same way as it was observed in Figure 9.6(b). These variations are caused by systematic errors in the tuning of the noise cancellation that implements the decryption operation. Additionally, the reconstruction of the Wigner functions is quite sensitive to the quality of the interference fringes at the homodyne detector, and any errors introduced by these imperfections are not statistically independent, but are correlated via the environment surrounding the experiment. Lastly, the encryption noise is not perfectly correlated with the signal used for the decryption operation. This results in residual noise which also reduces the fidelity. Even with these sources of error, the fidelity is shown to stay above 98.5 % for the investigated parameters, with a slight increase towards lower encryption noise. This is because the outputs of the noise generator for the encryption and decryption are better correlated for low voltages.

For the case of increased channel loss, the fidelities are slightly higher. This is caused by the loss forcing the states closer to vacuum, such that when everything is close to a vacuum state, fidelity naturally goes up. These measurements demonstrate the delegated universal quantum on encrypted quantum states is possible, and is largely independent on the quality of the implemented gates. In Figure 9.10(a), the signal-to-noise ratio in both quadratures is plotted for all protocol steps. This measure takes the quality of the gate into account, in the sense that for an ideal gate and lossless channel one would expect to recover the input SNR in the last step of the protocol. This is because the coherent excitation of the input state is affected by the same gain factor as the noise is, and so the signal and the noise change by same amount, the net effect being no change in SNR. The difference between the observed level for the plain-text output state and the input SNR quantifies the gate performance. The difference in SNR between the plain-text and decrypted outputs quantify the decryption performance as the fidelity plot in Figure 9.10(b). This shows that the gate implementation is quite lossy, 43 %, but the decryption operation performs quite well, almost independently of this. The losses in the gate implementation occur primarily on the server side. The mode matching of the encrypted input state into the squeezer was 97 %, as a consequence of the polarization asymmetry required for the Hänsch-Couillaud lock. The beam sampler for the locking signals introduces 2 % loss on the output by default. The Faraday rotator also incurred 3 % of loss on the squeezed output. There are also loss contributions on the client side, notably from the decryption operation which incurs another 2 % from the beam sampler, and the visibility of the homodyne detection was around 98 %. The quantum efficiency of the photodiodes in the detector was 99 %. These contributions do not bring the total loss of squeezing to 43 %, but it is possible that polarization impurities have contributed more than was originally anticipated. Polarization control was especially important on the server side and these impurities would not be readily apparent through measurements of the carrier power.

Concluding remarks

In this work we developed a protocol for universal quantum computing on encrypted continuous variable states. This protocol requires the use of a quantum channel and transfer of classical information for the implementation of the cubic phase gate $\hat{U}_3(T)$. All Gaussian transformations in the universal set can be implemented without this additional cost of classical information. The client needs to have arbitrary displacements within some energy threshold as a classical resource, and limited squeezing as a quantum resource.

Gates from the universal set can be composed and the output of the program can be decrypted by an overall correction operator that depends on the operations within the program. Quantum computing on encrypted data has, until now, never been theoretically investigated in the regime of continuous variables. In addition, it is the first time that secure delegated quantum computing has been performed over a lossy quantum channel, in either the DV or CV regime. Extending the range of this protocol will require some type of quantum repeater or relay structure [205], but the present work is an important first step towards delegated continuous variable quantum computing with provable security.

Conclusion

In this thesis a number of QKD protocols were developed and discussed. Of particular interest was the first ever proof-of-principle demonstration of CVMDIQKD, where we demonstrated that an asymmetric relay configuration is able to exchange correlations between the honest parties in order to provide quantum security, and the relay need not be trusted. The implementation of the protocol gave a bound for the secret key rate which indicates that this configuration is especially useful in metropolitan networks where distances are rather short. The idea is that CVQKD is generally more susceptible to loss, and thus degrades faster. However, when the distances are moderate higher modulation frequencies are easier to achieve than high repetition rates for the corresponding DVQKD implementation.

A number of outstanding challenges associated with this protocol still remain. For a simplified detection scheme as the one used in this experimental implementation a synchronization of the laser frequency of two sources, rather than one, presents an issue equivalent to what a local oscillator travelling through the quantum channel in a standard protocol implies. A mismatch in optical frequency will first of all lead to reduced interference between the beams at the relay, but it will also complicate the measurement process as the carrier and signal beats will be shifted with a time-dependent frequency. The net effect of this is the introduction of excess noise which degrades the secret key rate. As such, a field implementation of CVMDIQKD will most certainly require some sort of synchronization technique. This problem is of a purely classical nature, and technology derived from the field of classical optical communication should suffice to provide the necessary solution.

An additional concern has been whether the efficiency of the relay is sufficiently high, as any loss encountered here should be ascribed to Eve in a practical setting. The limiting factors here are the interference of the signal beams, which is again related to the synchronization issue, and the coupling losses of the optical fibers that will almost certainly be used in an in-field implementation, the alternative being a free space implementation in an atmospheric channel. Of course, atmospheric channels are also a viable option, for example with a low-orbit satellite acting as an untrusted relay. In either scenario the efficiency of the relay is important, but this is largely a technical consideration and does not provide a fundamental limitation to the performance of the protocol. Interference visibilities above 99 % are routinely achieved, and coupling losses can likely be lowered through anti-reflection coatings. Further, the detection efficiencies of the photodetectors can also go above 99 %, depending on the wavelength, though this will inevitably increase the cost of the hardware.

The same CVMDIQKD protocol was experimentally investigated under the addition of correlated thermal noise, simulating a weaker version of a generalized joint entangling cloner attack on the relay links. Since the practical MDIQKD protocol has an equivalent entanglement-based model, we may regard the action of the practical relay as distributing virtual bipartite entanglement between Alice and Bob. This equivalence allows us to investigate other protocols that use entanglement, notably entanglement swapping, teleportation and distillation and relate them to the performance of the MDIQKD protocol. We find that increasing correlations in the thermal noise injected into the joint quantum channel reactivates the protocols in the order swapping, teleportation, distillation and MDIQKD. We see experimentally that the MDIQKD protocol maintains security well past the threshold for the breaking of virtual entanglement. This result may be applicable to physical systems where correlated noise is prevalent, and we make the argument that these correlations should be seen as a resource to be exploited wherever possible.

Another way to consider noise in the context of QKD is the concept of preparation noise. In addition to the concept of excess noise that results from the quantum channel, we consider the situation where Alice's preparation of coherent states in a point-to-point QKD protocol has some additional noise that she does not control, which makes it harder for Bob to estimate which states she actually prepared. If we make the standard assumption that Alice's station is secure from eavesdropper tampering, we may regard this noise as trusted, and in this case it is not detrimental to the secure key rate, if direct reconciliation is used. This superiority of direct reconciliation is intuitively appealing because it is easier for Alice to estimate what Bob will receive than it is for Bob to estimate the prepared states, provided that the preparation noise is strong enough. We remark that the converse scenario with trusted detection noise at Bob has been considered in the literature before, and reinforces the standard superiority of reverse reconciliation [169]. The confirmation of this prediction is promising for the idea of implementing short range CVQKD with cheap noisy laser sources, which may simplify practical implementations and reduce their cost.

A further simplification of CVQKD is the concept of the single quadrature encoding. Security of CVQKD is, like for DVQKD, guaranteed through the non-orthogonality of the signal states and the no-cloning theorem. This fact is also exploited in the two state protocol with coherent states [49, 50], but a similar idea has never before been applied to a continuous alphabet of coherent states. Careful theoretical considerations [172] have shown that this requires a minimization over a channel parameter that cannot be estimated in practice, but otherwise the protocol still provides quantum security, with a very simplified implementation. This fact should come as no surprise to those well versed in the theory of CVQKD, but we have now conclusively demonstrated this in a proof-of-principle experiment in the asymptotic limit of infinite state exchanges where coherent attacks are equivalent to collective attacks and Gaussian extremality applies. A potential outlook for this protocol is a fiber implementation with a local local oscillator, which would represent a simple and cost-efficient way to implement quantum security while eliminating an important loophole in the security proof.

A straightforward variation on the single quadrature protocol is to use squeezed states for the alphabet rather than coherent states. Rather than focus on the superior secret key rate this alphabet provides, we instead emphasize an interesting advantage that the use of squeezing may provide. If the quantum channel is purely lossy, we have shown that the use of squeezing can force the Holevo bound to zero. By monitoring the correlations between Bob and Eve in a configuration where the channel is purely lossy, it was possible to show experimentally that these correlations indeed go to zero. Following the reconstruction of the global covariance matrix, we confirm that the Holevo bound also goes to zero. This is a demonstration of eavesdropper decoupling without the use of entanglement distillation, in fact only through the use of Gaussian operations. Additionally the decoupling was shown to be independent of transmission loss and squeezing purity. While this protocol is perhaps too involved to be a commercially viable solution to CVQKD, it is nevertheless an interesting effect that is not known to be achievable in the regime of discrete variables.

The last way we considered security was in the concept of delegated quantum computing through a weaker version of homomorphic encryption. This delegated quantum computing on encrypted data was demonstrated for the first time using continuous variables by implementing the displacement and squeezing operations from the universal quantum computing set for continuous variables. We do this, for the first time, over a simulated lossy quantum channel. The results indicate that, at least for Gaussian operations, this protocol is feasible for delegated quantum computing. While proving the security of the scheme remains an open problem, we have shown that the encryption operation reduces the classical mutual information between the client and the server. The reduction is asymptotic such that a complete decoupling would require infinite energy, but in practice there exists an optimal value that balances the need for security with low residual noise from the imperfect decryption.

We show that for reasonable values of this encryption noise, the quantum gate output can be recovered with high fidelity compared to the output that would be received by the client in an unencrypted setting. We implement the decryption using two different techniques, one with direct transmission through the optical modulators that decrypt the state, which causes a distortion of the spatial beam profile. Another technique interferes the state returned from the server with a strongly modulated beam that carries the coherent state that decrypts the output. This approach seems to be favourable because it allows for more precise control of the relative phase between encryption and decryption which is highly crucial for obtaining a good fidelity.

In conclusion we have experimentally demonstrated a number of novel quantum communication protocols in the CV regime that provide some form of security using Gaussian operations and measurements. We have investigated the effects of noise with Gaussian distributions and shown how this might be beneficial to the honest users in some configurations.

Bibliography

[1] Max Planck. Über das gesetz der energieverteilung im normalspektrum. *Annalen der Physik*, 306(3):553–563, 1901.

[2] Lord Kelvin. Nineteenth-century clouds over the dynamical theory of heat and light. *The London, Edinburgh and Dublin Philosophical Magazine and Journal of Science*, 2(6):1–40, 1901.

[3] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can Quantum-Mechanical Description of Physical Reality be considered complete? *Physical Review*, 47:777–780, 1935.

[4] John S. Bell. On the Einstein Podolsky Rosen Paradox. *Physics*, 1(3):195–200, 1964.

[5] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory.* Wiley-Interscience, 2nd edition, 2006.

[6] Stephen Wiesner. Conjugate Coding. *ACM SIGACT News*, 15(1):78–88, 1983.

[7] Charles H. Bennett and Gilles Brassard. Quantum Cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, volume 175, page 8, 1984.

[8] Richard P. Feynman. Simulating physics with computers. In *International Journal of Theoretical Physics*, volume 21, pages 467–488, 1982.

[9] A. Galindo and M. A. Martín-Delgado. Information and computation: Classical and quantum aspects. *Reviews of Modern Physics*, 74(2):347–423, 2002.

[10] Stephen M. Barnett. *Quantum Information.* Oxford University Press, 2009.

[11] Mark M. Wilde. *From Classical to Quantum Shannon Theory.* arXiv:1106.1445v7, 2016.

[12] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[13] H. K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, 1997.

[14] Dominic Mayers. Unconditionally Secure Quantum Bit Commitment is Impossible. *Physical Review Letters*, 78(17):3414–3417, 1997.

[15] Mark Hillery, Vladimir Buzek, and Andre Berthiaume. Quantum Secret Sharing. *Physical Review A*, 59(3):1829–1834, 1999.

[16] Anders Karlsson, Masato Koashi, and Nobuyuki Imoto. Quantum entanglement for secret sharing and secret splitting. *Physical Review A*, 59(1):162–168, 1999.

[17] Charles H Bennett. Quantum Cryptography Using Any Two Nonorthogonal States. *Physical Review Letters*, 68(21):3121–3124, 1992.

[18] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[19] Robert Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098–1105, 1996.

[20] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.

[21] Scott Aaronson and Alex Arkhipov. The Computational Complexity of Linear Optics. *Theory of Computing*, 9(4):143–252, 2013.

[22] J. G. Rarity, P. C. M. Owens, and P. R. Tapster. Quantum Random-Number Generation and Key Sharing. *Journal of Modern Optics*, 41(12):2435–2444, 1994.

[23] Ralf Schützhold and William G. Unruh. Quantum correlations across the black hole horizon. *Physical Review D*, 81(12):124033, 2010.

[24] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2):419–478, 2014.

[25] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526:682–686, 2015.

[26] Artur Ekert and Richard Jozsa. Quantum computation and Shor's factoring algorithm. *Reviews of Modern Physics*, 68(3):733–753, 1996.

[27] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[28] Hoi-Kwong Lo and H. F. Chau. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science*, 283(5410):2050–2056, 1999.

[29] Christopher Gerry and Peter Knight. *Introductory Quantum Optics*. Cambridge University Press, 2004.

[30] Samuel L. Braunstein and Peter van Loock. Quantum information with continuous variables. *Reviews of Modern Physics*, 77(April):513–577, 2005.

[31] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145–195, 2002.

[32] Antonio Acín, Serge Massar, and Stefano Pironio. Efficient quantum key distribution secure against no-signalling eavesdroppers. *New Journal of Physics*, 8:126, 2006.

[33] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

[34] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-Device-Independent Quantum Key Distribution. *Physical Review Letters*, 108(13):130503, 2012.

[35] Samuel L. Braunstein and Stefano Pirandola. Side-channel-free quantum key distribution. *Physical Review Letters*, 108(13):130502, 2012.

[36] Charles Ci Wen Lim, Boris Korzh, Anthony Martin, Félix Bussières, Rob Thew, and Hugo Zbinden. Detector-device-independent quantum key distribution. *Applied Physics Letters*, 105(22):221112, 2014.

[37] Marcos Curty, Feihu Xu, Wei Cui, Charles Ci Wen Lim, Kiyoshi Tamaki, and Hoi-Kwong Lo. Finite-key analysis for measurement-device-independent quantum key distribution. *Nature Communications*, 5:1–7, 2014.

[38] Tae Gon Noh. Counterfactual quantum cryptography. *Physical Review Letters*, 103(23):230501, 2009.

[39] Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew, and Hugo Zbinden. Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre. *Nature Photonics*, 9(3):163–168, 2015.

[40] Momtchil Peev et al. The SECOQC quantum key distribution network in Vienna. *New Journal of Physics*, 11:075001, 2009.

[41] Masahide Sasaki et al. Field test of quantum key distribution in the Tokyo QKD Network. *Optics Express*, 19(11):10387–10409, 2011.

[42] M. D. Reid. Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations. *Physical Review A*, 62(6):062308, 2000.

[43] M Hillery. Quantum cryptography with squeezed states. *Physical Review A*, 61(2):022309, 2000.

[44] T. C. Ralph. Security of continuous-variable quantum cryptography. *Physical Review A*, 62(6):062306, 2000.

[45] N. J. Cerf, M. Levy, and G. Van Assche. Quantum Distribution of Gaussian Keys with Squeezed States. *Physical Review A*, 63(5):052311, 2001.

[46] Christine Silberhorn, Natalia Korolkova, and Gerd Leuchs. Quantum Key Distribution with Bright Entangled Beams. *Physical Review Letters*, 88(16):167902, 2002.

[47] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Physical Review Letters*, 88(5):057902, 2002.

[48] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier. Quantum key distribution using Gaussian-modulated coherent states. *Nature*, 421:238–41, 2003.

[49] S. Lorenz, J. Rigas, M. Heid, U. L. Andersen, N. Lütkenhaus, and G. Leuchs. Witnessing effective entanglement in a continuous variable prepare-and-measure setup and application to a quantum key distribution scheme using postselection. *Physical Review A*, 74(4):042326, 2006.

[50] Yi Bo Zhao, Matthias Heid, Johannes Rigas, and Norbert Lütkenhaus. Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. *Physical Review A*, 79:012307, 2009.

[51] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam. Quantum cryptography without switching. *Physical Review Letters*, 93(17):170504, 2004.

[52] Andrew M. Lance, Thomas Symul, Vikram Sharma, Christian Weedbrook, Timothy C. Ralph, and Ping Koy Lam. No-switching quantum key distribution using broadband modulated coherent light. *Physical Review Letters*, 95(18):180503, 2005.

[53] Lars S. Madsen, Vladyslav C. Usenko, Mikael Lassen, Radim Filip, and Ulrik L. Andersen. Continuous variable quantum key distribution with modulated entangled states. *Nature Communications*, 3:1083, 2012.

[54] Tobias Gehring, Vitus Händchen, Jörg Duhme, Fabian Furrer, Torsten Franz, Christoph Pacher, Reinhard F. Werner, and Roman Schnabel. Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks. *Nature Communications*, 6:8795, 2015.

[55] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, Ch. Marquardt, and G. Leuchs. Atmospheric continuous-variable quantum communication. *New Journal of Physics*, 16:113018, 2014.

[56] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, 7:378–381, 2013.

[57] Paul Jouguet, Sébastien Kunz-Jacques, and Anthony Leverrier. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Physical Review A*, 84(6):062317, 2011.

[58] Duan Huang, Peng Huang, Dakai Lin, and Guihua Zeng. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Scientific Reports*, 6:19201, 2016.

[59] Leslie E. Ballentine. *Quantum Mechanics: A Modern Development.* World Scientific Publishing, 1998.

[60] Fabian Furrer, Johan Åberg, and Renato Renner. Min- and Max-Entropy in Infinite Dimensions. *Communications in Mathematical Physics*, 306(1):165–186, 2011.

[61] Renato Renner. *Security of Quantum Key Distribution.* PhD thesis, Swiss Federal Institute of Technology, 2013.

[62] D. R. Stinson. Atmospheric continuous-variable quantum communication. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 42:3, 2002.

[63] Marco Tomamichel, Adam Smith, Christian Schaffner, and Renato Renner. Left-over Hashing in the Presence of Quantum Side Information. In *IEEE Transactions on Information Theory*, volume 57, pages 5524–5535, 2010.

[64] Paul Jouguet, David Elkouss, and Sébastien Kunz-Jacques. High-bit-rate continuous-variable quantum key distribution. *Physical Review A*, 90(4):042329, 2014.

[65] Anthony Leverrier, Romain Alléaume, Joseph Boutros, Gilles Zémor, and Philippe Grangier. Multidimensional reconciliation for continuous-variable quantum key distribution. *Physical Review A*, 77(4):042325, 2008.

[66] Frédéric Grosshans and Philippe Grangier. Reverse Reconciliation Protocols for Quantum Cryptography with Continuous Variables. In *Proceedings of the Sixth International Conference on Quantum Communication, Measurement and Computing*, pages 351–356, 2003.

[67] Frédéric Grosshans, Nicolas J. Cerf, Jérôme Wenger, R. Tualle-Brouri, and Philippe Grangier. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Journal of Quantum Information and Computation*, 3:535–552, 2003.

[68] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1997.

[69] Eleni Diamanti and Anthony Leverrier. Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations. *Entropy*, 17:6072–6092, 2015.

[70] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dusek, Norbert Lütkenhaus, Momtchil Peev, and Miloslav Dušek. The Security of Practical Quantum Key Distribution. *Reviews of Modern Physics*, 81(3):1301–1350, 2009.

[71] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84:621, 2012.

[72] U.L. Andersen, G. Leuchs, and C. Silberhorn. Continuous-variable quantum information processing. *Laser & Photonics Reviews*, 4(3):337–354, 2010.

[73] Renato Renner and J. I. Cirac. de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography. *Physical Review Letters*, 102(11):110504, 2009.

[74] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Physical Review Letters*, 109(10):100502, 2012.

[75] Fabian Furrer. Reverse Reconciliation Continuous Variable Quantum Key Distribution Based on the Uncertainty Principle. *Physical Review A*, 90(4):042325, 2014.

[76] Anthony Leverrier. Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States. *Physical Review Letters*, 114(7):070501, 2015.

[77] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature communications*, 3:634, 2012.

[78] Jaromír Fiurášek. Gaussian Transformations and Distillation of Entangled Gaussian States. *Physical Review Letters*, 89(13):137904, 2002.

[79] Jens Eisert, Stefan Scheel, and Martin B. Plenio. Distilling Gaussian States with Gaussian Operations is Impossible. *Physical Review Letters*, 89(13):137903, 2002.

[80] Géza Giedke and J. I. Cirac. Characterization of Gaussian operations and distillation of Gaussian states. *Physical Review A*, 66(3):032316, 2002.

[81] Raúl García-Patrón and Nicolas J. Cerf. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Physical Review Letters*, 97(19):190503, 2006.

[82] Ulf Leonhardt. *Measuring the Quantum State of Light.* Cambridge University Press, 1997.

[83] Max Born and Emil Wolf. *Principles of Optics.* Cambridge University Press, 7th edition, 2005.

[84] Steven H. Strogatz. *Nonlinear Dynamics and Chaos.* Westview Press, 2000.

[85] Tobias Eberle. *Realization of Finite-Size Quantum Key Distribution based on Einstein-Podolsky-Rosen Entangled Light.* PhD thesis, Gottfried Wilhelm Leibniz University Hannover, 2013.

[86] A. Uhlmann. The "transition probability" in the state space of a *-algebra. *Reports on Mathematical Physics*, 9(2):273–279, 1976.

[87] Richard Jozsa. Fidelity for Mixed Quantum States. *Journal of Modern Optics*, 41(12):2315–2323, 1994.

[88] R. Simon. Peres-Horodecki separability criterion for continuous variable systems. *Physical Review Letters*, 84(12):2726–2729, 2000.

[89] Lu-Ming Duan, G. Giedke, J. I. Cirac, and P. Zoller. Inseparability criterion for continuous variable systems. *Physical Review Letters*, 84(12):2722–2725, 2000.

[90] Alessio Serafini, Fabrizio Illuminati, and Silvio De Siena. Symplectic invariants, entropic measures and correlations of Gaussian states. *J. Phys. B: At. Mol. Opt. Phys.*, 37:21–28, 2004.

[91] J. Williamson. On the Algebraic Problem Concerning the Normal Forms of Linear Dynamical Systems. *American Journal of Mathematics*, 58:141, 1936.

[92] R. Simon, N. Mukunda, and Biswadeb Dutta. Quantum-noise matrix for multimode systems: $U(n)$ invariance, squeezing, and normal forms. *Physical Review A*, 49(3):1567–1583, 1994.

[93] D. T. Smithey, M. Beck, J. Cooper, and M. G. Raymer. Measurement of number-phase uncertainty relations of optical fields. *Physical Review A*, 48(4):3159–3167, 1993.

[94] R. E. Slusher, L. W. Hollberg, B. Yurke, J. C. Mertz, and J. F. Valley. Observation of squeezed states generated by four-wave mixing in an optical cavity. *Physical Review Letters*, 55(22):2409–2412, 1985.

[95] Moritz Mehmet, Stefan Ast, Tobias Eberle, Sebastian Steinlechner, Henning Vahlbruch, and Roman Schnabel. Squeezed light at 1550 nm with a quantum noise reduction of 12.3 dB. *Optics Express*, 19(25):25763, 2011.

[96] Ulrik L. Andersen, Tobias Gehring, Christoph Marquardt, and Gerd Leuchs. 30 Years of Squeezed Light Generation. *Physica Scripta*, 91(5):053001, 2015.

[97] Vladyslav C. Usenko and Radim Filip. Squeezed-state quantum key distribution upon imperfect reconciliation. *New Journal of Physics*, 13:113007, 2011.

[98] Raúl García-Patrón Sánchez. *Quantum Information with Optical Continuous Variables: from Bell Tests to Key Distribution.* PhD thesis, Université Libre de Bruxelles, 2007.

[99] Marcos Curty, Maciej Lewenstein, and Norbert Lütkenhaus. Entanglement as a precondition for secure quantum key distribution. *Physical Review Letters*, 92(21):217903, 2004.

[100] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223:1–8, 1996.

[101] Asher Peres. Separability Criterion for Density Matrices. *Physical Review Letters*, 77(8):1413–1415, 1996.

[102] R. F. Werner and M. M. Wolf. Bound entangled Gaussian states. *Physical Review Letters*, 86(16):3658–3661, 2001.

[103] G Vidal and R F Werner. Computable measure of entanglement. *Physical Review A*, 65(3):32314, 2002.

[104] Edwin T. Jaynes. *Probability Theory - The Logic of Science.* Cambridge University Press, 2003.

[105] Gaetana Spedalieri, Carlo Ottaviani, and Stefano Pirandola. Covariance matrices under Bell-like detections. *Open Systems & Information Dynamics*, 20(2):1350011, 2013.

[106] A. S. Holevo and R. F. Werner. Evaluating capacities of bosonic Gaussian channels. *Physical Review A*, 63(3):302312, 2001.

[107] Stefano Pirandola, Samuel L. Braunstein, and Seth Lloyd. Characterization of Collective Gaussian Attacks and Security of Coherent-State Quantum Cryptography. *Physical Review Letters*, 101(20):200504, 2008.

[108] Stefano Pirandola, Raul García-Patrón, Samuel L. Braunstein, and Seth Lloyd. Direct and reverse secret-key capacities of a quantum channel. *Physical Review Letters*, 102(5):050503, 2009.

[109] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. In *Proceedings of the Royal Society A*, volume 461, pages 207–235, 2005.

[110] Renato Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3(9):645–649, 2007.

[111] Robert König, Renato Renner, Andor Bariska, and Ueli Maurer. Small accessible quantum information does not imply security. *Physical Review Letters*, 98(14):140502, 2007.

[112] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A*, 81(6):062343, 2010.

[113] Eric D. Black. An introduction to Pound–Drever–Hall laser frequency stabilization. *American Journal of Physics*, 69(1):79, 2001.

[114] Hans-A. Bachor and Timothy C. Ralph. *A Guide to Experiments in Quantum Optics*. Wiley-VCH, 2nd edition, 2004.

[115] George B. Arfken and Hans J. Weber. *Mathematical Methods for Physicists*. Elsevier Academic Press, 6th edition, 2005.

[116] Lars S. Madsen. *Quantum Information Processing with Mesoscopic Photonic States*. PhD thesis, Technical University of Denmark, 2012.

[117] G. D. Boyd and D. A. Kleinman. Parametric Interaction of Focused Gaussian Light Beams. *Journal of Applied Physics*, 39(8):3597–3639, 1968.

[118] Alex Abramovici and Jake Chapsky. *Feedback Control Systems: A Fast-Track Guide for Scientists and Engineers*. Springer Science and Business Media, 2000.

[119] R. W. P. Drever, J. L. Hall, F. V. Kowalski, J. Hough, G. M. Ford, A. J. Munley, and H. Ward. Laser phase and frequency stabilization using an optical resonator. *Applied Physics B*, 31(2):97–105, 1983.

[120] T. W. Hänsch and B. Couillaud. Laser Frequency Stabilization By Polarization Spectroscopy of a Reflecting Reference Cavity. *Optics Communications*, 35(3):441–444, 1980.

[121] M. G. Raymer, M. Beck, and D. F. McAlister. Complex Wave-Field Reconstruction Using Phase-Space Tomography. *Physical Review Letters*, 72(8):1137–1140, 1994.

[122] Alexander I. Lvovsky and Michael G. Raymer. Continuous-variable optical quantum-state tomography. *Reviews of Modern Physics*, 81(1):299–332, 2009.

[123] Z. Hradil. Quantum-state estimation. *Physical Review A*, 55(3):R1561–R1564, 1997.

[124] Jonas Schou Neergaard-Nielsen. *Generation of single photons and Schrödinger kitten states of light*. PhD thesis, Niels Bohr Institute, 2008.

[125] Marek Zukowski, Anton Zeilinger, Michael A. Horne, and Artur K. Ekert. "Event-Ready-Detectors" Bell Experiment via Entanglement Swapping. *Physical Review Letters*, 71(26):4287–4290, 1993.

[126] H. J. Briegel, W. Dür, J. Ignacio Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Physical Review Letters*, 81(26):5932–5935, 1998.

[127] H. J. Kimble. The quantum internet. *Nature*, 453(7198):1023–1030, 2008.

[128] SECOQC. `http://www.secoqc.net`. Accessed: 2016-08-11.

[129] Tokyo QKD network. `www.uqcc.org/QKDnetwork`. Accessed: 2016-08-11.

[130] Ilja Gerhardt, Qin Liu, Antía Lamas-Linares, Johannes Skaar, Valerio Scarani, Vadim Makarov, and Christian Kurtsiefer. Experimentally faking the violation of Bell's inequalities. *Physical Review Letters*, 107(17):170404, 2011.

[131] Ilja Gerhardt, Qin Liu, Antía Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Communications*, 2(349):1–6, 2011.

[132] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4:686–689, 2010.

[133] Audun Nystad Bugge, Sebastien Sauge, Aina Mardhiyah M Ghazali, Johannes Skaar, Lars Lydersen, and Vadim Makarov. Laser damage helps the eavesdropper in quantum cryptography. *Physical Review Letters*, 112(7):070503, 2014.

[134] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel. Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks. *Physical Review Letters*, 111(13):130501, 2013.

[135] T. Ferreira Da Silva, D. Vitoreti, G. B. Xavier, G. C. Do Amaral, G. P. Temporão, and J. P. Von Der Weid. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Physical Review A*, 88(5):052303, 2013.

[136] Yan-lin Tang et al. Measurement-device-independent quantum key distribution over 200 km. *Physical Review Letters*, 113(19):190501, 2014.

[137] J. H. Saltzer, D. P. Reed, and D. D. Clark. End-to-end arguments in system design. *ACM Transactions on Computer Systems*, 2(4):277–288, 1984.

[138] P. Baran. On Distributed Communications Networks. In *IEEE Transactions on Communications Systems*, volume 12, 1964.

[139] Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias Gehring, Christian S. Jacobsen, and Ulrik L. Andersen. High-rate measurement-device-independent quantum cryptography. *Nature Photonics*, 9(6):397–402, 2015.

[140] Stefano Pirandola, David Vitali, Paolo Tombesi, and Seth Lloyd. Macroscopic entanglement by entanglement swapping. *Physical Review Letters*, 97(15):150403, 2006.

[141] Christian Weedbrook, Stefano Pirandola, and Timothy Ralph. Continuous-variable quantum key distribution using thermal states. *Physical Review A*, 86(2):022318, 2012.

[142] J. Niset, A. Acín, U. L. Andersen, N. J. Cerf, R. García-Patrón, M. Navascués, and M. Sabuncu. Superiority of entangled measurements over all local strategies for the estimation of product coherent states. *Physical Review Letters*, 98(26):260404, 2007.

[143] Jérôme Lodewyck, Matthieu Bloch, Raúl García-Patrón, Simon Fossier, Evgueni Karpov, Eleni Diamanti, Thierry Debuisschert, Nicolas J. Cerf, Rosa Tualle-Brouri, Steven W. McLaughlin, and Philippe Grangier. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Physical Review A*, 76(4):042305, 2007.

[144] Bing Qi, Pavel Lougovski, Raphael Pooser, Warren Grice, and Miljko Bobrek. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Physical Review X*, 5(4):041009, 2015.

[145] Christian Weedbrook, Stefano Pirandola, Seth Lloyd, and Timothy C. Ralph. Quantum cryptography approaching the classical limit. *Physical Review Letters*, 105(11):110501, 2010.

[146] Christian Weedbrook, Carlo Ottaviani, and Stefano Pirandola. Two-way quantum cryptography at different wavelengths. *Physical Review A*, 89(1):012309, 2014.

[147] Peter Van Loock and Samuel L. Braunstein. Unconditional teleportation of continuous-variable entanglement. *Physical Review A*, 61:010302(R), 1999.

[148] R. Polkinghorne and T. Ralph. Continuous Variable Entanglement Swapping. *Physical Review Letters*, 83(11):2095–2099, 1999.

[149] Lev Vaidman. Teleportation of quantum states. *Physical Review A*, 49(2):1473–1476, 1994.

[150] Akira Furusawa, J. L. Sorensen, Samuel L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik. Unconditional quantum teleportation. *Science*, 282(5389):706–709, 1998.

[151] Stefano Pirandola, Jens Eisert, Christian Weedbrook, Akira Furusawa, and Samuel L. Braunstein. Advances in Quantum Teleportation. *Nature Photonics*, 9(10):641–652, 2015.

[152] Benjamin J. Metcalf, Justin B. Spring, Peter C. Humphreys, Nicholas Thomas-Peter, Marco Barbieri, W. Steven Kolthammer, Xian-min Jin, Nathan K. Langford, Dmytro Kundys, James C. Gates, Brian J. Smith, Peter G. R. Smith, and Ian A. Walmsley. Quantum teleportation on a photonic chip. *Nature Photonics*, 8(9):770–774, 2014.

[153] Genta Masada, Kazunori Miyata, Alberto Politi, Toshikazu Hashimoto, Jeremy L. O'Brien, and Akira Furusawa. Continuous-variable entanglement on a chip. *Nature Photonics*, 9(3):316–319, 2015.

[154] L. Steffen, Y. Salathe, M. Oppliger, P. Kurpiers, M. Baur, C. Lang, C. Eichler, G. Puebla-Hellmann, A. Fedorov, and A. Wallraff. Deterministic quantum teleportation with feed-forward in a solid state system. *Nature*, 500:319–322, 2013.

[155] H.-P. Breuer and F. Petruccione. *The Theory of Open Quantum Systems*. Oxford University Press, 2002.

[156] Mikael Lassen, Adriano Berni, Lars S. Madsen, Radim Filip, and Ulrik L. Andersen. Gaussian error correction of quantum states in a correlated noisy channel. *Physical Review Letters*, 111:180502, 2013.

[157] Glenn A. Tyler and Robert W. Boyd. Influence of atmospheric turbulence on the propagation of quantum states of light carrying orbital angular momentum. *Optics Letters*, 34(2):142–144, 2009.

[158] A. A. Semenov and W. Vogel. Quantum light in the turbulent atmosphere. *Physical Review A*, 80(2):021802(R), 2009.

[159] Robert W. Boyd, Brandon Rodenburg, Mohammad Mirhosseini, and Stephen Barnett. Influence of atmospheric turbulence on the propagation of quantum states of light using plane-wave encoding. *Optics Express*, 19(19):18310–18317, 2011.

[160] Cosmo Lupo, Vittorio Giovannetti, Stefano Pirandola, Stefano Mancini, and Seth Lloyd. Enhanced quantum communication via optical refocusing. *Physical Review A*, 84(1):010303(R), 2011.

[161] Cosmo Lupo, Vittorio Giovannetti, Stefano Pirandola, Stefano Mancini, and Seth Lloyd. Capacities of linear quantum optical systems. *Physical Review A*, 85(6):062314, 2012.

[162] M. Horodecki, P. W. Shor, and M. B. Ruskai. Entanglement Breaking Channels. *Reviews in Mathematical Physics*, 15(6):629–641, 2003.

[163] A. S. Holevo. Entanglement-breaking channels in infinite dimensions. *Problems of Information Transmission*, 44(3), 2008.

[164] Stefano Pirandola, Carlo Ottaviani, Christian S. Jacobsen, Gaetana Spedalieri, Samuel L. Braunstein, Tobias Gehring, and Ulrik L. Andersen. Non-Markovian Reactivation of Quantum Relays. *arXiv*, 1505.07457, 2015.

[165] Stefano Pirandola. Entanglement reactivation in separable environments. *New Journal of Physics*, 15:113046, 2013.

[166] Géza Giedke, Barbara Kraus, Maciej Lewenstein, and Ignacio J. Cirac. Separability properties of three-mode Gaussian states. *Physical Review A*, 64(5):052303, 2001.

[167] Benjamin Schumacher and M. A. Nielsen. Quantum data processing and error correction. *Physical Review A*, 54(4):2629–2635, 1996.

[168] Seth Lloyd. Capacity of the noisy quantum channel. *Physical Review A*, 55(3):1613–1622, 1997.

[169] Raúl García-Patrón and Nicolas J Cerf. Continuous-variable quantum key distribution protocols over noisy channels. *Physical Review Letters*, 102(13):130501, 2009.

[170] Christian S. Jacobsen, Tobias Gehring, and Ulrik L. Andersen. Continuous Variable Quantum Key Distribution with a Noisy Laser. *Entropy*, 17(7):4654–4663, 2015.

[171] Charles Ci Wen Lim, Marcos Curty, Nino Walenta, Feihu Xu, and Hugo Zbinden. Concise security bounds for practical decoy-state quantum key distribution. *Physical Review A*, 89(2):022307, 2014.

[172] Vladyslav C. Usenko and Frédéric Grosshans. Unidimensional continuous-variable quantum key distribution. *Physical Review A*, 92(6):062337, 2015.

[173] Tobias Gehring, Christian S. Jacobsen, and Ulrik L. Andersen. Single-Quadrature Continuous-Variable Quantum Key Distribution. *Quantum Information and Computation*, 16(13-14):16, 1081–1095.

[174] S. F. Pereira, Z. Y. Ou, and H. J. Kimble. Quantum communication with correlated nonclassical states. *Physical Review A*, 62(4):42311, 2000.

[175] Christian S. Jacobsen, Lars S. Madsen, Vladyslav C. Usenko, Radim Filip, and Ulrik L. Andersen. Elimination of information leakage in quantum information channels. *arXiv*, 1408:4566, 2014.

[176] Michael Naehrig, Kristin Lauter, and Vinod Vaikuntanathan. Can homomorphic encryption be practical? In *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop*, pages 113–124, New York, NY, USA, 2011. ACM.

[177] Ronald L. Rivest, Leonard M. Adleman, and Michael L. Dertouzos. On data banks and privacy homomorphisms. In *Foundations of Secure Computation*, volume 4, pages 169–180, 1978.

[178] Craig Gentry. *A fully homomorphic encryption scheme.* PhD thesis, Stanford University, 2009.

[179] Si-Hui Tan, Joshua A. Kettlewell, Yingkai Ouyang, Lin Chen, and Joseph F. Fitzsimons. A quantum approach to homomorphic encryption. *arXiv*, 1411:5254, 2015.

[180] Li Yu, Carlos A. Pérez-Delgado, and Joseph F. Fitzsimons. Limitations on information-theoretically-secure quantum homomorphic encryption. *Physical Review A*, 90(5):050303, 2014.

[181] A. M. Childs. Secure assisted quantum computation. *Quantum Information and Computation*, 5(6):456–466, 2005.

[182] IBM quantum computer. `http://www.research.ibm.com/quantum/`. Accessed: 2016-07-28.

[183] A. Broadbent, J. Fitzsimons, and E. Kashefi. Universal blind quantum computation. In *Foundations of Computer Science, 2009. FOCS '09. 50th Annual IEEE Symposium on*, pages 517–526, Oct 2009.

[184] Tomoyuki Morimae. Continuous-variable blind quantum computation. *Physical Review Letters*, 109:230502, Dec 2012.

[185] Tomoyuki Morimae and Keisuke Fujii. Blind topological measurement-based quantum computation. *Nature Communications*, 3:1036, 2012.

[186] Carlos A. Pérez-Delgado and Joseph F. Fitzsimons. Iterated gate teleportation and blind quantum computation. *Physical Review Letters*, 114:220502, Jun 2015.

[187] Vedran Dunjko, Elham Kashefi, and Anthony Leverrier. Blind quantum computing with weak coherent pulses. *Physical Review Letters*, 108:200502, May 2012.

[188] Stefanie Barz, Elham Kashefi, Anne Broadbent, Joseph F. Fitzsimons, Anton Zeilinger, and Philip Walther. Demonstration of blind quantum computing. *Science*, 335(6066):303–308, 2012.

[189] Vittorio Giovannetti, Lorenzo Maccone, Tomoyuki Morimae, and Terry G. Rudolph. Efficient universal blind quantum computation. *Physical Review Letters*, 111:230501, Dec 2013.

[190] Qin Li, Wai Hong Chan, Chunhui Wu, and Zhonghua Wen. Triple-server blind quantum computation using entanglement swapping. *Phys. Rev. A*, 89:040302, Apr 2014.

[191] K. A. G. Fisher, A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. J. Resch. Quantum computing on encrypted data. *Nature Communications*, 5:3074, 2014.

[192] Seth Lloyd and Samuel L. Braunstein. Quantum computation over continuous variables. *Physical Review Letters*, 82:1784–1787, Feb 1999.

[193] Nicolas C. Menicucci, Peter van Loock, Mile Gu, Christian Weedbrook, Timothy C. Ralph, and Michael A. Nielsen. Universal quantum computation with continuous-variable cluster states. *Physical Review Letters*, 97:110501, Sep 2006.

[194] Kevin Marshall, Christian S. Jacobsen, Clemens Schäfermeier, Tobias Gehring, Christian Weedbrook, and Ulrik L. Andersen. Practical Quantum Computing on Encrypted Data. *arXiv*, 1607:07372, 2016.

[195] Petr Marek, Radim Filip, and Akira Furusawa. Deterministic implementation of weak quantum cubic nonlinearity. *Physical Review A*, 84:053802, 2011.

[196] Kevin Marshall, Raphael Pooser, George Siopsis, and Christian Weedbrook. Repeat-until-success cubic phase gate for universal continuous-variable quantum computation. *Physical Review A*, 91:032321, Mar 2015.

[197] Yfke Dulek, Christian Schaffner, and Florian Speelman. Quantum homomorphic encryption for polynomial-sized circuits. *arXiv*, 1603:09717, 2016.

[198] Sergey Bravyi and Alexei Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Physical Review A*, 71(2):022316, 2005.

[199] Anne Broadbent and Stacey Jeffery. Quantum homomorphic encryption for circuits of low t-gate complexity. In *Advances in Cryptology - CRYPTO 2015*, pages 609–629, 2015.

[200] Seckin Sefi and Peter van Loock. How to decompose arbitrary continuous-variable quantum operations. *Phys. Rev. Lett.*, 107:170501, Oct 2011.

[201] Jun-ichi Yoshikawa, Yoshichika Miwa, Alexander Huck, Ulrik L. Andersen, Peter van Loock, and Akira Furusawa. Demonstration of a quantum nondemolition sum gate. *Physical Review Letters*, 101:250501, Dec 2008.

[202] Ryuji Ukai, Shota Yokoyama, Jun-ichi Yoshikawa, Peter van Loock, and Akira Furusawa. Demonstration of a controlled-phase gate for continuous-variable one-way quantum computation. *Physical Review Letters*, 107:250501, Dec 2011.

[203] Mitsuyoshi Yukawa, Kazunori Miyata, Hidehiro Yonezawa, Petr Marek, Radim Filip, and Akira Furusawa. Emulating quantum cubic nonlinearity. *Physical Review A*, 88:053816, Nov 2013.

[204] Kazunori Miyata, Hisashi Ogawa, Petr Marek, Radim Filip, Hidehiro Yonezawa, Jun-ichi Yoshikawa, and Akira Furusawa. Experimental realization of a dynamic squeezing gate. *Physical Review A*, 90:060302, Dec 2014.

[205] Nicolas Sangouard, Christoph Simon, Hugues de Riedmatten, and Nicolas Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Reviews of Modern Physics*, 83:33–80, Mar 2011.

List of Publications

2014

Articles

1. **Christian S. Jacobsen**, Lars S. Madsen, Vladyslav Usenko, Radim Filip, Ulrik L. Andersen, "Elimination of Information Leakage in Lossy Quantum Communication Channels", arXiv: 1408.4566

Educational talks

1. **Christian S. Jacobsen**, "Laserlys og kvantekommunikation", Danish Science Week 2014

Posters

1. "Elimination of Information Leakage in Lossy Quantum Communication Channels" for QCrypt 2014, Paris

2015

Articles

1. Stefano Pirandola, Carlo Ottaviano, Gaetana Spedalieri, Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias Gehring, **Christian S. Jacobsen** and Ulrik L. Andersen,"High-rate measurement-device-independent quantum cryptography", Nature Photonics, **9**, 397

2. **Christian S. Jacobsen**, Tobias Gehring, Ulrik L. Andersen, "Continuous Variable Quantum Key Distribution with a Noisy Laser", Entropy, **17**, 4654

3. Stefano Pirandola, Carlo Ottaviani, **Christian S. Jacobsen**, Gaetana Spedalieri, Samuel L. Braunstein, Tobias Gehring and Ulrik L. Andersen, "Non-Markovian Reactivation of Quantum Relays", arXiv:1505.07457

Popular science contributions

1. **Christian S. Jacobsen**, Tobias Gehring, Ulrik L. Andersen, "Kvantemekanik bruges til super sikker kommunikation", `http://videnskab.dk/teknologi/kvantemekanik-bruges-til-super-sikker-kommunikation` (in Danish)

Educational talks

1. **Christian S. Jacobsen**, "Laserlys og kvantekommunikation", Danish Science Week 2015

Posters

1. "Continuous Variable Quantum Key Distribution using Thermal States" for the Macroscopic Quantum Coherence Workshop 2015, St. Andrews

2. "High-rate measurement-device-independent quantum cryptography", QCrypt 2015, Tokyo

2016

Articles

1. Tobias Gehring, **Christian S. Jacobsen**, Ulrik L. Andersen, "Single Quadrature Continuous-Variable Quantum Key Distribution", Journal of Quantum Information and Computation, 16(14), 1081–1095

2. Kevin Marshall, **Christian S. Jacobsen**, Tobias Gehring, Christian Weedbrook, Ulrik L. Andersen, "Practical Quantum Computing on Encrypted Data", Nature Communications, arXiv:1607.07372

Conference talks

1. Kevin Marshall, **Christian S. Jacobsen**, Tobias Gehring, Christian Weedbrook, Ulrik L. Andersen, "Continuous Variable Quantum Computing on Encrypted Data", Trustworthy Quantum Information 2016 workshop, Shanghai