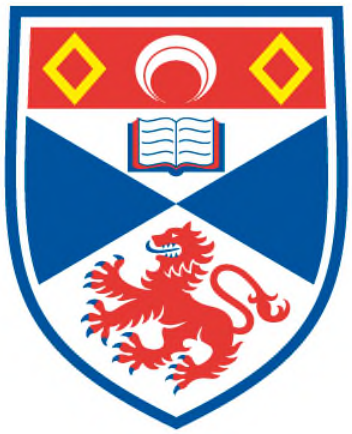
QUANTUM CORRELATIONS IN CONTINUOUS VARIABLE MIXED STATES

FROM DISCORD TO SIGNATURES

Callum Croal

A Thesis Submitted for the Degree of PhD
at the
University of St Andrews



2016

Quantum Correlations in Continuous Variable Mixed States

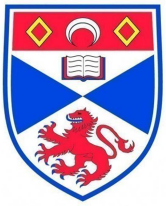
From Discord to Signatures

by

Callum Croal

Submitted for the degree of Doctor of Philosophy in Theoretical Physics

20th May 2016



University
of
St Andrews

Declaration

I, Callum Croal, hereby certify that this thesis, which is approximately 41000 words in length, has been written by me, or principally by myself in collaboration with others as acknowledged, that it is the record of work carried out by me and that it has not been submitted in any previous application for a higher degree.

Date Signature of candidate

I was admitted as a candidate for the degree of PhD in September 2012; the higher study for which this is a record was carried out in the University of St Andrews between 2012 and 2016.

Date Signature of candidate

I hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of PhD in the University of St Andrews and that the candidate is qualified to submit this thesis in application for that degree.

Date Signature of supervisor

Copyright Agreement

In submitting this thesis to the University of St Andrews I understand that I am giving permission for it to be made available for use in accordance with the regulations of the University Library for the time being in force, subject to any copyright vested in the work not being affected thereby. I also understand that the title and the abstract will be published, and that a copy of the work may be made and supplied to any bona fide library or research worker, that my thesis will be electronically accessible for personal or research use unless exempt by award of an embargo as requested below, and that the library has the right to migrate my thesis into new electronic forms as required to ensure continued access to the thesis. I have obtained any third-party copyright permissions that may be required in order to allow such access and migration, or have requested the appropriate embargo below.

The following is an agreed request by candidate and supervisor regarding the electronic publication of this thesis: Access to Printed copy and electronic publication of thesis through the University of St Andrews.

Date Signature of candidate

Date Signature of supervisor

Publications

The following is a list of publications that have arisen as a result of the research of this thesis.

(CCI) V. Chille, N. Quinn, C. Peuntinger, C. Croal, L. Mišta, C. Marquardt, G. Leuchs and N. Korolkova,
Quantum nature of Gaussian discord: experimental evidence and role of system-environment correlations,
Phys. Rev. A **91**, 050301(R) (2015).

(CCII) C. Croal, C. Peuntinger, V. Chille, C. Marquardt, G. Leuchs, N. Korolkova and L. Mišta,
Entangling the whole by beamsplitting a part,
Phys. Rev. Lett. **115**, 190501 (2015).

(CCIII) N. Quinn, C. Croal and N. Korolkova,
Quantum discord and entanglement distribution as the flow of correlations through a dissipative quantum system,
Journal of Russian Laser Research **36**, 550 (2015).

Manuscripts in Preparation

- C. Croal, C. Peuntinger, B. Heim, I. Khan, C. Marquardt, G. Leuchs, P. Wallden, E. Andersson and N. Korolkova,
  Free-space quantum signatures using heterodyne measurements,
  Submitted to Physical Review Letters.

Conference Presentations

The following is a list of conferences in which I have taken part.

1. 20$^{\text{th}}$ Central European Workshop on Quantum Optics (CEWQO 2013), Stockholm, Sweden, 2013, Poster Presentation.
2. Summer School on Quantum Optics and Nanophotonics, Les Houches, France, 2013, Poster Presentation.
3. Quantum Information Scotland (QUISCO), St Andrews, Scotland, 2013, Oral Presentation.
4. CLEO: QELS, San Jose, California, USA, 2014, Oral Presentation.
5. 21$^{\text{st}}$ Central European Workshop on Quantum Optics (CEWQO 2014), Brussels, Belgium, 2014, Oral Presentation.
6. W. E. Heraeus Seminar on Quantum Correlations Beyond Entanglement, Bad Honnef, Germany, 2015, Poster Presentation.
7. Workshop on Macroscopic Quantum Coherence, St Andrews, Scotland, 2015, Poster Presentation.
8. 22$^{\text{nd}}$ Central European Workshop on Quantum Optics (CEWQO 2015), Warsaw, Poland, 2015, Oral Presentation.

Research Visits

- Palacký University, Olomouc, Czech Republic, January 2013.
- University of Waterloo, Ontario, Canada, May-June 2014.
- Max Planck Institute for the Science of Light, Erlangen, Germany, May 2015.

Collaboration Statement

This thesis is the result of my own work carried out at the University of St Andrews between September 2012 and March 2016. Parts of the work presented in this thesis have been published in refereed scientific journals. In all cases the text in the chapters has been written entirely by me. All figures, unless explicitly stated in the text, have been produced by me.

- Chapter 3 is an extension of (CCI) with some work included from (CCIII). The theoretical work for Sections 3.2 and 3.4 was carried out in collaboration with N. Quinn and L. Mišta. The experimental results in Section 3.2 were provided by V. Chille, C. Peuntinger, C. Marquardt and G. Leuchs. The work presented in Sections 3.3, 3.5 and 3.6 is my own with assistance provided by Norbert Lütkenhaus and Marco Piani.

- Chapter 4 is an extension of (CCII). L. Mista developed the original idea for the project and I performed further theoretical analysis in collaboration with him. C. Peuntinger, V. Chille, C. Marquardt and G. Leuchs provided the experimental results for this chapter and aided with analysis of these results.

- Chapter 5 is a description of work performed for the manuscript in preparation entitled "Free-space quantum signatures using homodyne measurements". The protocol was developed in collaboration with P. Wallden and E. Andersson. C. Peuntinger, B. Heim, I. Khan, C. Marquardt and G. Leuchs performed the experiment. I carried out analysis of the obtained data in collaboration with C. Peuntinger.

The work in all chapters has been supported by my supervisor Dr Natalia Korolkova.

Abstract

This thesis studies continuous variable mixed states with the aim of better understanding the fundamental behaviour of quantum correlations in such states, as well as searching for applications of these correlations. I first investigate the interesting phenomenon of discord increase under local loss and explain the behaviour by considering the non-orthogonality of quantum states. I then explore the counter-intuitive result where entanglement can be created by a passive optical beamsplitter, even if the input states are classical, as long as the input states are part of a larger globally nonclassical system. This result emphasises the importance of global correlations in a quantum state, and I propose an application of this protocol in the form of quantum dense coding.

Finally, I develop a quantum digital signature protocol that can be described entirely using the continuous variable formalism. Quantum digital signatures provide a method to ensure the integrity and provenance of a message using quantum states. They follow a similar method to quantum key distribution (QKD), but require less post-processing, which means they can sometimes be implemented over channels that are inappropriate for QKD. The method I propose uses homodyne measurement to verify the signature, unlike previous protocols that use single photon detection. The single photon detection of previous methods is designed to give unambiguous results about the signature, but this comes at the cost of getting no information much of the time. Using homodyne detection has the advantage of giving results all the time, but this means that measurement results always have some ambiguity. I show that, even with this ambiguity, the signature protocol based on homodyne measurement outperforms previous protocols, with the advantage enhanced when technical considerations are included. Therefore this represents an interesting new direction in the search for a practical quantum digital signature scheme.

Acknowledgements

There are many people without whom the work in this thesis would not have been possible. I'd first like to thank my supervisor Dr Natalia Korolkova for her support and guidance throughout the duration of my PhD. I would also like to thank Dr Ladislav Mišta for sharing his expertise about all things related to quantum optics and quantum correlations. A thank you also goes to everyone I have collaborated with for sharing their knowledge and experience with me. In particular I would like to thank Christian Peuntinger for explaining the intricacies of a quantum optics experiment and teaching me how to use Python for data analysis. A thank you also goes to all my friends in St Andrews for making the last few years an enjoyable experience, even on those occasions when the work wasn't going very well. I would especially like to thank my family, especially Mum, Dad and Lyndsey, for their support and encouragement over the years; without them I would surely not be here today. Finally, and most importantly, I would like to thank Jo for her unwavering support and belief in me. She brings me confidence at work and happiness at home, without which life would not be the same.

Contents

1 Introduction

Towards the end of the 19th century, the classical theories of mechanics, thermodynamics and electromagnetism were considered to be the most important in physics. These theories all shared the common principle of determinism. That is, if one knows the initial conditions of a system one can exactly predict all future behaviour. However, this idea was completely turned on its head at the start of the 20th century with the advent of quantum theory, which introduced quantum uncertainty as an inherent property of all quantum systems. Heisenberg described this with his uncertainty principle, in which a measurement on one observable will often give a second observable unpredictable results. In particular, one can never know both the position and momentum of a quantum particle exactly.

Perhaps the strangest feature of a quantum state is the possibility of non-local behaviour [19], which is impossible in the classical realm. This seems to contradict Einstein's theory of special relativity, which states that no interaction can propagate faster than the speed of light. However due to the indeterministic nature of quantum mechanics, it can coexist with relativity without conflict. The first mathematical description of non-local correlations was the idea of quantum entanglement. In an entangled state of two particles, the individual particles cannot be said to have their own properties. Instead, we can only describe the global properties of the state. The result of this is that a measurement on one particle will instantaneously change the state of the other particle, no matter how far apart they are. However, whoever possesses the other particle cannot tell that the state has changed until he knows the measurement results on the first particle, which can only be learnt through the transmission of a conventional message. Therefore the transfer of information is limited by the speed of light, which is consistent with special relativity. Nevertheless, this is a counterintuitive result and the mechanism by which it occurs is still a matter of debate. However the result is undeniable and is regularly observed in laboratories throughout the world, for example in tests of Bell's inequalities [13, 14].

One of the fundamental questions still unanswered is, how do we define the boundary between the classical and quantum worlds? For a long time, entanglement was considered as the defining property of a multipartite quantum state. However experiments have shown that some multipartite states that are not entangled can still show signs of quantum

behaviour [20]. In fact entanglement, non-locality and non-classicality are only equivalent for pure quantum states. In the more general case of a mixed quantum state, we require a new description of non-classicality. This has led to the introduction of quantum discord [158] as an attempt to describe all non-classical correlations in a general mixed quantum state.

Quantum information theory is the attempt to use non-classical correlations to manipulate information as we desire. Correlations could potentially be used to carry out secure communication and faster computation, amongst other things. Entanglement has been identified as a useful resource for quantum communication [118], however its necessity for mixed state quantum computation is unclear [54]. Recently quantum discord has also been shown to have potential uses in computation [136], and it could also have applications in quantum metrology [32]. Quantum infomation theory can be studied in either discrete variables, e.g. qubits and single photons, or continuous variables, e.g. light modes. This thesis focuses on the continuous variable case.

This thesis has two main aims. Quantum correlations between two states have been extensively studied; however, when correlations are shared between three or more states they are less well understood. I investigate quantum correlations in multimode mixed states with the aim of further understanding the fundamental behaviour of entanglement and quantum discord in these conditions. Understanding this behaviour is necessary as quantum protocols are developed that work in the real world, which inevitably involves mixed states. The second aim of this thesis is to advance the field of quantum digital signatures by developing a new signature protocol based on coherent states and homodyne detection, whereas previous protocols are based on single photon detection. Such protocols could become a widespread part of future quantum communication networks due to the importance of digital signatures.

The structure of this thesis is as follows. Chapter 1 gives an introduction to quantum optics and provides the main tools required to study continuous variable systems in this thesis. Chapter 2 introduces the theory of entanglement, including how it can be identified and quantified. Chapter 2 also introduces nonclassical correlations beyond entanglement, with a focus on quantum discord. In Chapter 3, I investigate the phenomenon of discord increase under local loss, and seek to identify the primary physical reason for the increase. In Chapter 4, I study situations where entanglement can be created by a beamsplitter, even if the modes input to the beamsplitter are classical. I then provide an application for this process in terms of dense coding. In Chapter 5, I introduce the field of quantum digital signatures and describe the most important developments in the field so far. I then propose a quantum digital signature protocol based on homodyne measurements, opening up the study of quantum digital signatures to protocols entirely working with continuous variables.

1.1 Introduction to Quantum Optics

In 1900, Planck asserted that light is a quantum object in his explanation of blackbody radiation [26]. Light shows wave-like properties, for example diffraction and interference. It can also be shown to have a particle nature, i.e. photons, as shown by Einstein in his description of the photoelectric effect [63]. Light also has a great ability to carry information and is used in telecommunication today. The quantum nature of light as well as its ability to contain information makes it an ideal candidate for studying quantum information theory. The basics of quantum optics, the quantum language of light, have been discussed in many excellent resources [137, 39, 77]. Here I introduce those parts that are most relevant to our investigation of continuous variable quantum information theory.

1.1.1 Quantisation of the electromagnetic field

I begin with a classical description of electromagnetism. In a dielectric medium the physical quantities of light are described by the electromagnetic field strengths, the electric field $\mathbf{E}$, the displacement field $\mathbf{D}$, the magnetic field $\mathbf{H}$ and the magnetic induction $\mathbf{B}$. These are then linked by the constitutive equations, $\mathbf{D} = \epsilon\epsilon_\mathbf{0}\mathbf{E}$ and $\mathbf{B} = \mu\mu_\mathbf{0}\mathbf{H}$, where ϵ_0 is the permittivity of free space, ϵ is the permittivity of the material, μ_0 is the permeability of free space and μ is the permeability of the material. In his seminal work, Maxwell linked these together to give his famous equations which can be written in differential form as

$$\nabla \cdot \mathbf{D} = 0, \quad \nabla \cdot \mathbf{B} = 0, \quad \nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}, \quad \nabla \times \mathbf{H} = \frac{\partial \mathbf{D}}{\partial t}, \tag{1.1}$$

with the additional boundary conditions that the fields vanish at infinity. Note that these Maxwell's equations apply in regions with zero charges or currents.

Together with Newtonian mechanics, Maxwell's equations represented a period where it was thought that everything was deterministic and it was only a matter of time before Physics would provide a complete description of the universe. With the observations of Planck and Einstein in the early 20th century, it became clear that this was no longer true, and in fact quantum uncertainty must play a role. To convert Maxwell's equations into the quantum regime, we can make the simple assumption that the classical fields are in fact the expectation values of the quantum observables, e.g. $\langle \hat{\mathbf{E}} \rangle = \mathbf{E}$. Using this assumption it can be seen that due to their linearity, Maxwell's equations still hold for the quantum field strengths. Thus, simply by replacing the electric field strengths with their quantum equivalents, we can use Maxwell's equations to describe the quantum behaviour of light.

In classical electromagnetism the field strengths are often represented by the vector potential. We can do the same in the quantum case by introducing the operator of the vector potential $\hat{\mathbf{A}}$. In doing this, we assume that the fields can be rewritten as

$$\hat{\mathbf{E}} = -\frac{\partial \hat{\mathbf{A}}}{\partial t}, \qquad \hat{\mathbf{B}} = \nabla \times \hat{\mathbf{A}}. \tag{1.2}$$

By doing this, the middle two Maxwell's equations immediately hold. Since the electromagnetic field is gauge invariant we can introduce the Coulomb gauge

$$\nabla \cdot \epsilon \hat{\mathbf{A}} = 0, \tag{1.3}$$

which ensures that the first of Maxwell's equations also holds. Finally by rewriting the final Maxwell's equation in terms of the vector potential, we obtain the wave equation

$$\nabla^2 \hat{\mathbf{A}} - \frac{1}{c^2}\frac{\partial^2 \hat{\mathbf{A}}}{\partial t^2} = 0. \tag{1.4}$$

In deriving this equation, the speed of propagation of electromagnetic waves in a vacuum emerges as $c = 1/\sqrt{\mu_0 \epsilon_0}$.

We can now express the vector potential $\hat{\mathbf{A}}$ as a mode expansion by writing

$$\hat{\mathbf{A}}(\mathbf{r}, t) = \sum_k \left(\mathbf{A}_k(\mathbf{r}, t)\hat{a}_k + \mathbf{A}_k^*(\mathbf{r}, t)\hat{a}_k^\dagger \right). \tag{1.5}$$

In this expression, $\mathbf{A}_k(\mathbf{r}, t)$ forms a complete set of classical waves that obey the Coulomb gauge (1.3), Maxwell's equations (1.1) and the boundary conditions. For example the plane waves $A\exp(i\mathbf{k}\cdot\mathbf{r} - i\omega t)$ satisfy all these conditions. All of the quantumness of light is contained in the operators $\hat{a}_k^\dagger$ and $\hat{a}_k$, which are the creation and annihilation operators of mode k respectively, with the imposition that they are mutually adjoint.

We can now assume, as we did with Maxwell's equations, that the quantum Hamiltonian of the electromagnetic field can be found by taking the classical expression for the Hamiltonian and replacing the electromagnetic field strengths by their operator equivalents. By doing this we find the quantum Hamiltonian to be

$$\hat{H} = \frac{1}{2}\int_V \left(\hat{\mathbf{E}} \cdot \hat{\mathbf{D}} + \hat{\mathbf{B}} \cdot \hat{\mathbf{H}} \right) dV \tag{1.6}$$

with the volume integral taken over the entire space. By using the constitutive equations, writing in terms of the vector potential (1.2) and inserting the mode expansion (1.5), the Hamiltonian can be written as

$$\hat{H} = \frac{1}{2}\sum_{k=0}^{\infty} \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \hat{a}_k \hat{a}_k^\dagger \right). \tag{1.7}$$

Finally, we can use the Bose commutation relation [137]

$$\left[\hat{a}_k, \hat{a}_{k'}^\dagger \right] = \delta_{k,k'} \tag{1.8}$$

to write the Hamiltonian as

$$\hat{H} = \sum_{k=0}^{\infty} \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2} \right). \tag{1.9}$$

The electromagnetic field energy is thus the sum of the energies of the individual modes. The bosonic operators $\hat{a}_k$ and $\hat{a}_k^\dagger$ can be thought of as the annihilation and creation operators of photons respectively in mode k. An important result of the quantisation process is that the vacuum state $|0\rangle$, that is the state with no photons, has non-zero energy. This can be seen by calculating the energy in the vacuum as $\langle 0|\hat{H}|0\rangle = \sum_{k=0}^{\infty} \frac{\hbar\omega_k}{2}$, which is clearly non-zero. In fact, the energy is infinite, which is usually dealt with by some renormalisation process. This result is a manifestation of Heisenberg's uncertainty principle, a consequence of which is that the vacuum contains random fluctuations. The

result is that the electromagnetic field possesses energy even when there are no photons present. This is known as the zero-point energy and results in experimentally confirmed phenomena, for example the Casimir force [36], which causes two parallel conductors separated by the vacuum to feel an attractive force.

Now that the electromagnetic field is quantised and creation/annihilation operators have been introduced we can move onto alternative representations of continuous variable quantum states. In what follows, $\hbar = 1$ unless otherwise stated.

1.1.2 Quadrature states

In the following discussion I restrict to single mode representations where the subscript k has been dropped for convenience. I start by introducing the quadrature operators $\hat{x}$ and $\hat{p}$, which can be written in terms of the creation and annihilation operators as

$$\hat{x} = \frac{1}{\sqrt{2}}\left(\hat{a}^\dagger + \hat{a}\right), \quad \hat{p} = \frac{i}{\sqrt{2}}\left(\hat{a}^\dagger - \hat{a}\right). \tag{1.10}$$

These quadratures are often considered to be the in-phase and out-of-phase components of the electric field amplitude with respect to a reference phase. The operators are canonically conjugate and satisfy the commutation relation

$$[\hat{x}, \hat{p}] = i. \tag{1.11}$$

Although these operators have no relation to the position and momentum of a photon, this commutation relation allows us to treat $\hat{x}$ and $\hat{p}$ as perfect examples of position and momentum-like properties. In fact, by expressing the photon number operator $\hat{n} = \hat{a}^\dagger\hat{a}$ in terms of the quadrature operators, we obtain the equation

$$\hat{H} \equiv \hat{n} + \frac{1}{2} = \frac{\hat{x}^2}{2} + \frac{\hat{p}^2}{2}. \tag{1.12}$$

This equation represents the energy of a quantum harmonic oscillator of unity mass and frequency; the single mode is thus the electromagnetic oscillator with position $\hat{x}$ and momentum $\hat{p}$!

We can now introduce the quadrature states $|x\rangle$ and $|p\rangle$ as the eigenstates of the quadrature operators. That is

$$\hat{x}|x\rangle = x|x\rangle, \quad \hat{p}|p\rangle = p|p\rangle. \tag{1.13}$$

These states are both orthogonal and complete:

$$\langle x|x'\rangle = \delta(x - x'), \quad \langle p|p'\rangle = \delta(p - p'), \quad \int_{-\infty}^{\infty} |x\rangle\langle x|dx = \int_{-\infty}^{\infty} |p\rangle\langle p|dp = 1 \tag{1.14}$$

and are linked together by the Fourier transformation

$$|x\rangle = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} \exp(-ixp)|p\rangle dp, \quad |p\rangle = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} \exp(+ixp)|x\rangle dx. \tag{1.15}$$

These quadrature states are not physical as they are not truly normalisable, however they

can be used to define the quadrature wave functions

$$\psi(x) = \langle x|\psi\rangle, \quad \widetilde{\psi}(p) = \langle p|\psi\rangle. \tag{1.16}$$

Unlike the quadrature states, these are physical with their moduli squared giving the probability distributions of the pure state $|\psi\rangle$ for each of the quadratures.

1.1.3 Coherent states

Ideal laser light is a coherent electromagnetic wave that is the closest possible analogue to a classical electromagnetic wave. Since it has a well-defined amplitude the coherent states are defined as those that are eigenstates of the annihilation, or amplitude, operator $\hat{a}$,

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle. \tag{1.17}$$

Coherent states were first suggested by Schrödinger [179] as a response to a claim by Lorentz that quantum mechanics was not consistent with classical behaviour of light. They were then considered in mathematical detail by Roy J. Glauber [90, 88], which is why coherent states are sometimes known as Glauber states.

It can be seen that the photon number distribution for a coherent state is given by the Poissonian distribution as

$$p_n = \frac{|\alpha|^{2n}}{n!}e^{-|\alpha|^2}. \tag{1.18}$$

This is exactly the same probability distribution that we would get from a set of randomly distributed classical particles. Therefore a Poissonian distribution is essentially classical which allows us to say that coherent states give us the most classical quantum description of light.

It is important to note that the quantum vacuum is itself a coherent state, as it satisfies Eqn. (1.17) for $\alpha = 0$. To more clearly examine the link between the vacuum and coherent states, consider the displacement operator

$$\hat{D}(\alpha) = \exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a}). \tag{1.19}$$

Using this operator, a coherent state can be written, and therefore thought of, as a displaced vacuum state

$$|\alpha\rangle = \hat{D}(\alpha)|0\rangle. \tag{1.20}$$

To study this link in more detail, we can break up the amplitude α into its real and imaginary parts

$$\alpha = \frac{1}{\sqrt{2}}(x_0 + ip_0), \tag{1.21}$$

and therefore express the displacement operator in terms of the quadratures

$$\hat{D} = \exp(ip_0\hat{x} - ix_0\hat{p}). \tag{1.22}$$

The values of x_0 and p_0 are the displacements of the vacuum in the amplitude and phase quadratures respectively. By varying these two values, it is possible to create any possible coherent state. Using this operator and the fact that coherent states are just displaced

vacuum states, we obtain the position wave function of a coherent state

$$\psi_\alpha(x) = \pi^{-1/4} \exp\left(-\frac{(x-x_0)^2}{2} + ip_0x - \frac{ip_0x_0}{2}\right). \tag{1.23}$$

Similarly, the momentum wave function is

$$\tilde{\psi}_\alpha(p) = \pi^{-1/4} \exp\left(-\frac{(p-p_0)^2}{2} - ix_0p + \frac{ip_0x_0}{2}\right). \tag{1.24}$$

These wavefunctions show us that the quadrature probability distributions $|\psi_\alpha(x)|^2$ and $|\tilde{\psi}_\alpha(p)|^2$ are Gaussian with the same width as the vacuum; they are simply shifted by the real values x_0 and p_0. This means that only vacuum noise, which is impossible to eliminate, disturbs the quadrature amplitudes of a coherent state. Therefore coherent states possess the minimum possible uncertainty allowed by quantum mechanics. This is part of the reason that coherent states are such a valuable experimental tool.

1.1.4 Squeezed states

One of the basic assertions of quantum mechanics is that all quantum systems inherently contain uncertainty. In quantum optics this is demonstrated by Heisenberg's uncertainty principle [104]

$$\Delta x \Delta p \geq \frac{1}{2}. \tag{1.25}$$

In a vacuum or coherent state we know that the position and momentum quadratures have the same uncertainty and Heisenberg's uncertainty principle is saturated. This means the uncertainties in the x and p-quadratures are given by $\Delta x = \Delta p = 1/\sqrt{2}$.

States that saturate Eqn. (1.25) are called minimum uncertainty states for obvious reasons. Previously, we saw that coherent states are such states with equal uncertainty in the position and momentum quadratures; however these are not the only type of minimum uncertainty state. In a brilliantly simple proof [163] (translation [164]), Pauli demonstrated that a minimum uncertainty state $|\phi\rangle$ that saturates Eqn. (1.25) must also satisfy the equation

$$\frac{1}{2}\frac{x}{\Delta^2 x}\phi(x) + \frac{\partial}{\partial x}\phi(x) = 0 \tag{1.26}$$

where $\Delta^2 x$ is the variance of the position quadrature. Eqn.(1.26) allows us to have states where the variance in one quadrature reduces below $1/2$ as long as the variance in the conjugate quadrature increases accordingly. States of this form are known as squeezed states and are important in many quantum protocols.

To parametrise the squeezing I introduce the real parameter r so the variances can be written as

$$\Delta^2 x = \frac{1}{2}e^{-2r}, \quad \Delta^2 p = \frac{1}{2}e^{2r}. \tag{1.27}$$

Just as coherent states can be expressed as displaced vacuum states, so squeezed states can be expressed as squeezed vacuum states by introducing the squeezing operator

$$\hat{S}(r) = \exp\left[\frac{r}{2}\left(\hat{a}^2 - \hat{a}^{\dagger 2}\right)\right]. \tag{1.28}$$

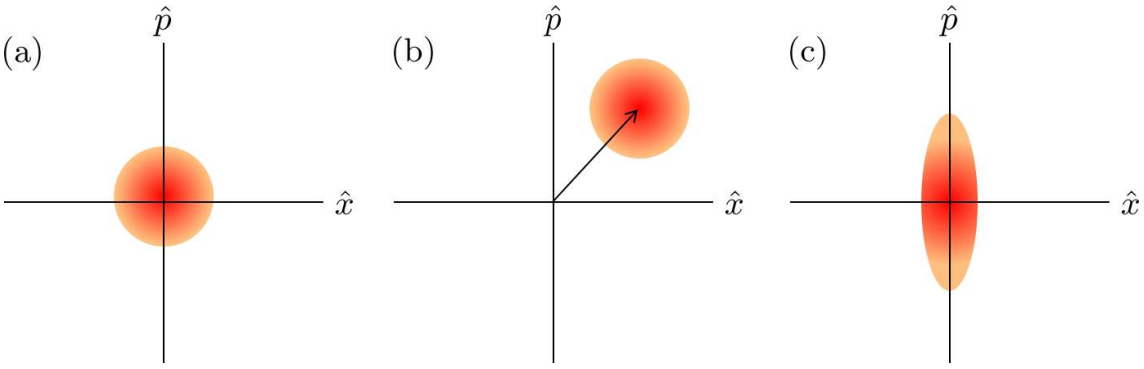


Figure 1.1: On a plot of position x and momentum p, a classical system could be represented as a point with an exact position and momentum. In a quantum system there is always inherent uncertainty in each of the quadratures. In the phase-space representation, the width of the ellipse in each quadrature gives the variance in that quadrature. (a) A vacuum state has equal uncertainty in each quadrature so is represented by a circle. It is also a minimum uncertainty state so the variance in each quadrature is 1/2. The vacuum state is centred on the origin. (b) A coherent state has the same uncertainty as the vacuum so can again be represented as a circle, however the coherent state is not centred on the origin. In this way we see why we can say that the coherent state is a displaced vacuum. (c) A squeezed state has reduced uncertainty in one quadrature and increased uncertainty in the other. Therefore we represent a squeezed state by an ellipse. In this case the vacuum has been squeezed in the $\hat{x}$-quadrature and anti-squeezed in the $\hat{p}$-quadrature.

Applying this operator to the vacuum results in the squeezed vacuum state

$$|\phi\rangle = \hat{S}(r)|0\rangle. \tag{1.29}$$

Applying the displacement operator to a squeezed state changes the average value of the quadratures without altering their variance. In fact, all minimum uncertainty states are displaced squeezed vacua, as long as the squeezing can take place in any direction. Due to the nonlinearity in Eqn. (1.28), squeezing is not a passive operation; it alters the number of photons in a state, which means that even a squeezed vacuum carries more energy than the vacuum itself.

Finally, it is important to note that, unlike coherent states, squeezed states are completely non-classical. The reduction of the noise in one of the quadratures is one illustration of its quantum properties. Another, is that if a squeezed vacuum is split on a beamsplitter, entanglement between the two outgoing modes is established [128, 29]. Entanglement is the strongest indicator of a quantum system, and the fact that it can be simply produced using a squeezed state, whereas it is impossible to create using passive operations on coherent states, is an obvious demonstration of the quantumness of squeezed states. Note that the quantumness of squeezed states can also be seen without the need for entanglement. This quantumness can be used, for example to implement measurements with accuracy beyond the classical limit. This nonclassicality can be observed from the photon statistics of squeezed states, for example in the second order correlation function [147].

A depiction of a vacuum state, coherent state and squeezed state in phase-space is seen in Fig. 1.1.

1.1.5 Thermal States

The final class of states introduced here is the set of thermal states. Historically a thermal state is one that is in thermal equilibrium with either its source or its environment. A

thermal state is in a state of maximal disorder so it has high entropy and is a mixed state. In the context of this work, this means that a thermal state is one that maximises the von Neumann entropy

$$S \equiv -\mathrm{Tr}(\hat{\rho}\log\hat{\rho}) \tag{1.30}$$

for fixed energy $\mathrm{Tr}(\hat{\rho}\hat{a}^\dagger\hat{a}) = \bar{n}$, where $\bar{n} \geq 0$ is the mean number of photons. The thermal state that satisfies this condition is one that has equal variance in both quadratures, where the variance depends on the mean photon number. Combining thermal states with the displacement and squeezing operators produces a class of states important for this thesis, namely the set of Gaussian states.

1.1.6 Purity

An important concept in quantum information theory is the purity of a quantum state. If a quantum state is pure it can be represented by a wavefunction $|\phi\rangle$, however if it is mixed it must be represented by a density operator $\hat{\rho}$. The purity of a quantum state $\hat{\rho}$ is defined as

$$P \equiv \mathrm{tr}(\hat{\rho}^2), \tag{1.31}$$

where P satisfies the relation $0 < P \leq 1$, with $P = 1$ corresponding to a pure state. The von-Neumann entropy $S(\hat{\rho})$ in Eq. (1.30) can also be used to differentiate between pure and mixed states, with the condition that $S(\hat{\rho}) = 0$ for pure states and $S(\hat{\rho}) > 0$ for mixed states. Since the von-Neumann entropy can be interpreted as the disorder in a system, this means that pure states have zero disorder, in other words we have perfect knowledge of pure states. Mixed states, on the other hand, always involve some classical ignorance; they are essentially an admission that we have lost information about a state. This information is lost via interactions with the unmeasured "environment" and is difficult to recover in most situations. All mixed states can be thought of as part of a larger pure state that holds all the information that has been lost to the environment. Of course in any real experiment, studied systems are constantly interacting with the environment and are therefore almost always in a mixed state. Therefore understanding the properties of mixed states, and how best to make use of them, is of vital importance in quantum information theory.

1.2 Quasiprobability distributions

1.2.1 Wigner Function

In classical mechanics, a state is entirely defined by its canonical position and momentum quadratures. The quadratures define a phase space and the dynamics of a system are defined by a trajectory in canonical phase space. For an uncertain classical system the statistics of the position x and momentum p components can be defined by a phase space distribution $W(x, p)$. This distribution gives the probability of finding a particular pair of x and p values after a simultaneous measurement. Once these results are known, a classical system is represented by a single point in phase space. In a quantum system the situation is more complicated. Heisenberg's uncertainty principle tells us that we can never precisely observe both position and momentum simultaneously. So we may think that the idea of a quantum phase space is a non-starter. However, we are familiar with using the idea of a quantum state to calculate observables despite the fact that the state has no physical meaning by itself. In the same way, we can use a quantum phase space distribution to calculate physical observables in a classical-like fashion.

Classically we consider the phase space distribution as a joint probability distribution, however in the quantum case we can no longer do this. The most obvious reason is that in the quantum case it is impossible to know both x and p at the same time, which can lead to a negative phase space distribution. Instead, this quantum phase space distribution is called a quasiprobability distribution and certain conditions are imposed on it so that it is useful for calculating observables [25]. This work follows the method of Leonhardt [137] to derive a useful form for the quasiprobability distribution describing a quantum state. In a classical probability distribution the marginal distributions give the probability distributions for the individual quadratures, i.e.

$$\int_{-\infty}^{\infty} W(x,p)dx = \mathrm{pr}(p), \qquad \int_{-\infty}^{\infty} W(x,p)dp = \mathrm{pr}(x) \tag{1.32}$$

where pr signifies a probability distribution. This is also required to hold for a quantum quasiprobability distribution. For a function to be considered a quasiprobability distribution it must also be normalised

$$\int_{-\infty}^{\infty} W(x,p)dxdp = 1 \tag{1.33}$$

and real as a representation of Hermitian operators. Finally, if the density matrix $\hat{\rho}$ describing the quantum state is rotated by an angle θ, then the quasiprobability distribution should transform as

$$W(x,p) \to W(x\cos\theta - p\sin\theta, x\sin\theta + p\cos\theta). \tag{1.34}$$

This relation means that the position probability distribution $\mathrm{pr}(x,\theta)$ can be calculated for all angles θ using the equation

$$\mathrm{pr}(x,\theta) \equiv \langle x|\hat{U}(\theta)\hat{\rho}\hat{U}^{\dagger}(\theta)|x\rangle = \int_{-\infty}^{\infty} W(x\cos\theta - p\sin\theta, x\sin\theta + p\cos\theta)dp. \tag{1.35}$$

The first part of this equation follows from the definition of a probability density, and the second part is a generalisation of equation (1.32) for any projection angle. This equation ensures that the equations in (1.32) are satisfied; $\theta = \pi/2$ reduces to the first equation and $\theta = 0$ reduces to the second. Equation (1.35) also ties $W(x,p)$ to quantum mechanics for the first time by introducing a connection to the density matrix. To fully understand the importance of this relationship, the Fourier transformed quasiprobability distribution $\tilde{W}(u,v)$, called the characteristic function, has to be introduced:

$$\tilde{W}(u,v) \equiv \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} W(x,p)\exp(-iux - ivp)dxdp, \tag{1.36}$$

as does the Fourier transformed position probability distribution

$$\tilde{\mathrm{pr}}(\xi,\theta) \equiv \int_{-\infty}^{\infty} \mathrm{pr}(x,\theta)\exp(-i\xi x)dx. \tag{1.37}$$

Inserting the second part of equation (1.35) into (1.37) results in the equation

$$\tilde{\mathrm{pr}}(\xi,\theta) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} W(x',p')\exp(-i\xi x)dxdp, \tag{1.38}$$

where x' and p' are the rotated quadratures

$$x' = x\cos\theta - p\sin\theta, \qquad p' = x\sin\theta + p\cos\theta. \tag{1.39}$$

Since $x = x'\cos\theta + p'\sin\theta$ from (1.39), the right hand side of (1.38) is just the definition of the characteristic function in a transformed coordinate system, i.e.

$$\tilde{\mathrm{pr}}(\xi,\theta) = \tilde{W}(\xi\cos\theta, \xi\sin\theta). \tag{1.40}$$

This means that the Fourier transformed position probability distribution is simply the characteristic function in polar coordinates.

We can now go back and use the first part of Eq. (1.35) to make use of the quantum nature of the quasiprobability distribution. Inserting it into Eq. (1.37) results in

$$\begin{aligned}\tilde{\mathrm{pr}}(\xi,\theta) &= \int_{-\infty}^{\infty} \langle x|\hat{U}(\theta)\hat{\rho}\hat{U}^{\dagger}(\theta)|x\rangle \exp(-i\xi\hat{x})dx \\ &= \mathrm{tr}\left\{\hat{\rho}\hat{U}^{\dagger}(\theta)\exp(-i\xi\hat{x})\hat{U}(\theta)\right\}.\end{aligned} \tag{1.41}$$

Now, since the second line of this equation causes a rotation of the quadrature operators, and the Fourier transformed probability distribution is the characteristic function in polar coordinates, we get the result

$$\tilde{W}(u,v) = \mathrm{tr}\left\{\hat{\rho}\exp(-iu\hat{x} - iv\hat{p}\right\}. \tag{1.42}$$

This means that the characteristic function is the quantum Fourier transform of the density operator. Since the characteristic function is defined as the Fourier transform of $W(x,p)$, the quasiprobability function $W(x,p)$ must be very closely related to the density operator $\hat{\rho}$. In fact, they are both one-to-one representations of the quantum state and so can be used interchangably to calculate properties of the quantum state.

There are many possible quasiprobability functions that are consistent with most of the above, but the only function for which the marginal distributions give the true statistics of the quadratures is the Wigner function. The Wigner function was first proposed by Eugene Wigner in 1969 [220], and can be written in terms of x and p as

$$W(x,p) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \exp(ipx)\left\langle x - \frac{q}{2}\right|\hat{\rho}\left|x + \frac{q}{2}\right\rangle dq. \tag{1.43}$$

This was "chosen from all possible expressions, because it seems to be the simplest" [220]. The Wigner function is a quasiprobability distribution that forms a classical-like phase space distribution for quantum mechanics. It is derived from Eq. (1.42) by application of the Baker-Campbell-Hausdorff formula

$$\exp(-iu\hat{x} - iv\hat{p}) = \exp\left(\frac{uv}{2}\right)\exp(-iu\hat{x})\exp(-iv\hat{p}). \tag{1.44}$$

The most important property of the Wigner function is the overlap formula, which when written for two Hermitian operators $\hat{\rho}$ and $\hat{O}$, takes the form

$$\mathrm{Tr}\left[\hat{\rho}\hat{O}\right] = 2\pi\int_{-\infty}^{\infty} W_{\rho}(x,p)W_{O}(x,p)dxdp. \tag{1.45}$$

This means that one can calculate the expectation value of any operator $\hat{O}$ in a quantum state $\hat{\rho}$ using only the Wigner function. Thus the Wigner function can be used to calculate expectation values of physical observables, which is the intended purpose for our quantum phase space distribution. An important property of the Wigner function is that it is not necessarily positive. This is one of the reasons why it can only be called a quasiprobability distribution. In fact this property of the Wigner function has a useful physical interpretation. Negativity of the Wigner function for a quantum state is often used as a signature of nonclassicality [144], although not all nonclassical states have a negative Wigner function.

1.2.2 Nonclassicality in Quantum Optics

As stated previously, there are many possible quasiprobability distributions that can be chosen to represent a quantum state. The Wigner function is the most commonly used, partially because it has a simple description, but also because it is a good compromise between a classical phase space distribution and a quantum mechanical representation. However, there are a number of other possibilities, some of which are particularly useful.

One of these representations is called the Q function, defined as

$$Q(x,p) \equiv \frac{1}{\pi}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} W(x',p')\exp\left(-(x-x')^2-(p-p')^2\right)dx'dp'. \tag{1.46}$$

From the overlap formula (1.45) it can be seen that the Q function defines the overlap between the Wigner function of the state $\hat{\rho}$ and that of a coherent state, i.e. it gives the probability distribution for finding the coherent states $|\alpha\rangle$ in the state $\hat{\rho}$, because

$$Q(x,p) = \frac{1}{2\pi}\mathrm{tr}\{\hat{\rho}|\alpha\rangle\langle\alpha|\} = \frac{1}{2\pi}\langle\alpha|\hat{\rho}|\alpha\rangle. \tag{1.47}$$

From this, it can be seen that the Q function must always be positive. This means that all the negativities that could be present in the Wigner function no longer exist in the Q function. For this reason the Q function is sometimes called the smoothed Wigner function. Since this smoothing eliminates all the negativities, they must be localised to small areas of the Wigner function. The Q function also has an application in calculating anti-normally ordered expectation values of the form $\mathrm{tr}\{\hat{\rho}\hat{a}\hat{a}^\dagger\}$.

Normally ordered expectation values play an important role in some areas of quantum optics [147] and a quasiprobability distribution for normal ordering is desirable. Similarly to the way that smoothing the Wigner function gives the quasiprobability for anti-normally ordered states, the Wigner function is obtained by smoothing the quasiprobability function for normal ordering, i.e.,

$$W(x,p) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} P(x_0,p_0)\frac{1}{\pi}\exp\left(-(x-x_0)^2-(p-p_0)^2\right)dx_0dp_0, \tag{1.48}$$

where $P(x_0,p_0)$ is the P function, the quasiprobability distribution for normal ordering.

The P function is also often known as the Glauber-Sudarshan due to its close relationship to coherent states [89, 199]. This was famously expressed in the optical equivalence theorem [129]

$$\hat{\rho} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} P(x,p)|\alpha\rangle\langle\alpha|dxdp. \tag{1.49}$$

This equation shows that the P function is the decomposition of the density operator into coherent states. This means that if the P function is positive everywhere, then the state can be written as a statistical mixture of coherent states. In Eq. (1.48) we saw that the Wigner function is the smoothed P function; this means that the P function is even more ill-behaved than the Wigner function, which itself can already be negative. Therefore the P function can have some very strange behaviour, including derivatives of the Dirac delta function. In fact, the behaviour of the P function has a very important role in quantum optics. States that have a completely positive P function are considered classical, and all others are thus nonclassical. This emphasises the consideration of coherent states as the classical states, since only those that can be expressed as a statistical mixture of coherent states are considered classical. Note that the P function, the Q function and the Wigner function are all one-to-one correspondences to the quantum state $\hat{\rho}$, and therefore knowledge of any one of these functions is enough to completely describe the quantum state.

It is important to note here that there are two different notions of nonclassicality used in this thesis and in the study of quantum optics. There is the definition stated above based on the behaviour of the P function. This relates to the nonclassicality of an individual quantum state, with squeezed states in particular being considered nonclassical. In addition, there is a definition that deals with the nonclassicality of correlations and is closely related to quantum discord, which is introduced in detail in Chapter 2. In this thesis, the term "nonclassical" is used to refer to both types of nonclassicality, and it should be inferred from context which definition is intended. Ferraro and Paris [73] provide a detailed discussion on the relationship between the two definitions.

1.3 Gaussian States

1.3.1 Definition of a Gaussian State

Up to this point, I have focussed on describing quantum states that consist of a single optical mode, for example squeezed states and coherent states. Since most interesting phenomena involve states of more than one mode, it is clearly necessary to be able to describe states with multiple modes, in principle up to an arbitrary number N, although two- and three-mode states are most important for this thesis. To aid discussion the vector of quadratures

$$\hat{\mathbf{x}} \equiv (\hat{x}_1, \hat{p}_1, ..., \hat{x}_N, \hat{p}_N)^T, \tag{1.50}$$

is introduced, where the quadratures are defined in terms of the bosonic field operators in Eq. (1.10). The construction of this vector allows the commutation relations between all the quadratures to be written in a concise way

$$[\hat{x}_i, \hat{x}_j] = i\Omega_{ij}, \tag{1.51}$$

where the matrix $\mathbf{\Omega}$ of the form

$$\mathbf{\Omega} \equiv \bigoplus_{\mathbf{k=1}}^{\mathbf{N}} \omega, \qquad \omega \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{1.52}$$

has been introduced, which is known as the symplectic form.

Some of the most important characteristics of a quantum state $\hat{\rho}$ are its statistical

moments. The first moment is the mean value of the quadratures

$$\bar{\mathbf{x}} \equiv \langle \hat{\mathbf{x}} \rangle = \mathrm{tr}(\hat{\mathbf{x}}\hat{\rho}), \tag{1.53}$$

and the second moment is the covariance matrix $\mathbf{V}$ defined as

$$V_{ij} \equiv \langle \Delta\hat{x}_i \Delta\hat{x}_j + \Delta\hat{x}_j \Delta\hat{x}_i \rangle \,, \tag{1.54}$$

where $\Delta\hat{x}_i = \hat{x}_i - \langle \hat{x}_i \rangle$. The diagonal elements of the covariance matrix are the variances of the individual quadratures, and the off-diagonal terms describe the correlations between different quadratures, both within a single mode and between different modes.

The first two statistical moments have a particular importance for the class of Gaussian states. Gaussian states are those that have a Gaussian Wigner function, i.e. one of the form

$$W(\mathbf{x}) = \frac{\exp[-1/2(\mathbf{x} - \bar{\mathbf{x}})^T \mathbf{V}^{-1} (\mathbf{x} - \bar{\mathbf{x}})]}{(2\pi)^N \sqrt{\det \mathbf{V}}}. \tag{1.55}$$

A Gaussian state is always fully described by its first two statistical moments, which is why the Wigner function depends only on these. This is in contrast to non-Gaussian states, where *all* the statistical moments must be known to fully characterise the state, which is not very useful considering there are infinitely many of them! This property clearly demonstrates the appeal of Gaussian states. States that are close to being Gaussian states are well approximated by their first two statistical moments. How close a state is to a Gaussian state can be determined by studying the higher order statistical moments. The appeal of Gaussian states is further enhanced by the fact that most quantum optical states in practical use are Gaussian, or at least close approximations. In fact it is difficult to create states that have significant non-Gaussianity and there is a strong area of research that aims to produce them. Photon number states and "Schrödinger cat" states are two popular examples of non-Gaussian states that have practical uses and are therefore of interest. For a rigorous review of quantum information theory with Gaussian states, see, for example, [216].

1.3.2 Symplectic Analysis

In most cases, the mean value of quadratures doesn't affect the properties of a quantum state, therefore for Gaussian states the most important quantity is the covariance matrix. One crucial example of the importance of the covariance matrix is in a version of Heisenburg's uncertainty principle [194]

$$\mathbf{V} + i\mathbf{\Omega} \geq 0, \tag{1.56}$$

which follows from the commutation relations in Eq. (1.51). As can be seen above, the symplectic form comes into the uncertainty relation along with the covariance matrix. In fact the symplectic group, of which the symplectic form is a part, provides the framework for investigating Gaussian states, and it gives its name to the branch of mathematics used to study them, symplectic analysis.

In any dynamic situation, quantum states undergo transformations that need to be described. Since the focus of this thesis is on Gaussian states, the class of Gaussian transformations, i.e. transformations that preserve the Gaussian nature of a quantum state, must be introduced. It turns out that all Gaussian channels are unitary operations gen-

erated from Hamiltonians $\hat{H}$ by $U = \exp(-i\hat{H}/2)$ where $\hat{H}$ are second order polynomials of the field operators. In terms of the quadrature operators, the unitary operations U can be fully described by the mapping

$$(\mathbf{S}, \mathbf{d}) : \hat{\mathbf{x}} \to \mathbf{S}\hat{\mathbf{x}} + \mathbf{d}, \tag{1.57}$$

where $\mathbf{d}$ is a vector of real numbers and $\mathbf{S}$ is a $2N \times 2N$ real matrix. Crucially, any operation must preserve the commutation relations, which happens in this case when the matrix $\mathbf{S}$ preserves the symplectic form, i.e.,

$$\mathbf{S}\boldsymbol{\Omega}\mathbf{S}^T = \boldsymbol{\Omega}. \tag{1.58}$$

Transformations of this form are called symplectic transformations and this further emphasises the importance of the symplectic form in the study of Gaussian states. Upon action of a Gaussian unitary operation, the statistical moments of a quantum state transform as

$$\bar{\mathbf{x}} \to \mathbf{S}\bar{\mathbf{x}} + \mathbf{d}, \qquad \mathbf{V} \to \mathbf{S}\mathbf{V}\mathbf{S}^T. \tag{1.59}$$

Since we are mostly interested in the covariance matrix, it can be seen that the matrix $\mathbf{S}$ is the most important characteristic of a Gaussian transformation.

Probably the most important result in symplectic analysis is Williamson's theorem [222]. It shows that any covariance matrix $\mathbf{V}$ can be put into a diagonal form using a symplectic matrix $\mathbf{S}$ such that

$$\mathbf{V} = \mathbf{S}\mathbf{V}^{\oplus}\mathbf{S}^T, \qquad \mathbf{V}^{\oplus} = \bigoplus_{k=1}^{N} \nu_k \mathbb{1}, \tag{1.60}$$

where the diagonal matrix $\mathbf{V}^{\oplus}$ is the Williamson form of $\mathbf{V}$ and $\mathbb{1}$ is the two-dimensional identity matrix. The N positive real numbers ν_k are the symplectic eigenvalues of $\mathbf{V}$ and can be calculated as the magnitude of the eigenvalues of the matrix $i\boldsymbol{\Omega}\mathbf{V}$. The symplectic eigenvalues are important as they can be used to calculate a number of fundamental properties of a system. For example, the uncertainty relation is equivalent to the statement $\nu_k \geq 1$, i.e. the symplectic eigenvalues of a physical quantum state must be greater than or equal to one. The symplectic eigenvalues can also be used to calculate the von-Neumann entropy of a Gaussian state [108], using the equation

$$S(\hat{\rho}) = \sum_{k=1}^{N} g(\nu_k), \qquad g(x) \equiv \left(\frac{x+1}{2}\right)\log\left(\frac{x+1}{2}\right) - \left(\frac{x-1}{2}\right)\log\left(\frac{x-1}{2}\right). \tag{1.61}$$

From this equation and remembering that the von-Neumann entropy is zero for a pure state, it can be seen that the symplectic eigenvalues of a pure state are all equal to one, whereas for a mixed state at least one of them is greater than one. The purity, P, of a Gaussian state can also be more easily calculated directly from the covariance matrix $\mathbf{V}$ by the equation $P = 1/\sqrt{\det \mathbf{V}}$, which means that $\det \mathbf{V} = 1$ for pure states and $\det \mathbf{V} > 1$ for mixed states.

Williamson's theorem has a useful application in calculating the purification of a mixed state [109], where the purifying modes contain all the information lost about the original modes. Given a Gaussian state with covariance matrix $\mathbf{V}$ that is diagonalised by $\mathbf{S}$ as in

(1.60), a purification of this state has the covariance matrix

$$\mathbf{V}_p = \begin{bmatrix} \mathbf{V} & \mathbf{SC} \\ \mathbf{C}^T\mathbf{S}^T & \mathbf{V}^{\oplus} \end{bmatrix}, \qquad \mathbf{C} \equiv \bigoplus_{k-1}^{N} \sqrt{\nu_k^2 - 1}\sigma_z, \tag{1.62}$$

where $\sigma_z = \mathrm{diag}(1, -1)$ is the Pauli-z matrix. For a general mixed state, there are many possible purifications of which this is only one of them. A purification that is of particular interest is the one of smallest dimension; unfortunately this method doesn't always give that purification, and it is often difficult to determine the purification with the fewest number of modes. Caruso *et al.* [35] developed a method to calculate the minimum number of modes required for a purification.

1.3.3 Common Symplectic Transformations

There are a number of symplectic transformations on Gaussian states that have particular importance. For a single-mode Gaussian state the most important transformations are displacement, rotation, and squeezing.

The displacement operation is described by the displacement operator defined in Eq. (1.19), which is the complex version of the Weyl operator. It has no effect on the covariance matrix of a Gaussian state and only changes the mean values of the quadratures by a displacement $\bar{\mathbf{x}} \to \bar{\mathbf{x}} + \mathbf{d}$, where $\alpha = (x_0 + ip_0)$ and $\mathbf{d} = (x_0, p_0)^T$. Application of an arbitrary displacement operation onto the vacuum results in the class of coherent states.

The squeezing operation is described by the squeezing operator defined in Eq. (1.28). It transforms the covariance matrix as $\mathbf{V} \to \mathbf{S}(r)\mathbf{V}\mathbf{S}(r)^T$, where

$$\mathbf{S}(r) \equiv \begin{pmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{pmatrix} \tag{1.63}$$

is the symplectic map describing the squeezing operation. Application of the squeezing operation to the vacuum results in a state with zero mean values of the quadratures and covariance matrix $\mathbf{V} = \mathbf{S}(2r)$, where the variance in one quadrature is reduced below the vacuum level and the variance is increased in the other. In other words, applying the squeezing operation to the vacuum creates the class of squeezed states.

Phase rotation of a Gaussian state results in the mixing of quadratures, and therefore introduces correlations between the quadratures of a single mode. It is described by the symplectic map

$$\mathbf{R}(\theta) \equiv \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}. \tag{1.64}$$

It has no effect on the mean value of the quadratures, and can accurately be thought of as a rotation of the Wigner function. Combining the rotation operation with the squeezing operation allows for squeezing in any direction.

Any general one-mode Gaussian state can be created by applying a combination of squeezing, displacement and rotation to a thermal state [216]. This demonstrates the importance of the three described operations. Thermal states have a covariance matrix $\mathbf{V} = (2\bar{n} + 1)\mathbf{I}$ with $\bar{n} \geq 0$, where $\bar{n} = 0$ corresponds to a vacuum or coherent state. A

general one-mode Gaussian state is therefore a state with mean $\mathbf{d}$ and covariance matrix

$$\mathbf{V} = (2\bar{n} + 1)\mathbf{R}(\theta)\mathbf{S}(2r)\mathbf{R}(\theta)^T, \tag{1.65}$$

where $\bar{n} = 0$ gives a general pure one-mode Gaussian state.

1.3.4 Two-mode Gaussian States

Now we want to study two-mode Gaussian states and study correlations between different light modes. A general two-mode Gaussian state is created by interactions between general one-mode Gaussian states. For this thesis, the most important transformation describing an interaction between two modes is the beamsplitter interaction. This transformation is described by the operator

$$B(\theta) = \exp[\theta(\hat{a}^\dagger \hat{b} - \hat{a}\hat{b}^\dagger)], \tag{1.66}$$

where $\hat{a}$ and $\hat{b}$ are the annihilation operators of the two modes and θ is related to the transmissivity of the beamsplitter by the relation $\tau = \cos^2\theta$. In terms of covariance matrices, the symplectic matrix describing the interaction is

$$\mathbf{B}(\tau) = \begin{pmatrix} \sqrt{\tau}\mathbf{I} & \sqrt{1-\tau}\mathbf{I} \\ -\sqrt{1-\tau}\mathbf{I} & \sqrt{\tau}\mathbf{I} \end{pmatrix}. \tag{1.67}$$

The beamsplitter operation hybridises the two input modes and each of the output modes can be thought of as a superposition of the two input modes, with the weighting of the superposition dependent on the transmissivity of the beamsplitter. The beamsplitter operation is a passive operation, as can be seen by the linearity of the beamsplitter operator in Eq. (1.66), which means that it preserves the photon number of the input beams. As well as describing the mixing of two modes, the beamsplitter is also useful to describe loss in a Gaussian channel, where the reflectivity $\rho = (1 - \tau)$ quantifies the loss and the reflected mode represents the lost part of the beam.

The partial trace is another operation on multi-mode Gaussian states that is of particular interest. Given a two mode state $\hat{\rho}_{AB}$ the partial trace over mode B has the action $tr_B(\hat{\rho}_{AB}) = \hat{\rho}_A$, where $\hat{\rho}_A$ is the state of mode A. The partial trace removes any information about mode B and just leaves the marginal state of mode A. The partial trace is often used to describe loss, as it models the elimination of part of a state. The definition of the partial trace can be trivially extended to include more modes and tracing over different modes. It is useful to note that applying the partial trace to a pure state, in general results in a mixed state, except for the case that the traced out mode is uncorrelated with the remaining mode or modes. The covariance matrix of a state after a partial trace is simply the covariance matrix of the state before the partial trace, but with the entries related to the traced-out mode deleted, which results in a covariance matrix with reduced dimension.

An important two-mode Gaussian state is the two-mode squeezed state, with applications in many quantum optics experiments [28]. It can be created by mixing two orthogonally squeezed states on a balanced ($\tau = 1/2$) beamsplitter. This results in a state with zero mean and a covariance matrix of the form

$$\mathbf{S}_2(r) = \begin{pmatrix} \cosh(2r)\mathbf{I} & \sinh(2r)\sigma_z \\ \sinh(2r)\sigma_z & \cosh(2r)\mathbf{I} \end{pmatrix}. \tag{1.68}$$

This state is also known as an Einstein-Podoslki-Rosen (EPR) state due to the nature of the correlations between the quadratures of the two modes. Note that this is the standard form of the EPR state, and the original squeezed modes could be at any angle, as long as they are orthogonal, resulting in a state with a different covariance matrix but the same entanglement properties. In the limit of $r \to \infty$ the result is an ideal EPR state with perfect correlations between the modes, i.e., $\hat{x}_A = \hat{x}_B$ and $\hat{p}_A = -\hat{p}_B$. Finally, it is interesting to note that taking the partial trace of an EPR state results in a thermal state for the remaining mode as can be seen from Eq. (1.68) and the definition of a thermal state. Due to this, it can be said that the EPR state is the purification of a thermal state.

1.3.5 Standard Form

Two-mode Gaussian states provide the simplest oppurtunity to study the global properties of a quantum state, and fortunately they can be simply characterised by analytical formulae. The covariance matrix of a two-mode Gaussian state ρ_{AB} can be written in block form

$$\mathbf{V} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}, \tag{1.69}$$

where $\mathbf{A}$ is the covariance matrix of the state ρ_A, $\mathbf{B}$ is the covariance matrix of the state ρ_B and $\mathbf{C}$ describes the correlations between the two modes. $\mathbf{A}$,$\mathbf{B}$ and $\mathbf{C}$ are all 2×2 real matrices. The symplectic eigenvalues $\{\nu_-, \nu_+\}$ of this matrix are given by

$$\nu_\pm = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4\det\mathbf{V}}}{2}}, \tag{1.70}$$

where $\Delta \equiv \det\mathbf{A} + \det\mathbf{B} + 2\det\mathbf{C}$, is the sum of the determinants of the 2×2 submatrices [185]. The terms $\det\mathbf{A}$, $\det\mathbf{B}$, $\det\mathbf{C}$ and $\det\mathbf{V}$ are called symplectic invariants of the state because they are unchanged after symplectic transformations. Importantly, this means that the symplectic eigenvalues of a state are invariant under the operation of symplectic transformations. Given a covariance matrix written in this form, the uncertainty principle is equivalent to the conditions [183, 171]

$$\mathbf{V} > 0, \qquad \det\mathbf{V} \geq 1, \qquad \Delta \leq 1 + \det\mathbf{V}. \tag{1.71}$$

In addition, it is always possible to convert the covariance matrix of any two-mode Gaussian state into the form

$$\mathbf{V} = \begin{pmatrix} a\mathbf{I} & \mathbf{C} \\ \mathbf{C} & b\mathbf{I} \end{pmatrix}, \qquad \mathbf{C} = \begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix}, \tag{1.72}$$

where $c_1 \geq |c_2|$ and a, b, c_1 and c_2 are all real numbers. This is known as the standard form [60, 193] and the covariance matrix of any two-mode Gaussian state can be put in this form using a series of local symplectic transformations. Note that the symplectic invariants of a state in standard form are the same as they are in any other form. An important class of states, since they simplify calculations, are those that satisfy the condition $c_1 = \pm c_2$, known as two-mode squeezed thermal states [83].

1.4 Quantum Measurement

1.4.1 Properties of Quantum Measurements

One of the most important properties of quantum mechanics is the difference between quantum and classical measurement. A classical measurement can be thought of as recording the state of a classical system before the measurement. It generally leaves the state of the system unperturbed and it is possible to measure the state of all observables simultaneously. In addition, if the exact state of the system is known, it is possible to deterministically predict the outcome of all measurements. Quantum measurements on the other hand follow none of these properties, except in the case where the system is in an eigenstate of the measurement operator.

One of the fundamental principles of quantum measurements is that they disturb the measured system. The measurement outcome tells us the state of the system after measurement, but doesn't tell us what the state was before measurement. Rather than recording the state of the system prior to the measurement, a quantum measurement projects the state onto a new state. In addition, an observable of a quantum state only has a definite value if the quantum state is in an eigenstate of the measurement operator corresponding to that observable. This means that performing a second measurement can change the state so that the new state is no longer in an eigenstate of the first measurement, which means that the result of the first measurement is no longer valid. In other words, it is impossible to simultaneously observe different observables, unless those observables commute with each other. Another consequence of this property is that even if the state of a system is known before a measurement, it is only possible to probabilistically predict the measurement outcome, unless the initial state was an eigenstate of the measurement. These properties play a crucial role in the security of many quantum cryptographic schemes. In particular, they limit the potential performance of an adversary, which can lead to the guaranteed security of quantum information protocols. The interested reader is referred to one of the many excellent comprehensive books on quantum measurement, for example [31].

Mathematically, a quantum measurement is described by a set of operators $\{E_i\}$ satisfying the completeness relation $\sum_i E_i^\dagger E_i = I$, where I is the identity operator. Each E_i corresponds to a possible measurement outcome i. For a measurement performed on an input state $\hat{\rho}$ that gives an outcome i, the state is projected into the new state

$$\hat{\rho}_i = \frac{E_i \hat{\rho} E_i^\dagger}{p_i}, \qquad p_i = \mathrm{tr}(\hat{\rho} E_i^\dagger E_i), \tag{1.73}$$

where p_i is the probability of measuring the outcome i. If we only care about the result of a measurement, and not the state after the measurment, we can introduce $\Pi_i \equiv E_i^\dagger E_i$ and describe the measurement as a positive operator-valued measure (POVM) [123] described by the new set of operators $\{\Pi_i\}$. For a continuous variable system where quantum measurements can have a continuous outcome, p_i becomes a probability distribution and sums are replaced by integrals. Here we are particularly interested in Gaussian measurements, which are defined as having a Gaussian probability distribution of outcomes. In fact, if a Gaussian measurement is made on N modes of an $N+M$ mode Gaussian state, the classical measurement outcomes follow a Gaussian distribution and the remaining M modes remain in a (generally different) Gaussian state.

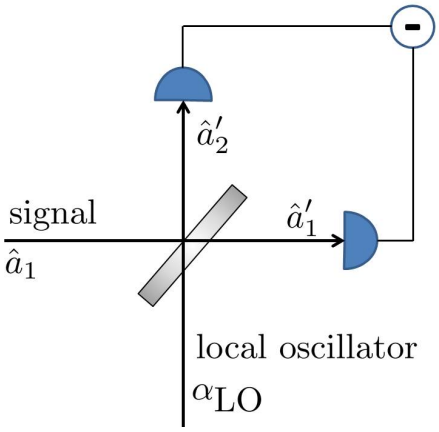


Figure 1.2: The signal is mixed with the local oscillator at a balanced beamsplitter. The photocurrent difference of the outgoing beams is proportional to the quadrature $\hat{x}_\theta$ with the phase set by the local oscillator.

1.4.2 Quantum Optical Measurements

The most important Gaussian measurement in quantum optics is balanced homodyne detection [228], which is effectively a measurement of the rotated quadrature $\hat{x}_\theta = \hat{x}\cos\theta - \hat{p}\sin\theta$, where $\theta = 0$ corresponds to the $\hat{x}$-quadrature and $\theta = 3\pi/2$ corresponds to the p-quadrature. Other values of θ allow any rotated quadrature to be measured. The measurement operators of homodyne detection are projectors onto the required quadrature basis, e.g. $|x\rangle\langle x|$, and the resulting outcome has a probability distribution given by the appropriate marginal distribution of the Wigner function, e.g. $P(x) = \int W(x,p)dp$. Practically, homodyne detection is realised following the procedure in Fig. 1.2 [1]. The signal state is interfered on a balanced beamsplitter with a coherent laser beam. The laser beam is known as the local oscillator and must be intense enough to give a precise phase reference, and be powerful enough to be treated classically by ignoring the quantum fluctuations. After the beamsplitter, the photocurrents I_1 and I_2 of the outputs are measured and then subtracted from each other to give the photocurrent difference I_{21}. It is assumed that the signal and local oscillator have a fixed phase reference, which is normally a safe assumption since they generally come from the same source, but must be ensured in an experiment. The bosonic operators of the output modes are given by

$$\hat{a}_1' = \frac{1}{\sqrt{2}}(\hat{a}_1 - \alpha_{LO}), \qquad \hat{a}_2' = \frac{1}{\sqrt{2}}(\hat{a}_1 + \alpha_{LO}), \tag{1.74}$$

where $\hat{a}_1$ is the amplitude of the signal and α_{LO} is the complex amplitude of the local oscillator. The photocurrent difference I_{21} is proportional to the photon number difference given by

$$\hat{n}_{21} = \hat{n}_2 - \hat{n}_1 = \alpha_{LO}^*\hat{a} + \alpha_{LO}\hat{a}^\dagger. \tag{1.75}$$

Using the definition of $\hat{x}_\theta = \hat{x}\cos\theta - \hat{p}\sin\theta$ from Eq. (1.39) we see that the measured photocurrent difference I_{21} is proportional to $\hat{x}_\theta$ since it can be shown from the above equation that

$$\hat{n}_{21} = \sqrt{2}|\alpha_{LO}|\hat{x}_\theta. \tag{1.76}$$

A homodyne detector thus measures the quadrature component $\hat{x}_\theta$, where the phase θ is provided by the local oscillator and can be adjusted by adding a phase shift to the local

oscillator. Note that the value of $|\alpha_{LO}|$ can be determined by keeping track of the photon sum current, which is important since $|\alpha_{LO}|$ is not generally known.

Homodyne measurements are particularly important when restricted to Gaussian quantum information theory since any Gaussian measurement can be achieved using only homodyne detection, linear optics and Gaussian ancilla modes [78]. One important extension of homodyne detection is heterodyne detection [229]. Heterodyne detection is implemented by first splitting the signal mode on a balanced beamsplitter where the other input is a vacuum mode, then performing homodyne detection on conjugate quadratures at the output [213]. Theoretically, it corresponds to a projection onto coherent states, so the measurement operators are $E(\alpha) \equiv \pi^{-1/2}|\alpha\rangle\langle\alpha|$. Homodyne and heterodyne detection are the most common measurements used in quantum optics with applications ranging from quantum key distribution to quantum state tomography.

1.4.3 Local Quantum Measurements

Often, part of a quantum system is measured to gain information that can be used while further processing the rest of the system. Therefore we need a way to describe the state of a subsystem after the rest of the system has been measured. For Gaussian states, this can be done using covariance matrices by considering a system consisting of two subsystems A and B, each consisting of an arbitrary number of modes. Here we restrict ourselves to the case where subsystem B has only one mode for simplicity, noting that this result can be generalised to more than one mode in the measured system.

Before measurement, the covariance matrix of the system can be written in block form as in Eq. (1.69), but with the matrix $\mathbf{A}$ no longer restricted to be that of a single mode. The state of subsystem A after Gaussian measurement of subsystem B then has a covariance matrix given by [65, 74]

$$\mathbf{A}' = \mathbf{A} - \mathbf{C}(\mathbf{B} + \sigma_0)^{-1}\mathbf{C}^T, \tag{1.77}$$

where σ_0 depends on the quantum measurement performed. For an arbitrary Gaussian measurement, σ_0 is the covariance matrix of an arbitrary one-mode pure Gaussian state, i.e. $\sigma_0 = R(\theta)\text{diag}\{\lambda, 1/\lambda\}R^T(\theta)$, where $\lambda \geq 0$ and $R(\theta)$ is given in Eq. (1.65). To extend this to the case of N modes in subsystem B, σ_0 should be the covariance matrix of an arbitrary N-mode pure Gaussian state. Note that the covariance matrix of subsystem A after the measurement depends only on the type of measurement performed and not on the measurement outcome obtained. In contrast, the displacement vector of the state depends on the outcome of the measurement. Note also, that if subsystems A and B are uncorrelated, measurement of mode B has no effect on subsystem A as should be expected.

For homodyne detection of the x-quadrature of mode B, the corresponding matrix describing the measurement is σ_0 with $\theta = 0$ and $\lambda \to 0$. For homodyne detection of the p-quadrature, $\theta = \pi/2$ and $\lambda \to 0$, or equivalently $\theta = 0$ and $\lambda \to \infty$. For heterodyne detection, $\theta = 0$ and $\lambda = 1$. In this way, the state of a subsystem after measurement on the remaining mode can be calculated for the most important Gaussian measurements.

1.5 Common Experimental Techniques

During my PhD, I have worked with experimental groups, describing the results of experiments with theoretical models. Therefore it has been important that I understand

commonly used experimental techniques and the sources of error that can be introduced. In this section, I give a brief summary of some of the most important techniques in modern experimental quantum optics. For a more complete overview, see, for example, [38].

1.5.1 Stokes Operators

Due to their technical convenience, experiments in quantum optics often use Stokes operators, a quantum version of the classical Stokes parameters [196], instead of position and momentum operators. Stokes operators describe continuous variable polarisation states, and are of particular interest since they can be measured by direct detection [132], polarisation is preserved in free space [103], and it is easy to map polarisation states to spin states and vice versa [97]. Stokes operators are described by

$$\begin{aligned} \hat{S}_0 &= \hat{a}_x^\dagger \hat{a}_x + \hat{a}_y^\dagger \hat{a}_y, & \hat{S}_1 &= \hat{a}_x^\dagger \hat{a}_x - \hat{a}_y^\dagger \hat{a}_y \\ \hat{S}_2 &= \hat{a}_x^\dagger \hat{a}_y + \hat{a}_y^\dagger \hat{a}_x, & \hat{S}_3 &= i(\hat{a}_y^\dagger \hat{a}_x + \hat{a}_x^\dagger \hat{a}_y), \end{aligned} \tag{1.78}$$

where $\hat{a}_x$ and $\hat{a}_y$ are the bosonic annihilation operators describing the x and y orthogonal polarisation modes. The operator $\hat{S}_0$ commmutes with the other three, and is proportional to the intensity of the described mode. The other Stokes operators obey the commutation relations

$$[\hat{S}_j, \hat{S}_k] = \epsilon_{jkl} 2i \hat{S}_l, \qquad j,k,l = 1,2,3. \tag{1.79}$$

Therefore it is impossible to measure simultaneously exact values of any two of these operators. From the commutation relations, the variances of the Stokes operators are bound by the uncertainty relations

$$V_i V_j \geq |\langle \hat{S}_k \rangle|^2, \qquad i \neq j \neq k, \tag{1.80}$$

where $V_j = \langle \hat{S}_j^2 \rangle - \langle \hat{S}_j \rangle^2$. Physically, from Eq. (1.78), it can be seen that $\hat{S}_1$ is the operator for linear polarisation, $\hat{S}_2$ is the operator for diagonal polarisation, and $\hat{S}_3$ is the operator for circular polarisation.

To draw a parallel with the previously introduced position and momentum operators, one can prepare the state with a strong excitation in one of the operators, for example $\hat{S}_3$, which is the case that will be considered from now on. This means that the state is circularly polarised, and the $\hat{S}_3$ operator is essentially classical with $|\langle \hat{S}_3 \rangle|^2 \gg 0$, whereas in contrast $\langle \hat{S}_1 \rangle = \langle \hat{S}_2 \rangle = 0$. From the relations in Eq. (1.80), it can be seen that the variance of $\hat{S}_3$ is unbounded, supporting the idea that it is classical, whereas the variance of $\hat{S}_1$ and $\hat{S}_2$ follow the relation $V_1 V_2 \geq |\langle \hat{S}_3 \rangle|^2$. It is often useful to renormalise the Stokes operators to simplify the uncertainty relation. For a strong excitation of $\hat{S}_3$, the Stokes operators are renormalised to [97]

$$\hat{S}_1' \equiv \frac{\hat{S}_1}{\sqrt{|S_3|}}, \qquad \hat{S}_2' \equiv \frac{\hat{S}_2}{\sqrt{|S_3|}}. \tag{1.81}$$

With the renormalised operators, the uncertainty relation is $V_1' V_2' \geq 1$. Since this relation has the same form as the Heisenburg uncertainty principle in Eq. (1.25), $\hat{S}_1$ and $\hat{S}_2$ can be thought of as being closely related to the position and momentum quadratures. In addition, the strong excitation of $\hat{S}_3$ allows the $\hat{S}_1$-$\hat{S}_2$ plane (often called the "dark plane" [132]) to be interpreted as the quadrature phase space.

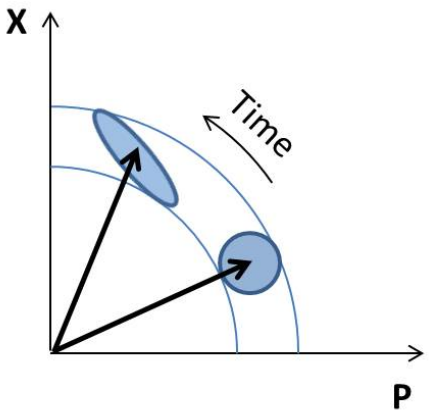


Figure 1.3: The initial coherent state (bottom right) travels through a medium with a Kerr nonlinearity. The higher amplitude parts of the coherent state experience a greater refractive index, and therefore those parts experience a greater phase shift. This causes the circle in phase space to be converted to an ellipse, with a variance in one direction that is lower than the coherent variance. Therefore a squeezed state has been created.

1.5.2 Polarisation Squeezing

For polarisation squeezing, the polarisation fluctuations must be reduced below some level, however unlike for quadrature squeezing there is no unique squeezing criterion [142]. By assuming a strong excitation in $\hat{S}_3$, $\hat{S}_1$ and $\hat{S}_2$ are analogous to the quadrature operators and so polarisation squeezing is easy to define. With this condition, the coherent polarisation state is the one where $V_1 = V_2 = |\langle \hat{S}_3 \rangle|$. More importantly, squeezed polarisation states can be defined as those that have a variance in one operator that is less than the coherent state variance. For a state squeezed in the $\hat{S}_1$ operator, this means $V_1 < |\langle \hat{S}_3 \rangle|$, and therefore conversely, $V_2 > |\langle \hat{S}_3 \rangle|$. This is important, because the easiest way to produce entanglement in continuous variable quantum information theory is by splitting a squeezed state on a beamsplitter.

Experimentally, polarisation squeezed states can be produced by exploiting the Kerr nonlinearity of optical fibres [100]. The Kerr nonlinearity is a $\chi^{(3)}$ nonlinearity, which means it is most easily observable in media that demonstrate inversion symmetry, where all the even orders of the electromagnetic susceptibility are zero. The optical Kerr effect occurs when a bright beam travels through an optical fibre with a Kerr nonlinearity. It is characterised by an intensity dependent refractive index [38]

$$n = n_0 + n_2 I, \qquad n_2 = \frac{3}{4} \frac{Re(\chi^{(3)})}{n_0^2 \epsilon_0^2 c}, \tag{1.82}$$

where $\chi^{(3)}$ is the third order electromagnetic susceptibility and I is the intensity of the electromagnetic field. The creation of squeezed light using the Kerr effect can be intuitively understood by considering the diagram in Fig. 1.3 [38]. Since different amplitudes of the coherent state exhibit a different refractive index, as the state travels through the medium, the different parts of the coherent state experience a different phase shift, causing the initially circular coherent state to become a squeezed elliptical state.

This method has been used to create polarisation squeezed states in many different experiments [188, 101], and, importantly, it is possible to produce states that are squeezed

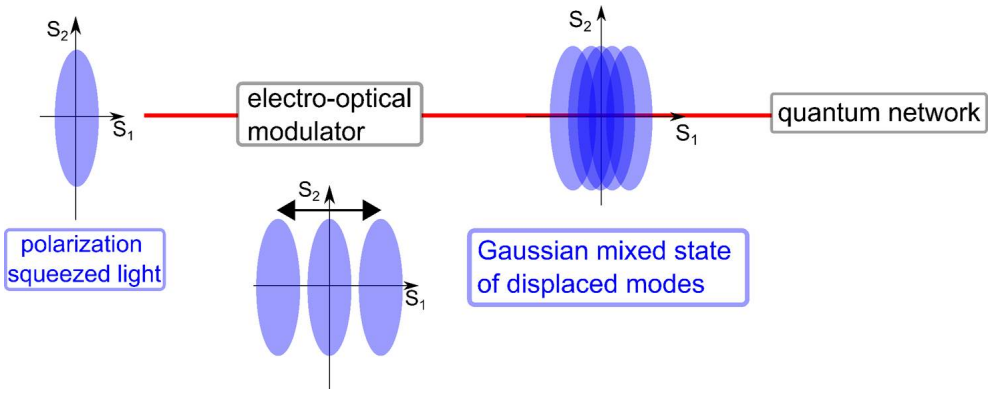


Figure 1.4: The initial state (here a squeezed state) is sent through an electro-optical modulator that displaces the squeezed state by some amount. These states are mixed together in post-processing to produce a Gaussian mixed state of the displaced modes. Credit: Vanessa Chille.

in different directions by application of a phase shift to one of the squeezed states. This allows this method to be used for experiments that involve creating entanglement by mixing two orthogonally squeezed states on a beamsplitter [191, 91].

1.5.3 Production of Correlated Mixed States

It is often of interest to study multimode correlated mixed states in quantum optics experiments. These states can be produced in a number of ways, but here I focus on a method that uses correlated modulation, as this is what was done in the experiments discussed later in this thesis [40, 50].

The method for producing a mixed state is shown in Fig. 1.4. The first step in correlated modulation is to perform a random displacement on a quantum state. Theoretically, this is done by applying a displacement operator to a quantum state, with a random value for the displacement. Experimentally, displacement is achieved by first passing the state through an electro-optical modulator. By applying a sinusoidal frequency to the electro-optical modulator, the size of the displacement can be varied. A phase matched electronic local oscillator, with the same frequency as that applied to the electro-optical modulator, is then used to down-mix the Stokes measurement signal, resulting in the desired displacement of the quantum state.

Next, the measurement results from different displaced states are digitally mixed together, leading to a mixed state with increased uncertainty in the displaced quadrature. As long as the different displacements that were mixed together follow a Gaussian distribution, the resultant mixed state is also Gaussian. This means the symplectic formalism for Gaussian states can be applied, as it can be for pure states.

Now, to get a correlated mixed state, the method above has to be followed for two different states, where the displacement applied to the two states is the same at each run of the experiment. Finally, by mixing together the results for the two states, ensuring that the displacements follow the same Gaussian distribution, the result will be a two-mode correlated Gaussian mixed state. This state can then be further processed to study complicated protocols involving more than two modes.

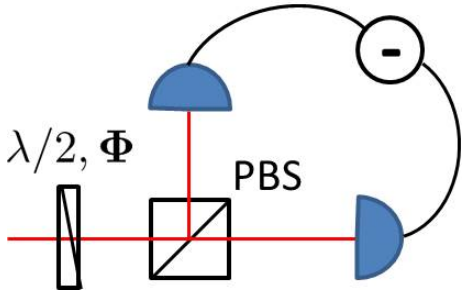


Figure 1.5: A Stokes measurement is performed by first passing the beam through a rotatable half-wave plate. The mode is then split on a polarising beamsplitter. The photocurrents are measured at each of the outputs of the beamsplitter. The photocurrent difference is proportional to the required Stokes operator. Varying the angle of the half-wave plate changes what Stokes operator is being measured. A phase shift of 0 gives measurement of the $\hat{S}_1$ operator, a phase shift of $\lambda/2$ gives measurement of the $\hat{S}_2$ operator and a phase shift of $3\lambda/4$ gives measurement of $\hat{S}_3$.

1.5.4 Stokes Measurements

One of the main benefits of Stokes operators is the ease with which they can be measured. Whereas for accurate homodyne detection, it is important to have a phase-matched local oscillator at all times, this is not necessary for Stokes operators. This is because the strong excitation of the $\hat{S}_3$ operator can be used as an inbuilt local oscillator instead [132]. This is automatically phase-matched with the quantum state since it travels along with it, and therefore removes the technical difficulty of ensuring the local oscillator is phase matched at all times. Therefore Stokes measurement is effectively a direct detection.

A depiction of a Stokes measurement procedure is found in Fig. 1.5. When the half-wave plate has a rotation angle of $\Phi = 0$, the polarising beamsplitter splits the polarisation mode corresponding to $\hat{a}_x$ into one output of the beamsplitter, and the polarisation mode corresponding to $\hat{a}_y$ to the other. The photocurrent at one output of the beamsplitter is thus proportional to $\hat{a}_x^\dagger \hat{a}_x$, and the photocurrent of the other output is proportional to $\hat{a}_y^\dagger \hat{a}_y$. The photocurrent difference I_- is thus proportional to $\hat{a}_x^\dagger \hat{a}_x - \hat{a}_y^\dagger \hat{a}_y$. Therefore from Eq. (1.78), we have $I_- \propto \hat{S}_1$. The proportionality is dependent only on the intensity of the initial state, and therefore can be found simply by calculating the sum photocurrent. The $\hat{S}_2$ operator is found by rotating the waveplate by an appropriate angle, and following the same procedure.

1.6 Summary of Chapter 1

In Chapter 1, I have introduced the basics of quantum optics, starting from the fundamental theoretical principles, moving through some of the most useful tools to analyse continuous variable states, and finally building up to some commonly used experimental methods. The material introduced here will form the basis for much of the work that follows.

The Wigner function provides an important tool to visualise quantum optical states and understand their properties. Symplectic analysis is the main work-horse for studying Gaussian states, and will be used extensively in Chapters 2 to 4. The properties of quantum measurements are some of the fundamental differences between classical and quantum physics, and their importance will repeatedly be evident. Understanding commonly used experimental techniques is vital whenever theoretical models are compared to experimental

results, particularly when it comes to describing errors that appear in experiments.

2

Quantum Correlations

2.1 Entanglement

Since the early days of the theory of quantum mechanics, it has been recognised that the Copenhagen interpretation leads to curious predictions about the nature of reality. This was most famously presented in 1935 when Einstein, Podolsky and Rosen presented their paper questioning the completeness of quantum mechanics [64]. They introduced a state of two subsystems with perfect correlations in both position and momentum, meaning that if one subsystem is measured, the state of the other subsystem is immediately known, no matter how far apart the subsystems are. Einstein called this "spooky action at a distance", which contradicted the idea of locality. He further argued that if the measuring party could choose between two different measurements, and since the two systems are unable to interact instantaneously, this would lead to the possibility "to assign two different wave functions to the same reality". Thus quantum mechanics leads to a contradiction, since it should not be possible for a system to have two different realities at once.

This paper was part of the motivation for Schrödinger's famous triplet of papers later that year [180] (translation [204]), where he first introduced the term "entanglement" [181]. He said that when two quantum systems interact, they can no longer be described by a representation of individual systems. Instead it is only possible to describe the whole state of the two systems. This he called "the characteristic trait of quantum mechanics", now known as entanglement. With this property, the contradiction in Einstein's earlier paper is addressed, since measurement on one system causes the wavefunction of the other to collapse into a single reality. This "spooky action at a distance" is a crucial part of quantum theory, introducing the idea of nonlocality, which contrasts with the relativistic assumption of the finite propagation time of all effects. However, this apparent contradiction is resolved by considering the transfer of information between two parties. Only when a conventional message is sent between the two parties can any information be transferred. Therefore information can at best be transferred at the speed of light, which means the no-signalling theorem is satisfied and quantum mechanics and special relativity can coexist peacefully.

Quantum entanglement remained a controversial issue until Bell's statistical tests for nonlocality [19], which are described in the next section, were used to experimentally confirm the presence of nonlocality in quantum mechanics [13, 14]. Recently there has been an increased interest in quantum entanglement through the field of quantum information theory [117, 116, 37]. Thanks to the description of entanglement in terms of entropic quantities, it is now possible to investigate the utility of entangled quantum states for information processing tasks. Entanglement is a vast resource, with a wide range of applications, including quantum cryptography [67, 52], quantum computation[127, 189, 66], quantum dense coding [139] and quantum teleportation [21, 75].

2.1.1 Nonlocality

John Bell led a reemergence of interest in quantum entanglement when he introduced Bell's inequalities [19]. These inequalities built on the Einstein-Podoslky-Rosen paper of 1935 by starting with the same assumptions of locality and reality, and deriving a restriction on the statistics of measurement results. In doing this, it follows that if there is a violation of the inequality, then at least one of the assumptions of locality or reality must be false.

Consider the case where Alice and Bob have a pair of quantum particles, created via some quantum experiment. They each have two measurement devices described by non-commuting bases (A_1 and A_2 for Alice, and B_1 and B_2 for Bob), and they can independently choose which one to use. They simultaneously observe the two particles by performing a measurement with one of their devices. Assuming that each measurement can have the outcome of +1 or -1, Bell's inequality states that for a state obeying locality and reality,

$$\langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle \leq 2. \tag{2.1}$$

This inequality is independent of the measurement apparatus used, and only depends on expectation values of the results. Inspired by Bell's work, there have been similar inequalities derived, most importantly the Clauser-Horne-Shimony-Holt (CHSH) inequalities [46]. Bounds like Bell's inequality have proven experimentally difficult to violate, and it was Aspect [13, 14] that provided the first strong evidence of violation of a Bell inequality. Recently [87, 106, 186], experiments have been performed that provide a loophole-free violation of Bell's inequalities, thus providing the strongest evidence yet that a local-realist view of the Universe can be ruled out. An additional achievement of Bell's inequalities was to rule out local hidden variable theories that describe experimental results by some underlying unknown variable. Even today there are still some popular hidden variable theories, however all must allow for some nonlocality [112], thus cementing the idea of nonlocality in quantum mechanics.

It has been shown that all pure entangled states must violate a Bell inequality [86], however there are some mixed states that are entangled, but do not violate a Bell inequality, for example the Werner state [218].

2.1.2 Separability Criteria

Although Schrödinger introduced entanglement in 1935, it took until 1989 for a formal definition of an entangled state to be produced [218]. More exactly, a separable state was defined, and any state that is not separable is considered to be entangled. A quantum

state $\hat{\rho}_{AB}$ is separable if it can be written as a convex mixture of product states, i.e.,

$$\hat{\rho}_{AB} = \sum_j p_j \hat{\rho}_{A,j} \otimes \hat{\rho}_{B,j}, \tag{2.2}$$

is a separable state, and any state that cannot be written in this way is entangled. This fits in with Schrödinger's description of an entangled state, since for an entangled state it is not possible to define a local description of the state; instead, it is only possible to give a global description. This definition also has a useful interpretation in terms of state preparation. Any separable state can be prepared by local operations and classical communication (LOCC) [206], whereas an entangled state must be produced by some quantum interaction between the two reduced states [218].

Using only Eq. (2.2), it can be seen that it is practically impossible to show that a state is entangled, since one would have to show that all possible arrangements of Eq. (2.2) are ruled out. Thankfully a number of useful tools have been developed to practically determine whether a system is entangled or not.

For this thesis, the most important of these tools is the Peres-Horodecki criterion [166, 116], also called the positive partial transpose criterion (PPT). It states that for a separable quantum state, $\hat{\rho}_{AB} = \sum_j p_j \hat{\rho}_{A,j} \otimes \hat{\rho}_{B,j}$, the partial transpose $\hat{\rho}_{AB}^{T_A} = \sum_j p_j \hat{\rho}_{A,j}^T \otimes \hat{\rho}_{B,j}$, is also a physical density matrix. Analogously, $\hat{\rho}_{AB}^{T_B}$ must be a physical density matrix. Taking the transpose of a quantum state is equivalent to performing a time reversal of that state. For an individual quantum object, time reversal leads to a valid quantum state, however for an entangled state, time reversal can lead to an unphysical state. Therefore the PPT criterion is a necessary condition for separability. For Gaussian states, it was shown that for states of $1 \times N$ modes, i.e. 1 mode in system A and N modes in system B, the PPT criterion is a necessary and sufficient criterion for separability [219].

Simon extended the PPT criterion to bipartite Gaussian states [193]. He showed that for Gaussian states, the partial transpose of a state described by the covariance matrix $\mathbf{V}$ is

$$\tilde{\mathbf{V}} = \lambda_N \mathbf{V} \lambda_N, \qquad \lambda_N = (\oplus_{i \neq j=1}^{n-1} \mathbb{1}^{(i)}) \oplus \sigma_z^{(j)}, \tag{2.3}$$

where $\tilde{\mathbf{V}}$ is the covariance matrix of the partially transposed state, $\sigma_z^{(j)} = \mathrm{diag}(1, -1)$, and the transpose is taken with respect to mode j. The physicality of the state is checked using a version of Heisenberg's uncertainty principle. The state is separable if

$$\tilde{\mathbf{V}} + i\mathbf{\Omega}_N > 0, \tag{2.4}$$

where $\mathbf{\Omega}$ is defined in Eq. (1.52). A further nice result of Simon's work is that any two-mode Gaussian state in the block form of Eq. (1.69) that satisfies $\det \mathbf{C} \geq 0$ is separable. This gives a convenient first check of the separability of a two-mode Gaussian state.

Duan *et al.* [60] developed an additional criterion for continuous variable states in terms of the quadrature operators. For a continuous variable state with two modes A and B the operators $\hat{u}$ and $\hat{v}$ can be constructed

$$\hat{u} = |a|\hat{x}_A + \frac{1}{a}\hat{x}_B, \qquad \hat{v} = |a|\hat{p}_A - \frac{1}{a}\hat{p}_B, \tag{2.5}$$

where a is some positive real number. Duan's criterion states that a separable state must

satisfy, for all a, the inequality

$$\langle(\Delta\hat{u})^2\rangle + \langle(\Delta\hat{v})^2\rangle \geq a^2 + \frac{1}{a^2}. \tag{2.6}$$

The advantage of this criterion is that measurement of correlations between quadratures is not required, whereas these measurements are required for criteria based on the covariance matrix. Experimentally, this means that fewer measurements are required to determine whether a state is entangled.

2.1.3 Entanglement Measures

We are now able to determine whether a given state is entangled, but it is often desirable to quantify the amount of entanglement present in a state. For pure Gaussian states, it is easy to quantify the entanglement shared between two parties. This is done using the entropy of entanglement, given by the von-Neumann entropy of the reduced states. For a pure state $|\phi\rangle$ with reduced states $\hat{\rho}_{A,B} = \mathrm{Tr}_{B,A}(|\phi\rangle\langle\phi|)$, the entropy of entanglement is [23]

$$E_V(|\phi\rangle) = S(\hat{\rho}_A) = S(\hat{\rho}_B). \tag{2.7}$$

The entropy of entanglement defines the number of pairs of entangled bits, i.e., singlet states, that can be extracted from an entangled state.

This quantification of entanglement leads to an interesting result about mixed states. All mixed states have non-zero entropy, and they can be purified by extending to a larger system. The entropy of entanglement therefore tells us that every mixed state is entangled to its purifying subsystem. If you have a pure entangled state that undergoes loss to the environment, the entanglement will decay and eventually disappear. But since the remaing state is mixed, it must be entangled to the subsystem that purifies it. The entanglement has not disappeared, it has simply spread out to a larger system. If all the losses could be recovered the entanglement could be restored. Practically, of course, this is impossible, but it does raise an interesting question about entanglement. Most of what we see is in a mixed state, so does that mean that almost everything is entangled to something, and if we could observe its purification by possessing everything that it has interacted with, we would see that entanglement is much more prevalent than it first appears? The study of mixed states could help us understand how to use this spread-out entanglement effectively.

In mixed states it is much more difficult to quantify the entanglement of a given state, largely because every mixed state has an infinite number of possible pure-state decompositions. This has led to numerous different methods to quantify entanglement in mixed states, each best suited to a different purpose. Some important properties that a good entanglement measure must satisfy are given below [206].

- $E(\hat{\rho}) = 0$ for a separable state, and $E(\hat{\rho}) > 0$ for an entangled state.
- $E(\hat{\rho})$ is invariant under local unitary transformations, i.e.,

$$E((\hat{U}_1 \otimes \hat{U}_2)\hat{\rho}(\hat{U}_1^\dagger \otimes \hat{U}_2^\dagger)) = E(\hat{\rho}). \tag{2.8}$$

- $E(\hat{\rho})$ must be nonincreasing under LOCC operations, i.e.,

$$E(\hat{O}_{LOCC}(\hat{\rho})) \leq E(\hat{\rho}). \tag{2.9}$$

Entanglement of Formation

Closely related to the pure state entropy of entanglement, one of the most commonly used entanglement measures is the entanglement of formation [23], defined as

$$E_F(\hat{\rho}) = \min_{\{p_k,\phi_k\}} \sum_k p_k E_V(|\phi_k\rangle), \tag{2.10}$$

where the minimisation is taken over all possible decompositions $\hat{\rho} = \sum_k p_k |\phi_k\rangle\langle\phi_k|$. The asymptotic regularisation of the entanglement of formation is the same as the entanglement cost, which defines the minimum number of singlets needed to prepare the states by LOCC [99]. Due to the potentially infinite number of possible decompositions, this optimisation is generally difficult to carry out. Exact results are known for the entanglement formation for two-qubit states [225], Werner states [211], and isotropic states in arbitrary dimension [203]. In continuous variables, the Gaussian entanglement of formation [224] is a useful quantity, where the Gaussian entanglement of formation $GE_F(\hat{\rho})$ is defined in the same way as the entanglement of formation, but with the minimisation carried out over Gaussian decompositions. Interestingly, for symmetric two-mode Gaussian states, the Gaussian entanglement of formation has been shown to be equivalent to the entanglement of formation [81], and it is an open question as to whether this is true for all Gaussian states. Adesso and Illuminati [6] provided a useful method to calculate the Gaussian entanglement of formation for bipartite Gaussian states.

Distillable Entanglement

Many quantum information protocols, for example teleportation, rely on entanglement shared between two quantum states held by Alice and Bob. However, often when maximally entangled states are distributed between two parties, the entanglement is degraded by losses to the environment. It is desirable for Alice and Bob to be able to improve this entanglement. In 1996, Bennett *et al.* [22, 23] provided a method to achieve this entanglement purification. If Alice and Bob share N copies of a bipartite mixed state $\hat{\rho}$ containing noisy entanglement, they can extract M ideal Bell pairs by performing LOCC operations. The optimal fraction M/N that can be achieved in the limit of large N defines the distillable entanglement $E_D(\hat{\rho})$, i.e.,

$$E_D(\hat{\rho}) = \max_{\{LOCC\}} \lim_{N\to\infty} \frac{M}{N}. \tag{2.11}$$

Over the years, many distillation procedures have been developed [118] in both the discrete variable [56] and continuous variable [159] settings. For Gaussian states, distillable entanglement can be defined, but since Gaussian entanglement cannot be distilled using Gaussian operations [65], it is almost impossible to calculate. However it has been shown that entanglement in bipartite Gaussian states can be distilled if and only if the state has a non-positive partial transpose [79]. States that possess entanglement that cannot be distilled are called bound entangled states [114]. There are numerous examples of such states [44], but it is not yet known whether there are states with a negative partial transpose that cannot be distilled.

Logarithmic Negativity

Another useful measure of entanglement in Gaussian states is the logarithmic negativity [209], which defines by how much a quantum state violates the PPT criterion. It is defined by

$$E_N(\hat{\rho}) = \sum_k \max\{-\log(\tilde{\nu}_k), 0\}, \tag{2.12}$$

where $\tilde{\nu}_k$ are the symplectic eigenvalues of $\hat{\rho}^{T_j}$. Since for all separable states $\tilde{\nu}_k \geq 1$, the logarithmic negativity is zero for separable states. It has also been shown to be nonincreasing under LOCC [173]. The obvious appeal of the logarithmic negativity is its ease of calculation. In addition, it provides an upper bound on the distillable entanglement described above [209].

2.1.4 Entanglement in Multimode States

For a bipartite continuous variable state, it is comparatively easy to say whether the state is entangled; either the two modes are entangled, or the state is separable. However when more modes are included the situation becomes more complicated. The obvious next step is to look at three-mode states made up of modes A, B and C. In a three-mode state there are numerous different bipartitions that can be entangled, and the entanglement can be between two individual modes, or delocalised between three modes. Thankfully, the PPT criterion is a necessary and sufficient test for entanglement across any of these partitions [219], which means that the separability properties of a three-mode state can be fully qualitatively characterised.

To do this, it must first be recognised that there are three different bipartitions that can be entangled. A state is called $A - BC$ biseparable if mode A is separable from modes BC taken together, with a similar definition holding for the other two bipartitions. Separability across the $A-BC$ bipartition can be tested by taking the partial transpose of mode A and checking if the new matrix satisfies the uncertainty relation. By considering all the possible ways in which a three-mode state can be biseparable, this leads to five possible classes that a three-mode state can fall in to [80]:

- Class 1: *Fully inseparable states* are those which are not biseparable under any of the three bipartitions.
- Class 2: *One-mode biseparable states* are separable under only one of the bipartitions.
- Class 3: *Two-mode biseparable states* are separable under exactly two of the three bipartitions.
- Class 4: *Three-mode biseparable states* are separable with respect to all three bipartitions, but they cannot be written as a mixture of tripartite product states.
- Class 5: *Fully separable states* can be written as a mixture of tripartite product states.

In addition, within some of the classes, there are different cases with respect to two mode entanglement. For example, consider a class 2 state where A is entangled with BC, B is entangled with AC but C is separable from AB. Mode A may or may not be entangled with mode B if mode C was traced out, and this set of classes makes no distinction between

these two types of state. Finally, note that the PPT criterion can be used to distinguish between all these classes, except for classes 4 and 5. A more complicated criterion is needed to distinguish between these two classes [80].

2.2 Quantum Discord

An important question in quantum mechanics has always been, where is the quantum-classical boundary? The question applies for correlations just as it does for physical states. For a long time it was thought that entanglement was equivalent to any quantum correlations, and separable states were just classically correlated. This is true for pure states, however for mixed states the situation is more complicated. Entanglement is fundamentally a consequence of the superposition principle, however superposition is not the only feature unique to quantum mechanics. One of the other fundamental properties in quantum mechanics is the fact that not all observables are simultaneously observable. Mathematically this is a consequence of the non-commutativity of certain observables, for example position and momentum. This means that, even in a separable state, measurement of one part of the state can disturb the rest, in contrast to what one would expect classically. Therefore the correlations may have a quantum nature, despite the state being separable.

The study of quantum correlations beyond entanglement became more prevalent after observations that the *deterministic quantum computation with one quantum bit* (DQC1) protocol [130], which allows the normalised trace of a unitary operator to be calculated more quickly than classically possible, appears to work without the presence of entanglement. It was quickly recognised that more general nonclassical correlations could assist with the speed-up in this protocol [134]. Later it was shown that quantum correlations beyond entanglement, measured by quantum discord, were present at the end of the protocol [55], thus suggesting that such quantum correlations could provide the figure of merit for this protocol. Since then, discord has been identified as playing a role in many information processing protocols (see Section 2.2.3), including the phenomenon of entanglement distribution by separable states [198] and the measurement of information encoded into quantum states [96].

There are numerous measures of nonclassical correlations beyond entanglement that have been developed in recent years [154]. These nonclassical correlations are mostly dependent on the properties of quantum measurement and often depend on some optimisation over all possible measurements. The most popular of these measures is the quantum discord [158, 105], discussed further in the following sections. Understanding these measures helps to define the boundary between quantum and classical correlations.

2.2.1 Definition of quantum discord

Quantum discord [158, 105] was originally defined in terms of entropic quantities, however states that possess discord can also be defined in a similar way to entangled states. A bipartite state $\hat{\rho}_{AB}$ with classical correlations can be written in the form [160]

$$\hat{\rho}_{AB} = \sum_{ab} p_{ab} |a\rangle\langle a| \otimes |b\rangle\langle b|, \tag{2.13}$$

where $\{|a\rangle\}$ and $\{|b\rangle\}$ form an orthonormal basis for systems A and B respectively. Any state that cannot be written in this form possesses quantum discord [53]. From this and Eq. (2.2) it can immediately be seen that any entangled state must also possess quantum discord, however the converse is clearly not true. The definition also suggests an interpretation of quantum correlations; a state possesses quantum correlations if measurement on one subsystem disturbs the state of the other [154].

Ollivier and Zurek [158] originally defined quantum discord in terms of different definitions of the mutual information. Classically [49], the mutual information is defined as

$$I(A,B) = H(p_A) + H(p_B) - H(p_{AB}), \tag{2.14}$$

where $H(p_i) = -\sum_j p_{i=j} \log(p_{i=j})$ is the Shannon entropy. The Shannon entropy is the uncertainty of a random event, which means that the mutual information represents how much less uncertain a joint event is than the two individual events. In other words it is a measure of the total correlations between the two events. Using Bayes' rule

$$p_{A|B=b} = \frac{p_{A,B=b}}{p_{B=b}}, \tag{2.15}$$

the classical mutual information can be rewritten as

$$J_c(A,B) = H(p_A) - \sum_b p_{B=b} H(p_{A|B=b}), \tag{2.16}$$

with a similar expression holding where A and B are swapped round. From this equation, the mutual information can be interpreted as the average reduction of the uncertainty of A after a measurement on B. Classically this is equivalent to the previous definition of mutual information, however it should be evident that this is not the case in the quantum realm due to the properties of quantum measurements.

Ollivier and Zurek [158] studied what happens when these expressions are converted to the quantum regime. The first expression for mutual information is generalised simply by converting the Shannon entropies to von-Neumann entropies S, such that the quantum mutual information is defined as

$$I(\hat{\rho}_{AB}) = S(\hat{\rho}_A) + S(\hat{\rho}_B) - S(\hat{\rho}_{AB}). \tag{2.17}$$

This measure of the quantum mutual information defines the total correlations present in a state, as measured by the minimum amount of local noise that has to be added to convert the state into a product state.

However converting J_c into the quantum regime is not so easy, due to the difficulties surrounding quantum measurements. Namely, the state of A after a measurement on B depends on the measurement performed. Bearing that in mind, the classical mutual information converted to the quantum regime can be expressed as [105]

$$\begin{aligned} J^{\leftarrow}(\hat{\rho}_{AB}) &= S(\hat{\rho}_A) - \inf_{\{\hat{\Pi}_i\}} \sum_i p_i S(\hat{\rho}^i_{A|B}), \\ J^{\rightarrow}(\hat{\rho}_{AB}) &= S(\hat{\rho}_B) - \inf_{\{\hat{\Pi}_i\}} \sum_i p_i S(\hat{\rho}^i_{B|A}). \end{aligned} \tag{2.18}$$

The infimum is taken because the measurement is chosen that minimises the uncertainty

in A (B) after a measurement on B (A). In other words, it is the measurement that maximises the information gained about A. Note that a left-facing arrow means that the measurement is performed on mode B, and a right-facing arrow means that the measurement is performed on mode A. These quantities are usually called the one-way classical correlations, and are generally different to one another. The infimum minimises the entropy over all POVM measurements [154], and in general it is difficult to find the optimal measurement, especially for continuous variable states. Note that for uncorrelated states, measurement on one subsystem gives no information about the other subsystem, so the classical correlations are zero. Also, note that that the quantum mutual information is never smaller than the one-way classical correlations.

In a classical system, the one-way classical correlations must be the same as the quantum mutual information. Therefore any difference between these quantities is evidence of the quantum nature of the correlations. This led to the definition of one-way quantum discord as the difference between the quantum mutual information and the one-way classical correlation [158],

$$\begin{aligned} D^{\leftarrow}(\hat{\rho}_{AB}) &= I(\hat{\rho}_{AB}) - J^{\leftarrow}(\hat{\rho}_{AB}) \\ &= S(\hat{\rho}_B) - S(\hat{\rho}_{AB}) + \inf_{\{\hat{\Pi}_i\}} \sum_i p_i S(\hat{\rho}^i_{A|B}); \end{aligned} \tag{2.19}$$

$$\begin{aligned} D^{\rightarrow}(\hat{\rho}_{AB}) &= I(\hat{\rho}_{AB}) - J^{\rightarrow}(\hat{\rho}_{AB}) \\ &= S(\hat{\rho}_A) - S(\hat{\rho}_{AB}) + \inf_{\{\hat{\Pi}_i\}} \sum_i p_i S(\hat{\rho}^i_{B|A}). \end{aligned} \tag{2.20}$$

Clearly, the above definitions for discord are asymmetric since they depend on which part of the state is measured. A symmetric version of quantum discord, sometimes called the two-way quantum discord, is defined as

$$D(\hat{\rho}_{AB}) = \max\{D^{\leftarrow}(\hat{\rho}_{AB}), D^{\rightarrow}(\hat{\rho}_{AB})\}. \tag{2.21}$$

This quantity is only equal to zero for states that can be written in the form of Eq. (2.13), i.e., the only states with zero discord are those that have only classical correlations. This definition gives an interpretation for quantum discord as those correlations that cannot be accessed by local measurements [158].

2.2.2 Properties of quantum discord

We have already seen that quantum discord is non-zero for all states that have nonclassical correlations. However, there are some states for which one of the versions of one-way quantum discord is zero. Namely, for a state $\hat{\rho}_{AB}$,

$$D^{\rightarrow}(\hat{\rho}_{AB}) = 0 \quad \text{if} \quad \hat{\rho}_{AB} = \sum_i p_i |i\rangle\langle i| \otimes \hat{\rho}_{B,i}, \tag{2.22}$$

$$D^{\leftarrow}(\hat{\rho}_{AB}) = 0 \quad \text{if} \quad \hat{\rho}_{AB} = \sum_j p_j \hat{\rho}_{A,j} \otimes |j\rangle\langle j|, \tag{2.23}$$

where $\{|i\rangle\}$ and $\{|j\rangle\}$ are orthonormal bases for modes A and B respectively. To see that this is the case, consider the state $\hat{\rho}_{AB} = \sum_i p_i |i\rangle\langle i| \otimes \hat{\rho}_{B,i}$. Now if a projective

measurement into its orthonormal basis is performed on mode A, the new state is

$$\begin{aligned}\hat{\rho}'_{AB} &= \sum_k (|k\rangle\langle k| \otimes \mathbf{I})\hat{\rho}_{AB}(|k\rangle\langle k| \otimes \mathbf{I}), \\ &= \sum_{i,k} p_i |k\rangle\langle k|i\rangle\langle i|k\rangle\langle k| \otimes \hat{\rho}_{B,i}, \\ &= \sum_k p_k |k\rangle\langle k| \otimes \hat{\rho}_{B,k}, \\ &= \hat{\rho}_{AB}.\end{aligned} \tag{2.24}$$

In other words, there is a measurement on mode A that leaves the state of mode B unchanged, therefore the one-way quantum discord is zero. States of this form are often called "classical-quantum states" [115]. Note that the two-way quantum discord is not generally zero, since a measurement on mode B will in general disturb the state of mode A.

Similar to entanglement, there are a number of properties that should be satisfied by a good measure of quantum correlations. Some of these properties are given below, all of which are satisfied by quantum discord [154].

- $D(\hat{\rho}_{AB}) = 0$ for all states of the form of Eq. (2.13) and $D(\hat{\rho}_{AB}) > 0$ for states not of that form.
- $D(\hat{\rho}_{AB})$ is invariant under local unitary transformations, i.e.,

$$D((\hat{U}_1 \otimes \hat{U}_2)\hat{\rho}_{AB}(\hat{U}_1^\dagger \otimes \hat{U}_2^\dagger)) = D(\hat{\rho}_{AB}). \tag{2.25}$$

However, in contrast to entanglement, there are local nonunitary operations that can lead to increase, or even emergence, of discord. This is discussed in detail in Chapter 3.

2.2.3 Interpretations of quantum discord

The definition of discord has a strong mathematical motivation, however it is also desirable to have a physical interpretation of quantum discord. In recent work, many such interpretations have been found that give discord, and other nonclassicality measures, a quantifiable interpretation. As mentioned previously, the DQC1 protocol was the first instance where discord was suggested as a possible figure of merit of a quantum protocol. This result has since been confirmed experimentally using photons [136] and nuclear magnetic resonance (NMR) [162, 15]. Since then, further protocols have been found where discord provides the figure of merit of a protocol.

Quantum metrology

One area where discord has been found to be particularly applicable is quantum metrology. For example, a measurement scheme inspired by the DQC1 protocol has been devised that uses highly mixed states to perform quantum metrology [32]. The discord present at the output of the scheme can be thought of as the quantum resource that enables the performance of the protocol. In addition, it has been shown that discord provides a resource for phase estimation of an unknown quantum state [84]. The importance of discord to quantum metrology was also extended to the case of optical interferometry using

Gaussian probe states [3]. In that work, discord is identified as the essential characteristic that probe states must possess to be sensitive to a variety of local dynamics.

Quantum illumination

Quantum illumination [140] is a related protocol to quantum metrology. In quantum illumination, one part of a maximally entangled state is sent through a noisy region for target detection. If there is an object present, the sent state is reflected and detected with the kept part of the entangled state using a joint measurement. Surprisingly, even though there is no entanglement left at the end of the scheme, an entangled source improves the performance of the protocol. Weedbrook *et al.* [217] showed that the quantum advantage of the protocol is quantified by quantum discord, demonstrating that discord is the resource underlying the performance of quantum illumination.

Discord consumption

Another interpretation of quantum discord related to quantum metrology is its importance to information decoding [96]. Consider a two-mode quantum state ρ_{AB} that then has a signal encoded into mode A, resulting in the state $\tilde{\rho}_{AB}$. If one is restricted to local measurements on the two modes, i.e., if the two modes cannot interfere, then the maximum amount of information about the signal that can be gained is I_c. Now if one can also interfere the two modes and therefore perform global measurements, then the maximum amount of information that can be gained is I_q. In [96], it was shown that

$$D^{\leftarrow}(\rho_{AB}) - I(\tilde{\rho}_{AB}) \leq I_q - I_c \leq D^{\leftarrow}(\rho_{AB}) - D^{\leftarrow}(\tilde{\rho}_{AB}). \tag{2.26}$$

This means that the advantage that a global measurement has over local measurements is upper bound by the discord consumed when the signal is encoded. Note that as the strength of the signal increases, the correlations in the state $\tilde{\rho}_{AB}$ tend towards 0. In the case of an infinitely strong signal, Eq. (2.26) reduces to $I_q - I_c = D^{\leftarrow}(\rho_{AB})$. The discord present in the initial state defines the maximum advantage that a global measurement can have over local measurements. In other words, quantum discord defines the correlations that can only be utilised using a coherent operation.

Quantum discord in quantum communication

It has been observed that many quantum communication protocols originate from a single "mother" protocol [2], thus providing a hierarchical structure of such protocols. The "mother" protocol achieves both quantum-communication assisted entanglement distillation and state transfer simultaneously. This and related protocols, such as state merging [115], require entanglement to be successful; however Madhok and Datta [145] showed that discord is important when such protocols operate in a noisy environment. They found that quantum discord quantifies the minimum loss in performance due to decoherence. This shows that the optimum state to use in these protocols is dependent on both entanglement and quantum discord.

Entanglement distribution and discord

Quantum discord also has an interpretation in terms of entanglement distribution using an ancilla mode [51, 167, 72]. Entanglement distribution is where Alice and Bob want to

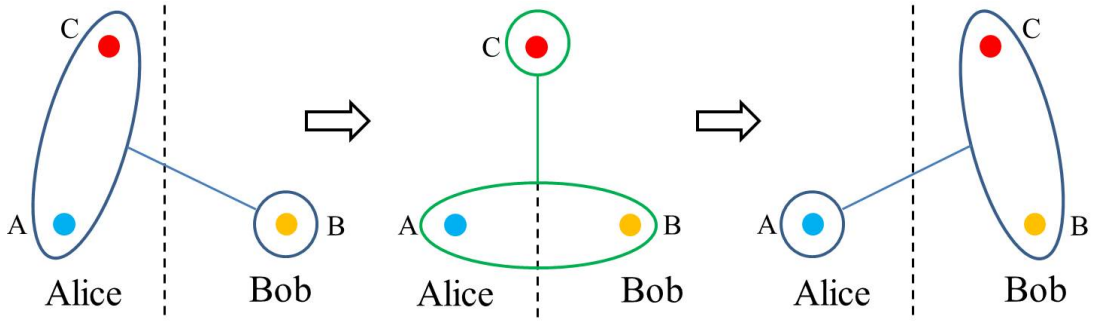


Figure 2.1: Alice initially holds modes A and C, and Bob holds mode B. Initially, there could be some entanglement shared between Alice's modes A and C and Bob's mode B. Alice then distributes mode C to Bob. For entanglement to be distributed, the discord between mode C and modes A and B must be non-zero. At the end of the procedure, Bob holds modes B and C and Alice holds mode A. If successful, the entanglement between Alice and Bob will have increased during the protocol.

establish or increase entanglement between them. This can only be done by transmitting a quantum state between them. Consider the case shown in Fig. 2.1 where Alice holds modes A and C, and Bob holds mode B. In an attempt to establish entanglement, Alice sends mode C to Bob. The amount of entanglement present between Alice and Bob after the distribution of mode C is bounded by the amount of discord between the sent mode and the other two, as shown in the equation [198, 41]

$$E_{A:CB}(\rho) \leq E_{B:AC}(\rho) + D_{AB|C}(\rho), \tag{2.27}$$

where the notation $D_{AB|C}(\rho)$ means that the measurement is performed on mode C. In this equation, entanglement (discord) is quantified by the relative entropy of entanglement (discord). In the case where Alice and Bob initially share no entanglement, the entanglement at the end is upper bounded only by the discord that is distributed. This highlights the important relationship between discord and entanglement in mixed states. Note that for pure states, Eq. (2.27) reduces to the Araki-Lieb inequality [11]

$$|S(\hat{\rho}_A) - S(\hat{\rho}_B)| \leq S(\hat{\rho}_{AB}). \tag{2.28}$$

2.2.4 Gaussian quantum discord

Due to the optimisation procedure required, quantum discord is generally difficult to calculate explicitly for most states. This problem becomes even greater in the continuous variable regime, since it is necessary to calculate the overlap of the relevant state with all possible one-mode Wigner functions. For this reason, the study of quantum discord in continuous variable states has been focussed on Gaussian states.

Since discord is invariant under local unitary transformations [154], it is sufficient to calculate the discord of a state in the standard form of Eq. (1.72). A Gaussian version of discord is defined by carrying out the optimisation over generalised Gaussian POVM measurements on the relevant subsystem. In fact, it is even sufficient to restrict the measurement to pure Gaussian states [184]. This simplifies the calculation vastly, and an analytical solution for Gaussian quantum discord has been found for squeezed thermal states [83] and for all two-mode Gaussian states [5].

Using the entropic equation for discord in Eq. (2.19), and the formula for entropy in Eq. (1.61), the Gaussian discord of a state in the standard form can be written as [5]

$$D_G^{\leftarrow}(\hat{\rho}_{AB}) = g(b) - g(\nu_+) - g(\nu_+) + g(\sqrt{\inf_{\sigma_0} \det \epsilon}), \tag{2.29}$$

where σ_0 is the covariance matrix of the Gaussian measurement on B, and ϵ is the state of A after the measurement on B:

$$\epsilon = a\mathbb{1} - \begin{pmatrix} c_+ & 0 \\ 0 & c_- \end{pmatrix} (b\mathbb{1} + \sigma_0)^{-1} \begin{pmatrix} c_+ & 0 \\ 0 & c_- \end{pmatrix}. \tag{2.30}$$

For a one-mode Gaussian measurement, σ_0 corresponds to an arbitrary pure one-mode Gaussian state, i.e., a rotated squeezed state: $\sigma_0 = R(\theta)\text{diag}\{\lambda, 1/\lambda\}R^T(\theta)$, where $\lambda \geq 0$ and $R(\theta)$ is the rotation matrix defined in Eq. 1.64. The optimal value of $\det \epsilon$ is found by optimising over all Gaussian measurements to be [5]

$$\inf_{\sigma_0} = \begin{cases} \dfrac{2c_+c_-^2 + (b^2-1)(\det\gamma - a^2) + 2|c_+c_-|\sqrt{c_+^2c_-^2 + (b^2-1)(\det\gamma - a^2)}}{(b^2-1)^2} \\ \\ \text{if} (\det\gamma - a^2b^2)^2 \leq (b^2+1)c_+^2c_-^2(\det\gamma + a^2); \\ \dfrac{a^2b^2 - c_+^2c_-^2 + \det\gamma - \sqrt{c_+^4c_-^4 + (\det\gamma - a^2b^2)^2 - 2c_+^2c_-^2(a^2b^2 + \det\gamma)}}{2b^2} \\ \\ \text{otherwise.} \end{cases} \tag{2.31}$$

States that are members of the second category have homodyning as their optimal measurement, but for states in the first category a more general measurement is required involving projections onto squeezed states. A similar expression for the right discord can easily be defined by swapping a and b in the above equation.

With this expression it is therefore possible to analytically calculate the Gaussian quantum discord of any two-mode Gaussian state. Since the Gaussian discord restricts the optimisation to Gaussian POVMs, it follows that

$$D^{\leftarrow}(\hat{\rho}_{AB}) \leq D_G^{\leftarrow}(\hat{\rho}_{AB}). \tag{2.32}$$

There are some states for which it has been proven that Gaussian discord is equivalent to the true discord [172], and it is conjectured that Gaussian discord is indeed the true discord for two-mode Gaussian states, with this suggestion supported by numerical evidence [82, 157].

It is interesting to note that there are very few Gaussian states for which the Gaussian discord vanishes. Only states with covariances matrices of the form $\gamma = \gamma_A \oplus \gamma_B$ have zero Gaussian discord [5]. This means that any correlated Gaussian state has nonclassical correlations, in contrast to the qubit scenario where it is easy to write a purely classically correlated state. This is a consequence of the fact that all Gaussian states are non-orthogonal to each other due to the infinite extent of their Wigner functions.

2.2.5 Koashi-Winter relation

As the study of nonclassical correlations beyond entanglement developed, it became clear that the relationship between nonclassicality and entanglement is an important area of study. For pure states, the idea of nonclassicality and entanglement are equivalent, with quantum discord being equal to entanglement of formation. In mixed states, they are not the same, however it is possible to find relationships between them, as has been shown in the case of entanglement distribution.

An important result in the study of entanglement is that states can only become entangled up to a certain degree. In addition, if two systems A and B are maximally entangled, then neither A or B can be entangled at all to any other party [47]. This property was named monogamy of entanglement and is an important difference between classical and quantum correlations. In fact, Koashi and Winter [131] showed that if two states are maximally entangled, they cannot even be classically correlated to another state! Consider a three-mode state $\hat{\rho}_{ABC}$; the degree by which the modes can become correlated is limited by the Koashi-Winter relation [131]

$$S(\hat{\rho}_A) \geq E_F(\hat{\rho}_{AB}) + J^{\leftarrow}(\hat{\rho}_{AC}), \tag{2.33}$$

where the equality holds if $\hat{\rho}_{ABC}$ is a pure state. Similar expressions also hold by swapping B and C and by taking all permutations of the three modes. This gives a set of six equations that demonstrate how the correlations between the three modes can be shared. As Koashi and Winter discussed, these equations show that the entropy of a state is a measure of its ability to form correlations.

The Koashi-Winter relations demonstrate an important link between classical correlations and entanglement, and due to the close relation between discord and classical correlations, they also show how to link discord to entanglement. By application of the various Koashi-Winter relations it is possible to derive a number of useful relations. Fanchini *et al.* [71] used them to demonstrate their "quantum conservation law" for a tripartite pure state

$$E_F(\hat{\rho}_{AB}) + E_F(\hat{\rho}_{AC}) = D^{\leftarrow}(\hat{\rho}_{AB}) + D^{\leftarrow}(\hat{\rho}_{AC}). \tag{2.34}$$

This shows that the sum of the entanglement of formation between particular subsystems is the same as the sum of the discord between the same subsystems. A chain rule can also be derived that relates entanglement to the discord of the three systems [70]

$$E_F(\hat{\rho}_{AB}) = D^{\leftarrow}(\hat{\rho}_{AB}) + D^{\leftarrow}(\hat{\rho}_{BC}) - D^{\rightarrow}(\hat{\rho}_{BC}). \tag{2.35}$$

A Gaussian version of the Koashi-Winter relations can also be written, simply by replacing the classical correlations and entanglement of formation by their Gaussian versions. Since this provides a relationship between Gaussian entanglement of formation and Gaussian discord, results that are known for one can be applied to the other. For example, it is known that for symmetric two-mode Gaussian states, the Gaussian entanglement of formation is equal to the true entanglement of formation [81]. Therefore, for any two-mode Gaussian state that has a three-mode purification with AC or BC symmetric, the Gaussian discord must be the true discord [5].

2.3 Summary of Chapter 2

In this chapter, I have discussed the notion of quantum correlations, starting by describing quantum entanglement, before introducing quantum correlations beyond entanglement with a focus on quantum discord. Quantum entanglement is known to have numerous applications in quantum information protocols, and recently, quantum discord has been shown to be important in many protocols involving mixed states. The relationship between entanglement and discord, particularly in mixed states, is of interest as the search for implementable quantum protocols continues. The Koashi-Winter relation provides a useful way to relate entanglement to discord and suggests the two are closely connected.

In the next two chapters I aim to advance understanding of discord and entanglement by studying their behaviour in multipartite mixed-state systems. In this way, I hope to shine a light on some interesting features of quantum correlations in mixed states. This is important because all realistic protocols run in noisy environments resulting in mixed states. By understanding all possible forms of correlation present, we can maximise our ability to utilise them effectively.

3

Discord Increase Under Local Loss

Entangled states have no local description and therefore an interaction between states is required to create entanglement. It is impossible to create entanglement using local operations and classical communications [118]. It therefore follows that it is also impossible to increase entanglement using local operations. This is the reason that entanglement distribution requires transmission of a quantum state between different parties. Entanglement is invariant under local unitary operations [118], however nonunitary local operations can reduce entanglement by degrading the correlations, for example by dissipation.

Whereas entanglement can be seen as a consequence of the superposition principle, discord [158, 105] is related to the non-commutativity of observables and, in mixed states, can be created by local operations and classical communication. For example, discord can be created by correlated modulation of two quantum states as described in Section 1.5.3. Similarly to entanglement, quantum discord is invariant under local unitary operations [154], but it can change under local nonunitary operations. However, unlike entanglement, discord can increase under local operations [197, 34]. This can only occur under local operations on the measured part of the state; discord can never increase if the operation is on the unmeasured system. In addition, discord can even be created from a classically correlated state by local operations or even loss [42, 120]. This is surprising, as loss is normally considered to decrease the quality of a quantum state, but if loss can increase discord, perhaps loss can sometimes be made useful.

3.1 Discord increase with discrete variables

Streltsov *et al.* [197] described the conditions by which discord in a discrete variable system can increase under the action of a noisy channel, where a noisy channel is one that can be described by a completely positive trace preserving map. Consider the classically correlated state of two qubits

$$\rho_{cc} = \frac{1}{2}|0^A\rangle\langle 0^A| \otimes |0^B\rangle\langle 0^B| + \frac{1}{2}|1^A\rangle\langle 1^A| \otimes |1^B\rangle\langle 1^B|. \tag{3.1}$$

From this state, a quantum correlated state can be created by applying a local noisy channel to mode A. A local measurement on mode A, followed by a replacement, leads to the state

$$\rho = \frac{1}{2}|0^A\rangle\langle 0^A| \otimes |0^B\rangle\langle 0^B| + \frac{1}{2}|+^A\rangle\langle +^A| \otimes |1^B\rangle\langle 1^B|, \tag{3.2}$$

where $|+^A\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. After this operation, the states that make up mode A form a non-orthogonal basis, which means there is now discord present in the state if the measurement is performed on mode A. The quantum channel needed to implement this change is the completely positive trace-preserving map

$$\rho = \Lambda_A(\rho_{cc}) = E_1\rho E_1^\dagger + E_2\rho E_2^\dagger \tag{3.3}$$

with local Kraus operators $E_1 = |0^A\rangle\langle 0^A|$ and $E_2 = |+^A\rangle\langle 1^A|$. The state in Eq. (3.2) is called quantum-classical because it has zero right discord, while the left discord is nonzero. This operation shows the ease with which discord can be created using local operations on a discrete variable state.

Streltsov *et al.* [197] went further by showing which channels could possibly cause an increase in discord. For qubits, they showed that a channel can cause discord increase only if it is neither semi-classical nor unital. A unital channel is one that maps the maximally mixed state $\frac{1}{2}\mathbb{1}$ onto itself, i.e., $\Lambda(\frac{1}{2}\mathbb{1}) = \frac{1}{2}\mathbb{1}$. A semi-classical channel is one that maps all input states into a state that is diagonal in the same basis

$$\Lambda_{sc}(\rho) = \sum_k p(k)|k\rangle\langle k|. \tag{3.4}$$

This is not to say that a channel that is neither semi-classical nor unital will always cause an increase in discord. It just means that there is at least one state that will undergo an increase in discord when passed through this channel. It can be easily seen that the channel in Eq. (3.3) is non-unital by applying it to the maximally mixed state $\rho = \frac{1}{2}\mathbb{1}$. For larger finite-dimensional systems it has been shown that the only operations that can never create discord are local commutativity-preserving operations [119].

An example of a situation where dissipative loss results in the emergence of discord was shown by Ciccarello and Giovannetti [42]. Consider the state

$$\rho_0 = \frac{1}{2}|0^A\rangle\langle 0^A| \otimes |+^B\rangle\langle +^B| + \frac{1}{2}|1^A\rangle\langle 1^A| \otimes |-^B\rangle\langle -^B|, \tag{3.5}$$

where $|\pm^A\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Clearly this is a classically correlated state since it is diagonal in two local orthonormal bases. Now mode B is subject to a dissipative Markovian bath, while mode A remains untouched. This channel is described by the quantum map

$$\Lambda(\rho_0) = E_0\rho E_0^\dagger + E_1\rho E_1^\dagger, \tag{3.6}$$

where $E_0 = |0^B\rangle\langle 0^B| + \sqrt{1-p}|1^B\rangle\langle 1^B|$ and $E_1 = \sqrt{p}|0^B\rangle\langle 1^B|$. If $|1\rangle$ is the state with one photon and $|0\rangle$ is the state with zero photons, then this can be thought of as a lossy channel with probability p that the photon will be lost. Application of this channel to ρ_0 results in a state with non-zero discord. This can be seen because the channel acts differently on the two parts of mode B in ρ_0. This results in a state that is no longer diagonal in a local orthonormal basis, and therefore it possesses discord.

In summary, we have seen that for qubits, not only can discord be increased by local operations, it can even be created. Loss, normally considered to be a negative, can result in the establishment of quantum correlations. This is in marked contrast to the situation with entanglement and demonstrates one reason why quantum correlations beyond entanglement are of interest.

3.2 Discord increase with continuous variables

For Gaussian states, the relevant quantity to study quantum correlations is Gaussian quantum discord [5, 83]. Similarly to the discrete case, Gaussian quantum discord is unaffected by local unitary operations, but can change under the action of local non-unitary channels. In addition Gaussian quantum discord can increase under local loss [43, 146], as was seen for discrete variables. Note that the only states with zero Gaussian discord are product states [5, 152]. This means that a local loss channel cannot create Gaussian discord; it can only increase what is already there. Gaussian quantum discord is equal to quantum discord for states studied here [172], which justifies its use.

In the remainder of this chapter, I study situations where quantum discord increases under local loss. Quantum correlations beyond entanglement are a promising resource for quantum information protocols. Therefore it is important to understand their fundamental properties, for example discord increase, so they can be effectively used. I investigate under what conditions discord increase is most pronounced, and what physical reason there is for this increase.

3.2.1 Discord increase scheme

The easiest way to create Gaussian discord is by splitting a thermal state on a beamsplitter, as was studied in detail in [29]. The behaviour of discord under local loss is then studied by implementing a variable loss channel on the output mode B and calculating the discord at the output. The basic situation is presented in Fig. 3.1. An experiment based on this scheme was carried out in [40], with a similar experiment performed in [146]. The input state can be varied by changing the noise added to each quadrature in order to investigate the behaviour of discord after loss. The transmission of the first beamsplitter can also be varied, resulting in an asymmetric state $\hat{\rho}_{AB}$ after the first beamsplitter. By studying how discord is affected by loss in all these cases, we can gain a better understanding of why discord increases under local loss.

The state before the beamsplitter is a one-mode Gaussian state described by the covariance matrix

$$\gamma_1 = \begin{pmatrix} V_x & 0 \\ 0 & V_p \end{pmatrix}, \tag{3.7}$$

where $V_{x,p} \geq 1$ are the uncertainties in the x- and p-quadratures after the noise is added. Splitting this state on a beamsplitter with transmission T results in the state

$$\gamma_{AB} = \begin{pmatrix} T^2\gamma_1 + R^2\mathbb{1} & RT(\mathbb{1} - \gamma_1) \\ RT(\mathbb{1} - \gamma_1) & R^2\gamma_1 + T^2\mathbb{1} \end{pmatrix}, \tag{3.8}$$

where $T^2 + R^2 = 1$. Mode B is then sent through an attenuating beamsplitter with

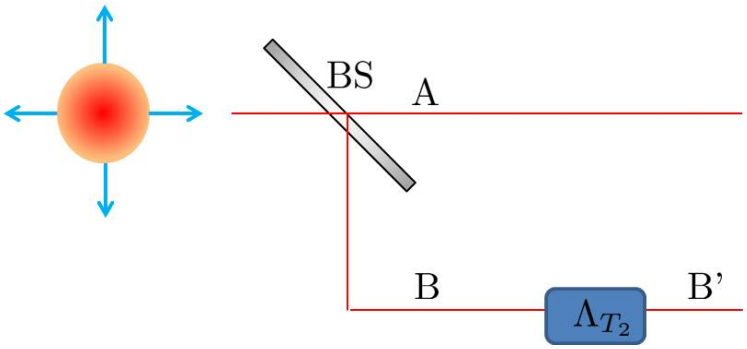


Figure 3.1: A thermal state is prepared by symmetrically modulating a coherent state in the $x-$ and $p-$directions. Alternatively, modulation can be performed asymmetrically to produce a squeezed thermal state. The state is then split on a beamsplitter (BS) with transmission T to produce the discordant state ρ_{AB}. Mode B undergoes local loss resulting in the state $\hat{\rho}_{AB'}$, which generally has a different amount of Gaussian discord than the initial state.

variable transmission T_2 to give the final state $\rho_{AB'}$ with covariance matrix

$$\gamma_{AB'} = \begin{pmatrix} T^2\gamma_1 + R^2\mathbb{1} & T_2RT(\mathbb{1} - \gamma_1) \\ T_2RT(\mathbb{1} - \gamma_1) & T_2^2(R^2\gamma_1 + T^2\mathbb{1}) + R_2^2 \end{pmatrix}, \tag{3.9}$$

where $T_2^2 + R_2^2 = 1$. Now the Gaussian quantum discord can be calculated using the method in [5] and plotted as a function of T_2 for various T, V_x and V_p to study how this influences the discord increase.

What affects discord increase?

Here I first study how the parameters in the state of (3.9) affect the phenomenon of discord increase, before explaining the behaviour in the next subsection. First I look at the case of an input thermal state with $V_x = V_p = V$ split on a balanced beamsplitter $T^2 = \frac{1}{2}$. Fig. 3.2 (a) shows the discord plotted against attenuation for various numbers of thermal photons in the input thermal state, where attenuation is defined as $Att = 1 - T_2^2$. The first thing to notice is that as V increases the total amount of discord increases. For low V, there is no discord increase, but once V exceeds about 5.8 shot noise units, discord increase does occur. One shot noise unit is the experiementally measured minimum uncertainty of a vacuum state. As V increases, the increase in discord becomes more pronounced, and the maximum value of discord occurs at a higher value of attenuation, as can be seen more clearly in Fig. 3.2 (b), where the curves have been normalised to start from the same point. This shows that it is necessary to have enough thermal noise in the initial state in order to observe an increase in discord, and increasing thermal noise accentuates the discord increase effect.

The next case I study is that of input states with constant $V_x = 32$ but varying V_p, split on a balanced beamsplitter. These states are often called squeezed thermal states because they can be created by applying a squeezing operation to a thermal state. Fig. 3.2 (c) shows the discord plotted against attenuation for states with varying V_p. The first thing to note is that the overall value of discord decreases as V_p decreases. The more interesting result is seen more clearly in Fig. 3.2 (d), normalised so that the curves start from the same value of discord. As V_p decreases, initially the discord increase dies away until it is no longer observable, however when V_p decreases further, the discord increase is recovered

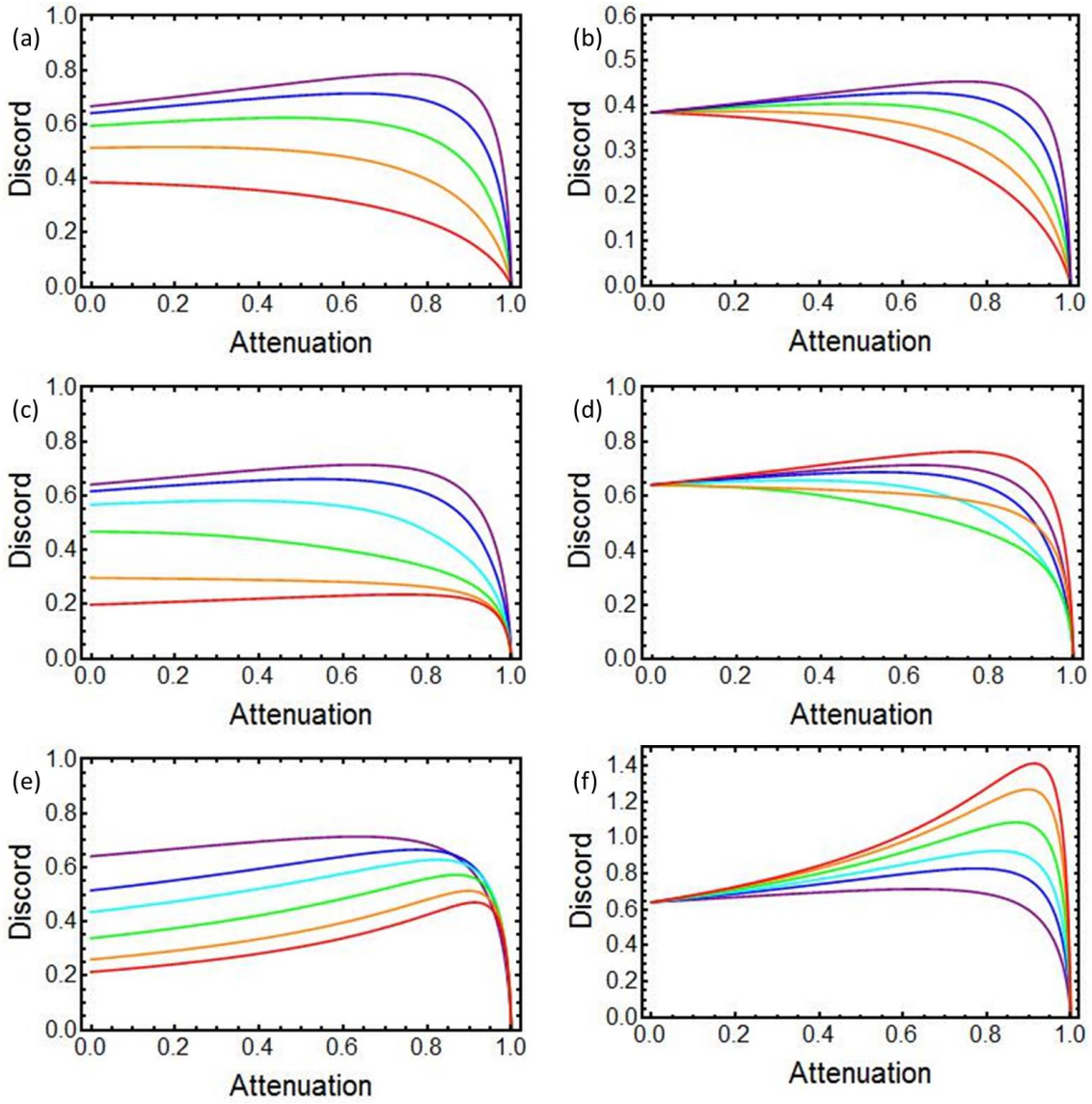


Figure 3.2: (a) Discord increase with loss for thermal states with various initial thermal noise, where the left discord $D^{\leftarrow}(\hat{\rho}_{AB})$ is plotted in each graph. Red: V=4, Orange: V=8, Green: V=16, Blue: V=32, Purple: V=64. (b) Same graphs as (a) but normalised to start from the same value of discord. (c) Discord increase with loss for squeezed thermal states with various initial V_p and constant V_x=32. Purple: V_p=32, Blue: V_p=16, Cyan: V_p=8, Green: V_p=4, Orange: V_p=2, Red: V_p=1. (d) Same graphs as (c) but normalised so that they start from the same value of discord. (e) Discord increase with loss for thermal states with initial V=32 and varying first beamsplitter transmission. Purple: T^2=1/2, Blue: T^2=1/3, Cyan: T^2=1/4, Green: T^2=1/6, Orange: T^2=1/9, Red: T^2=1/12. (f) Same graphs as (e) but normalised so that they start from the same value of discord.

until it is at its most prominent at $V_p = 1$. This effect shows that the behaviour of discord under loss is difficult to explain and has many different influencing factors.

Finally, I consider the case in which the transmission T of the initial beamsplitter is varied. Fig. 3.2 (e) shows the discord increase for varying levels of transmission. The initial value of discord decreases as the transmission decreases, but it can be clearly seen in Fig. 3.2 (f) that the discord increase becomes steadily more pronounced as the transmission decreases, with the maximum value occurring at a higher level of transmission.

Analysis of discord increase

To analyse the causes of discord increase we first need an interpretation of discord. One interpretation of quantum discord is related to information gained by local measurements [158]. Mutual information is how much shared information is stored in the modes, and the one-way classical correlations are the information gained about A after a measurement on B. Therefore discord, being the difference between them, is the shared information that cannot be gained by local measurement. It is therefore closely related to the uncertainty about mode A after a measurement on mode B. With this interpretation, we can try to explain the phenomenon of discord increase.

The first effect to note from Fig. 3.2 (a) is that increasing the modulation of the input thermal state increases the initial value of the discord. This is because, with a higher modulation there is more uncertainty in the quadratures of each mode. Therefore there is more information to be gained about one mode using the other, so the correlations between the mode are larger. Therefore mutual information, classical correlations and quantum discord all increase with increasing thermal noise.

In Fig. 3.2 (b) we see that increasing the thermal noise also increases the level of the discord increase. This can be explained by remembering that a thermal state can be thought of as a mixture of non-orthogonal overcomplete coherent basis states. Increasing the thermal noise means the coherent states making up the mixture are more distinguishable. When loss acts on mode B, these states become less distinguishable, which means that a local measurement will give less information about the state of mode A. This explains why discord increases under the action of local loss for high enough thermal noise. However discord increase doesn't occur for low thermal noise, because loss also degrades the total amount of correlation between the modes. There is a balancing act between the positive and negative effects that loss has on discord. This also explains why discord has to drop to zero as attenuation reaches one, because at that point there is no correlation between the modes, so there is no shared information between modes A and B.

In Fig. 3.2 (c) we again see that reducing the modulation decreases the initial discord in the system. This is for the same reason as the thermal state case. Also, as expected from the above explanation, decreasing the modulation results in a reduction in the discord increase until the increase is no longer observable. However, at some point the discord increase is revived and the increase is most apparent when there is no modulation in the p-quadrature, i.e., V_p=1, as seen in Fig. 3.2 (d). To explain this we need to consider the fact that discord depends on the optimal measurement that maximises the information gained about mode A. In the thermal state (purple curve), the optimal Gaussian measurement is heterodyne detection and since the thermal noise is high enough, discord is seen to increase with loss. In the case of no modulation in the p-quadrature, the optimal Gaussian measurement is homodyne detection of the x-quadrature, and since the thermal

noise in that quadrature is high enough, there is again an observable discord increase with loss. The increase for the red curve is greater because, with homodyne detection, no additional vacuum noise is added by a beamsplitter before measurement, and therefore the measurement is effectively performed on a noisier thermal state, resulting in a larger discord increase. In between these two cases, the optimal measurement is more complicated. In essence, the reduction of the noise in the p-quadrature (from purple to red) suppresses the discord increase, but the switch towards homodyne detection means that the discord increase related to the x-quadrature is accentuated. It is only for low V_p that the latter takes precedence resulting in a revival of the discord increase.

In Fig. 3.2 (e) we see that reducing the transmission decreases the total amount of discord present before loss. This could come from two effects. First, less of the light is transmitted to mode A, so there is less information to gain about mode A by a measurement on mode B. Second, the amplitude in mode B is higher, so a local measurement gives more information than it would for smaller modulation, resulting in a lower value for discord. It is likely that these two effects combine to give the observed reduction in quantum discord.

In Fig. 3.2 (f) it is clear that using a beamsplitter with lower transmission results in a larger increase in discord. This is for the same reason that noisier thermal states experience greater discord increase. As the transmission decreases, the thermal noise in mode B grows, which means the component states are relatively distiguishable. When loss acts on mode B the states become less distinguishable, so a local measurement gives less information about mode A, which causes an increase in discord.

In conclusion there are three main effects that explain the observed behaviour. First, increasing the thermal noise increases the total amount of information available, so the value of discord goes up. Second, discord increases with loss because the states become more indistinguishable meaning local measurements give less information. This is balanced by the fact that loss reduces the total shared information, which explains why discord increase is not always observed. Finally, discord depends on the optimal measurement and when this measurement changes, this can lead to complicated behaviour as seen in Fig. 3.2 (d). These three effects all fit in with the interpretation of discord as shared information that cannot be accessed by local measurements, justifying its use in this case.

3.2.2 Experimental results

An experiment was carried out to investigate whether discord can be observed to increase in a realistic environment [40], and whether experimental imperfections can affect the degree of this increase. This was done using two different methods, one starting from a coherent state, and one starting from a squeezed state. The experimental setup for each of these is shown in Fig. 3.3. The experiment was implemented using Stokes operators [38] with a high excitation of the $\hat{S}_3$ operator so that the $\hat{S}_1$-$\hat{S}_2$ plane (the "dark plane" [132]) can be thought of as analogous to the $\hat{x}$-$\hat{p}$ plane. In both cases, a coherent state was first produced using a soliton laser with pulse length ∼200 fs at a wavelength of 1559 nm (repetition rate: 80 MHz). For the experiment involving a squeezed state, the coherent state was then sent through a polarisation maintaining fibre (FS-PM-7811, Thorlabs, 13 m), exploiting the nonlinear Kerr effect to generate polarisation squeezing in the $\hat{S}_\theta$ direction as described in Section 1.5.2. Thermal noise was added to each of the states by modulating the Stokes observable $\hat{S}_\theta$ with an electro-optical modulator (EOM) as described in Section 1.5.3. The

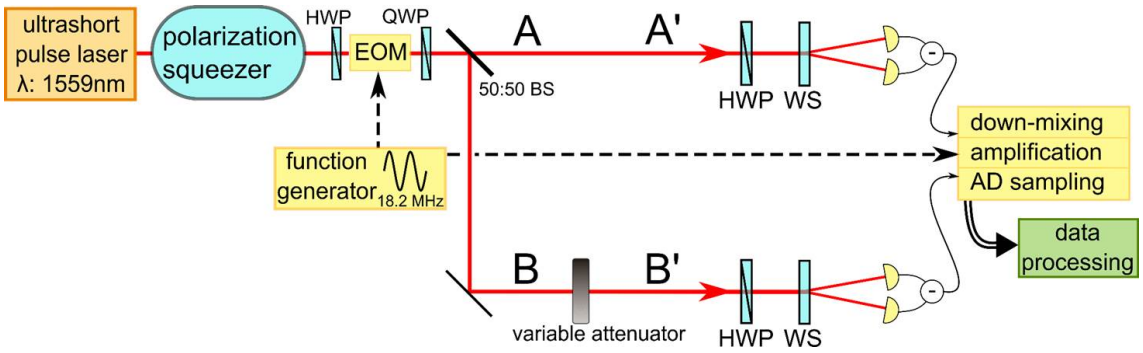


Figure 3.3: Experimental setup for discord increase. EOM: electro-optical modulator, HWP: half-wave plate, QWP: quarter-wave plate, WS: Wollaston prism, BS: beamsplitter. In the experiment involving a mixture of coherent states, the polarisation squeezer is removed. Figure reproduced from [40]

modulated Stokes observable $\hat{S}_\theta$ was adjusted before the EOM by a half-wave plate, and after the EOM by a quarter-wave plate.

The mode was then split on a balanced beamsplitter into two modes A and B, with mode B sent through a variable attenuator. The Stokes observables were then measured as described in Section 1.5.4. The polarising beamsplitter was realised using a Wollaston prism and the photocurrents were measured using PIN photodiode detectors. The Stokes measurement results were used to calculate the covariance matrix by considering all possible combinations of the measurement results. From this the discord was calculated following the method in Section 2.2.4.

For the coherent state case, the modulation in the $\hat{S}_\theta$ direction resulted in a V_x value of 7.1, and since no modulation was carried out in the other direction $V_p = 1$. The results for the discord as a function of attenuation are presented in Fig. 3.4 (a). For the squeezed state case, the modulation in the $\hat{S}_\theta$ direction resulted in a V_x value of 9.84, and the antisqueezing in the $\hat{S}_{\theta+\pi/2}$ direction meant that $V_p = 38.4$. The results for the discord as a function of attenuation are presented in Fig. 3.4 (b).

In both graphs of Fig. 3.4 a theoretical model is fitted to the experimental data. The ideal theoretical model with the appropriate parameters doesn't fit the data very well, however when imperfect common mode rejection (CMR) is included, similarly to [146], the theoretical model is improved. Stokes measurement is based on the photocurrent difference between two beams, and with ideal common mode rejection anything shared between the beams will be cancelled out. This is crucial for the accurate performance of Stokes measurements and homodyne detection [195]. However in a realistic case the CMR will never be perfect and therefore there will always be additional noise present in the measured operators.

To account for this imperfection, we add noise to the theoretical Stokes measurement results to give the operators that are actually measured. The new operators are now

$$\hat{S}_i = \hat{S}_{i,t} + \hat{S}_{i,N}, \tag{3.10}$$

where $\hat{S}_{i,t}$ is the theoretical Stokes measurement result, $\hat{S}_{i,N}$ is the additional noise that comes from imperfect CMR, and $\hat{S}_i$ is the measured Stokes operator. Since the noise is completely uncorrelated to the ideal result, these operators give a covariance matrix that

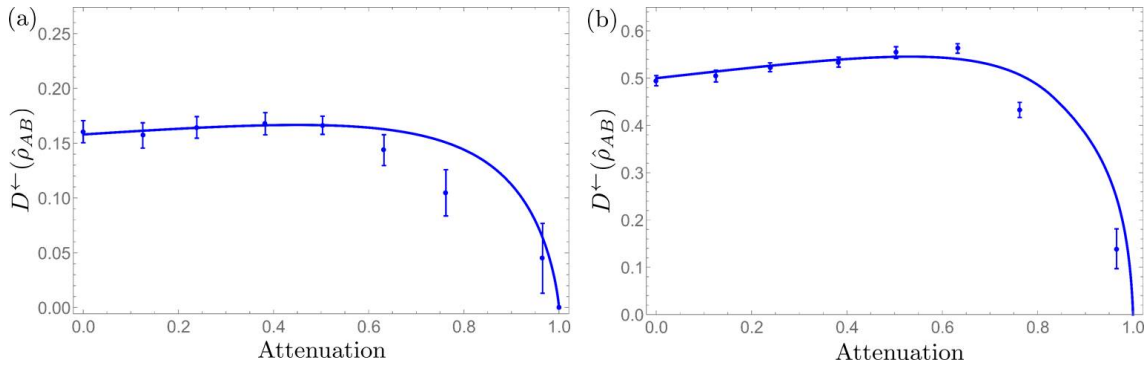


Figure 3.4: (a) Experimental results for discord of modulated coherent state, $V_x = 7.1$, $V_p = 1$. (b) Experimental results for discord of modulated squeezed state, $V_x = 9.84$, $V_p = 38.4$. In both cases a theoretical curve including imperfect CMR is fitted. Note that the theoretical model matches the experimental data less well at high loss. This is because at low light level the accuracy of some of the components is less reliable.

can be written in the form

$$\gamma = \gamma_t + \gamma_{\mathrm{CMR}}, \tag{3.11}$$

where γ_t is the theoretical ideal covariance matrix from Eq. (3.9), γ_{CMR} is the noise matrix coming from imperfect CMR, and γ is the covariance matrix that should give results matching the theory.

To calculate γ_{CMR} we can first note that the $\hat{S}_{i,N}$ for each of the modes are completely uncorrelated and therefore γ_{CMR} is a diagonal matrix. Second, after the first beamsplitter, the two modes are symmetric and the imperfection in the CMR should be the same for both $\hat{S}_1$ and $\hat{S}_2$. Therefore before the loss, the matrix should have the same value on the diagonal. Finally it has to be noted that the biggest contributor to the noise comes from the local oscillator, so the noise is proportional to the amplitude of the local oscillator. For a Stokes measurement the local oscillator travels along with the mode and therefore also undergoes loss when mode B is attenuated. Therefore the noise coming from the imperfect CMR is also attenuated by the loss. Taking all this together, the matrix describing the imperfect CMR is

$$\gamma_{\mathrm{CMR}} = \begin{pmatrix} N & 0 & 0 & 0 \\ 0 & N & 0 & 0 \\ 0 & 0 & T_2^2 N & 0 \\ 0 & 0 & 0 & T_2^2 N \end{pmatrix}, \qquad T_2^2 + R_2^2 = 1, \tag{3.12}$$

where T_2 is the transmission related to the attenuation of mode B, and N is the additional variance caused by the imperfect CMR. This matrix was added to the covariance matrix of Eq. (3.9) to give the covariance matrix used to calculate the theoretical curve in Fig. 3.4, with N optimised to give the best fit to the experimental data.

In both graphs of Fig. 3.4 it can be seen that discord increase is observed, but it is a relatively modest increase. The increase is larger in the squeezed state case, but this is only because of the larger values of V_x and V_p, and has nothing to do with the original squeezed state. The modest increase is due to the fairly small values of V_x and V_p rather than experimental effects. In fact, the experimental increase is larger than the ideal theoretical increase. This is because the imperfect CMR amplifies the discord increase, since the noise in mode B decreases with attenuation, as can be seen in Eq. (3.12). This

shows the importance of separating effects that are a genuine property of the state, and effects that arise from imperfections in the measurement technique.

The phenomenon of discord increase by local loss is an interesting effect and is in stark contrast to the behaviour of entanglement under purely local lossy conditions. It suggests that loss can be used as a positive control mechanism in mixed states, enriching the quantumness possessed by the state. This idea is supported by other work, where it was shown that controlled dissipation can lead to entanglement [124, 155]. It has even been shown that particular forms of environmental dissipation can drive a system to a steady-state that is useful for quantum computation [208]. In both of these cases, dissipation occurs from different parts of the state to a common reservoir, so is consistent with the fact that entanglement must decrease under local loss. Optimism about the phenomenon of discord increase should be cautious, as it is not yet clear whether this effect will be useful or if it is just another unusual property of quantum discord.

3.3 Purification of the discord increase state

All quantum information experiments occur in open quantum systems, which means that correlations arise between the studied system and the environment. These correlations are unobservable, but they are still of interest, and could even be useful. By purifying a quantum state, we can gain insight into the correlations with the environment and perhaps determine how best to use them.

The state $\hat{\rho}_{AB}$ after the first beamsplitter in the discord increase scheme of Fig. 3.1 can be purified by the addition of a third party E that carries all the information about the state that is imprinted on the environment. The state $|\psi\rangle_{ABE}$ is a pure state with $\hat{\rho}_{AB} = \mathrm{Tr}_E(|\psi\rangle_{ABE}\langle\psi|)$. As mode B is attenuated, more information is lost to the environment, and this information has to be absorbed by E giving a new E' to maintain the purification. In general E' would have to be a two-mode state to guarantee that the purification can be maintained, however in this case, since one of the symplectic eigenvalues of $\hat{\rho}'_{AB}$ is equal to one, it is possible to maintain the purification using a one-mode E' for all values of loss [109]. This makes it possible to analyse the flow of correlations between mode A and the environment E' during the attenuation.

Analysing the flow of correlations between $\hat{\rho}_{AB}$ and the environment for the discord increase scheme is complicated by the fact that there are two environmental modes. To calculate entanglement it is necessary to combine these two modes into one, which can be done by purifying the two-mode state γ_{AB} [174]. However this is a complicated calculation and leads to an unintuitive purification that isn't in the simplest form. Instead, the discord increase scheme can be rewritten so that the final state $\hat{\rho}'_{AB}$ emerges from a pure state while there are only ever three modes present in the scheme.

The first step to achieve this purification is to bring the second beamsplitter in front of the first, so that the loss happens before mode A is split into two modes. As long as the transmissions of the beamsplitters are correctly adapted, the final state will be the same. A representation of this is shown in Fig. 3.5, where we have restricted ourselves to the case where the first beamsplitter in the discord increase scheme is balanced.

To find the required values of T_1 and T_2 in Fig. 3.5, one simply has to start with an initial mode A with covariance matrix $\gamma_1 = \mathrm{diag}(V_x, V_p)$, and calculate the resultant covariance matrix $\gamma_{AB'}$ after the two beamsplitters with transmission T_1 and T_2. This

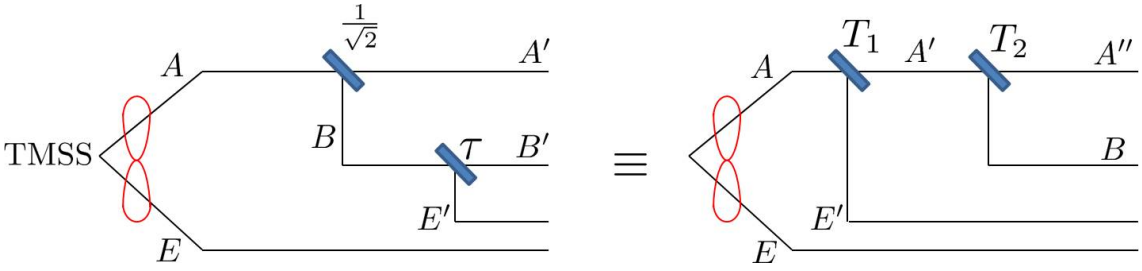


Figure 3.5: On the left is the original discord increase scheme. On the right is the new scheme with the second beamsplitter brought in front of the first. In both cases the initial purification is the same two-mode squeezed state. The additional environmental mode E' is required because of the loss at the lossy beamsplitter. $T_{1,2}$ have to be found so that the final two-mode state $\hat{\rho}_{AB'}$ is the same in both cases.

results in the covariance matrix

$$\gamma_{AB'} = \begin{pmatrix} 1 + T_1^2 T_2^2(\gamma_1 - \mathbb{1}) & -T_1^2 T_2^2 \sqrt{\frac{1-T_2^2}{T_2^2}}(\gamma_1 - \mathbb{1}) \\ -T_1^2 T_2^2 \sqrt{\frac{1-T_2^2}{T_2^2}}(\gamma_1 - \mathbb{1}) & 1 + T_1^2(1-T_2^2)(\gamma_1 - \mathbb{1}) \end{pmatrix}. \tag{3.13}$$

Comparison of this matrix with the one calculated in Eq. (3.9) with $T^2 = R^2 = 1/2$, we get the simple conditions $T_1^2 T_2^2 = \frac{1}{2}$ and $\frac{1-T_2^2}{T_2^2} = \tau^2$. Some simple algebra gives the solutions of these as

$$T_1^2 = \frac{\tau^2 + 1}{2}, \qquad T_2^2 = \frac{1}{\tau^2 + 1}. \tag{3.14}$$

Swapping the order of the beamsplitters has still left a four-mode scheme with two environmental modes; however, if we take mode A' after the first beamsplitter in the right side of Fig. 3.5 as the starting point, we can rewrite it as a three-mode scheme. This is because mode A' is a one-mode state and therefore has a simple two-mode purification. Splitting mode A' on a beamsplitter with the required transmission will result in the final state from the discord increase scheme, but with a three-mode purification allowing properties such as entanglement with the environment to be calculated.

The initial mode A' has the covariance matrix

$$\gamma_{A'} = \begin{pmatrix} V'_x & 0 \\ 0 & V'_p \end{pmatrix}, \qquad V'_{x,p} = \frac{1+\tau^2}{2} V_{x,p} + \frac{1-\tau^2}{2}. \tag{3.15}$$

States of this form have a simple purification of the form

$$\gamma'_{AE} = \begin{pmatrix} V'_x & 0 & \sqrt{V'_x V'_p - 1} & 0 \\ 0 & V'_p & 0 & -\sqrt{V'_x V'_p - 1} \\ \sqrt{V'_x V'_p - 1} & 0 & V'_p & 0 \\ 0 & -\sqrt{V'_x V'_p - 1} & 0 & V'_x \end{pmatrix}. \tag{3.16}$$

To get the final state for discord increase, the last step is to pass mode A' through the T_2

beamsplitter, which results in the three-mode pure state with covariance matrix

$$\gamma'_{ABE} = \begin{pmatrix} \frac{1}{2}(\gamma_1 + \mathbb{1}) & \frac{\tau}{2}(\mathbb{1} - \gamma_1) & \frac{1}{\sqrt{1+\tau^2}} C\sigma_z \\ \frac{\tau}{2}(\mathbb{1} - \gamma_1) & \frac{\tau^2}{2}(\gamma_1 + \mathbb{1}) + \rho^2 \mathbb{1} & -\frac{\tau}{\sqrt{1+\tau^2}} C\sigma_z \\ \frac{1}{\sqrt{1+\tau^2}} C\sigma_z & -\frac{\tau}{\sqrt{1+\tau^2}} C\sigma_z & \gamma_E \end{pmatrix}, \tag{3.17}$$

where

$$\gamma_1 = \begin{pmatrix} V_x & 0 \\ 0 & V_p \end{pmatrix}, \quad \gamma_E = \begin{pmatrix} V'_p & 0 \\ 0 & V'_x \end{pmatrix}, \quad C = \sqrt{V_x V'_p - 1}, \quad \tau^2 + \rho^2 = 1. \tag{3.18}$$

Tracing out mode E gives the same state as for the discord increase scheme, and it can be easily verified to be a pure state by checking that it has vanishing von-Neumann entropy. Therefore the three-mode purification of the state that exhibits discord increase has been successful and it can now be used to investigate the flow of correlations between modes A, B and the environment during loss. This method provides a relatively simple way to calculate the purification and gives the pure state in a form that is easy to understand.

3.4 Flow of correlations

From the Koashi-Winter relation [131] we know that in a three-party pure state, classical correlations and entanglement are related by

$$S(\hat{\rho}_A) = J^{\leftarrow}(\hat{\rho}_{AB}) + E_F(\hat{\rho}_{AE}), \tag{3.19}$$

where E_F is the entanglement of formation defined in Section 2.1.3. Due to the close relationship between classical correlations and quantum discord, it is therefore also possible to study the dynamics of quantum discord and entanglement, and see where they are related. Comparing the dynamics of discord and entanglement in an open system could help draw deeper insight about the phenomenon of discord increase by loss.

The purification of $\hat{\rho}'_{AB}$ calculated in the previous section can be used to analyse the flow of correlation between the modes during the attenuation. The Gaussian versions of each of the terms in Eq. (3.19) can be calculated for the state with covariance matrix (3.17) by taking the appropriate partial trace. Fig. 3.6 shows how the Gaussian entanglement of formation and classical correlations are affected by loss. The Gaussian entanglement of formation was calculated using the method of Adesso and Illuminati [6]. It can be seen from Fig. 3.6 that the entanglement of formation between mode A and the environment rises with increasing attenuation. This rise is matched by the fall in classical correlations. Thus during loss there is a flow of correlations from the classical correlations between modes A and B to entanglement between mode A and the environment. It can be seen from the graph, and confirmed numerically, that the entanglement and classical correlations always add up to the entropy of mode A, as predicted by the Koashi-Winter relation.

As we have seen earlier, the increasing entanglement with the environment is accompanied by an increase in discord between modes A and B. In addition, if the loss is applied to mode A, the discord $D^{\leftarrow}(\hat{\rho}_{AB})$ and the entanglement with the environment $GE_F(\hat{\rho}_{AE})$ both decrease. This shows that in this case the increase in entanglement is related to the

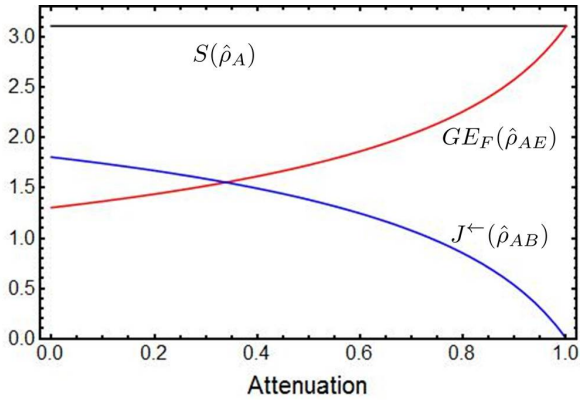


Figure 3.6: $GE_F(\hat{\rho}_{AE})$: Gaussian entanglement of formation between mode A and the environment, $J^{\leftarrow}(\hat{\rho}_{AE})$: classical correlations between modes A and B as measured by mode B, $S(\hat{\rho}_A)$: entropy of mode A, all for $V_x = V_p = 32$. These are plotted against attenuation for the state in Eq. (3.17).

discord increase. As loss acts on mode B, the entanglement between mode A and the environment increases. This results in a decrease in classical correlations between modes A and B, which is accompanied by discord increase. Olivares and Paris [157] studied the relationship between Gaussian discord and Gaussian entanglement of formation in a three-mode pure state, where they found the relationship

$$D^{\leftarrow}(\hat{\rho}_{AB}) + S(\hat{\rho}_E) = S(\hat{\rho}_B) + E_F(\hat{\rho}_{AE}). \tag{3.20}$$

This demonstrates the relationship between the dynamics of discord and entanglement with the environment. As expected, in this work this equation is satisfied, with the increase in entanglement accompanied by discord increase. Only when loss becomes high, and $S(\hat{\rho}_B)$ drops rapidly, does the discord start to decrease. This shows how important the behaviour of entanglement with the environment is to discord dynamics, however the local entropies also play a part. Therefore the behaviour of discord depends on an interesting mixture of entanglement with the environment and local entropies.

In the qubit case, system-environment interactions have also been shown to have some relationship to discord increase. Discord increase can be achieved between two parties A and B by applying an entangling operation to mode A and some additional environmental mode [202]. In this work they also show that the discord increase emerges as a by-product of changes to the other correlation measures. A recent experiment has also been carried out that studies the flow of correlations between a two-qubit state and the environment [7], where they show that the decay of entanglement in a system is accompanied by the growth of multipartite entanglement and discord.

3.5 Alternative analysis of discord increase

The method of purification used in Section 3.3 also opens up a new avenue to interpret the phenomenon of discord increase. In what follows I consider the case where $V_x' = V_p' = V'$ to ease discussion, however the results would be similar if this restriction was lifted. During the purification, we saw that the discord increase scheme can be rewritten as simply splitting a thermal state on a beamsplitter, where both the size of the thermal state and the transmission of the beamsplitter depend on the level of attenuation. The situation is represented in Fig. 3.7 and this means that discord increase with loss can instead be

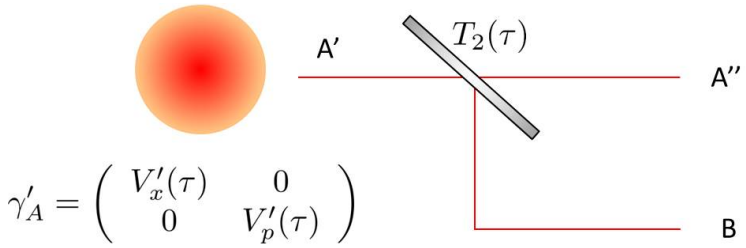


Figure 3.7: Mode A' is a thermal state with variance $V'_x = V'_p$ that depends on the loss. It is split on a beamsplitter with transmission T_2 that also depends on the loss. The final state can be used to study discord increase as long as both the initial variance and the transmission are varied correctly.

interpreted in terms of splitting a thermal state on an asymmetric beamsplitter.

To do this analysis one has to be aware of how the initial variance and transmission depend on loss. From Eq. (3.15), the variance V' is a decreasing function of loss. It decreases from V with no loss to $\frac{V+1}{2}$ for complete attenuation. From Eq. (3.14), the transmission increases from $T_2^2 = \frac{1}{2}$ for no loss to $T_2^2 = 1$ for complete attenuation. To study the behaviour of discord, we can consider both of these effects individually.

First we look at how varying the transmission of the beamsplitter affects the discord behaviour. We only need to consider the case where $T_2^2 \geq \frac{1}{2}$, since those are the values that are needed to compare to the discord increase scheme. In fact, $T_2^2 \leq \frac{1}{2}$ corresponds to the case when loss is applied to mode A, or it gives the behaviour of $D^{\rightarrow}(\hat{\rho}_{AB})$ when loss is applied to mode B. Therefore by considering all values of transmission we can study the right and left-discord simultaneously.

Fig. 3.8 shows the discord as a function of T_2^2 for a range of thermal states. Increasing T_2^2 from 0.5 to 1 is the same as applying loss in the original discord increase scheme. As can be seen in Fig. 3.8 (a), increasing the variance of the thermal state increases the total amount of discord, and it also increases the level of the discord increase. For larger thermal noise, the maximum of discord also occurs at a higher value of transmission, which explains why the maximum of discord was achieved at a higher loss level in the original discord increase scheme. In this case, increasing T_2 means mode B has less thermal noise, which gives a higher level of discord since the basis states making up the mixture are less distinguishable. In Fig. 3.8 (b) the discord as a function of T_2^2 is extended to the full range of transmission values. Reducing transmission from $T_2^2 = 0.5$ to $T_2^2 = 0$ represents the behaviour of the right-discord in the discord increase scheme as loss is increased. Clearly the discord always decreases during this change, which, combined with the fact that the starting variance also reduces with loss, means that the right-discord can never increase as a result of loss on mode B.

It is important to note that any thermal state with $V' > 1$ will give an increase in discord as T_2^2 is increased from 0.5 to 1. However discord increase through loss only happens if the variance is high enough. This is because the variance of the initial thermal state reduces to model increasing loss. This reduces the total discord, so there is a balance between increasing the discord with increasing T_2, and decreasing the discord with decreasing V'. Fig. 3.9 shows a contour plot demonstrating this behaviour. The black lines are the path, from bottom to top, followed by a state as loss is increased in the discord increase scheme. The value of discord varies along the black line in the same way as it varies in the discord increase scheme with increasing loss. In the left-most black line

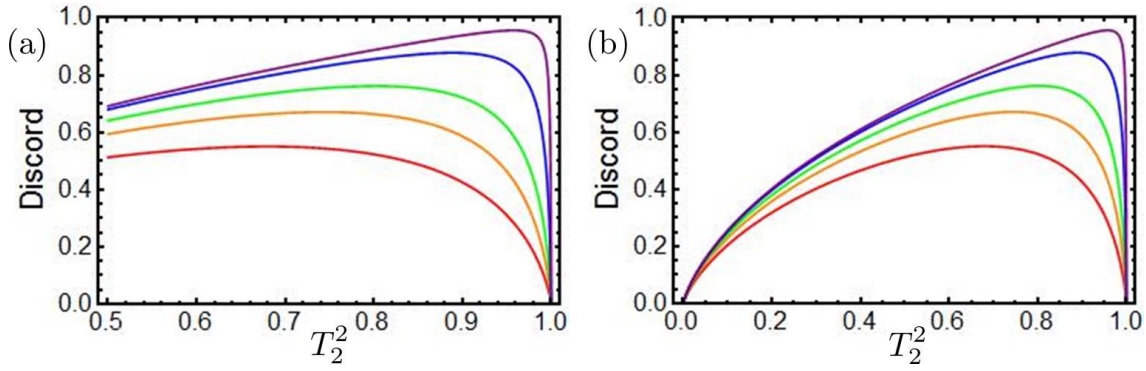


Figure 3.8: Discord $D^{\leftarrow}(\rho'_{AB})$ as a function of T_2^2 for the scheme in Fig. 3.7. Red: $V' = 8$, Orange: $V' = 16$, Green: V'=32, Blue: $V' = 128$, Purple: $V' = 1024$. (a) shows the behaviour between $0.5 \leq T_2^2 \leq 1$. (b) extends the graph down to $T_2^2 = 0$.

corresponding to $V = 4$, it can be seen that the discord immediately begins to fall. For the third line from the left $V = 12$ it is clear that discord initially rises. This increase becomes even larger for lines further to the right, indicating the larger increase in discord for larger thermal states.

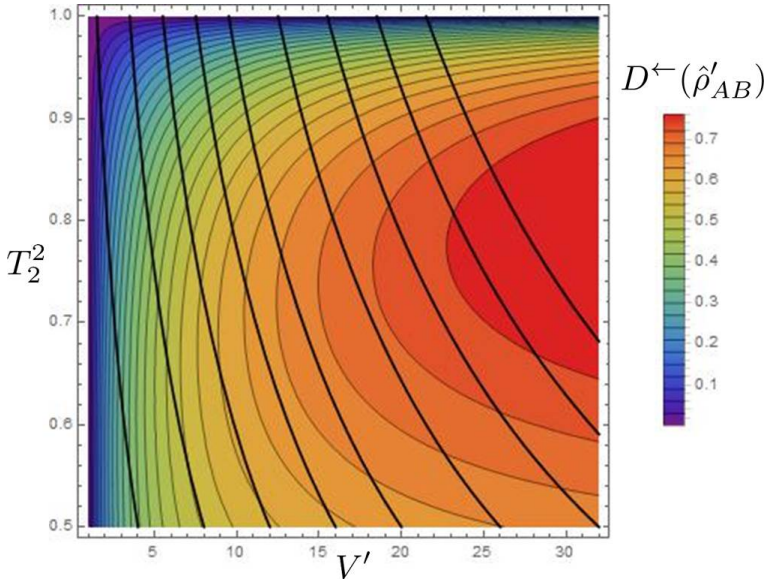


Figure 3.9: Contour plot of $D^{\leftarrow}(\hat{\rho}'_{AB})$ against V' and T_2^2. Black lines: from bottom to top, the path of a state with V=4, 8, 12, 16, 20, 26, 32, 38, 44 from left to right. The discord change along that path is the discord change observed in the discord increase scheme. Note that $V = V'$ at $T_2^2 = 0.5$. V is the variance from the original discord increase scheme and remains constant along each black line.

This graph gives a visualisation of the balance between two different effects related to discord increase. From $T_2^2 = 0.5$, discord increases as you move up and to the right of the graph. Therefore moving up along the black line contributes to discord increase, but moving to the left results in a decrease in discord. At low V, the movement to the left cancels out the small increase in discord that would be observed from moving up the graph, however for larger V, discord increases faster moving up the graph than the reduction caused by moving to the left. Therefore discord increase is observed for larger V but not for small V. This demonstrates that the complicated behaviour of discord increase

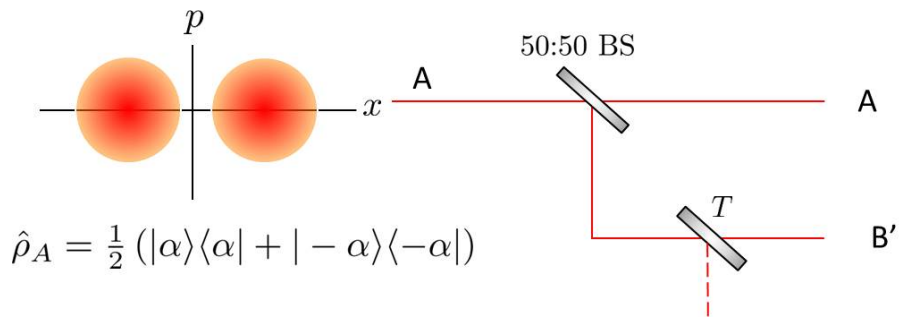


Figure 3.10: A mixture of two coherent states with equal amplitude is sent through a balanced beamsplitter. Loss is then applied to mode B by a variable attenuating beamsplitter.

under local loss can be understood by considering the simpler case of splitting a thermal state.

3.6 Mixture of two coherent states

In previous sections I have discussed that the phenomenon of discord increase is closely related to the non-orthogonality of states. States that are more non-orthogonal are less distinguishable, and therefore a local measurement reveals less of the shared information between two modes. Since loss on mode B makes the states more non-orthogonal, this can result in discord increase. With Gaussian states, it is quite difficult to picture this because each Gaussian state is a continuous mixture of coherent states with different amplitudes, and therefore talking about the non-orthogonality of the states in the mixture is complicated. Here I consider the simpler case of a mixture of two coherent states with the same amplitude but opposite sign. This makes it easier to think about the overlap of the two states making up the mixture as loss is applied.

The situation we consider is presented in Fig. 3.10. The state is initially prepared as a mixture of two coherent states $\hat{\rho}_A = \frac{1}{2}(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|)$. This state is then split on a balanced beamsplitter resulting in the two-mode state

$$\hat{\rho}_{AB} = \frac{1}{2}\left(\left|\frac{\alpha}{\sqrt{2}}\right\rangle_A\left\langle\frac{\alpha}{\sqrt{2}}\right| \otimes \left|\frac{\alpha}{\sqrt{2}}\right\rangle_B\left\langle\frac{\alpha}{\sqrt{2}}\right| + \left|\frac{-\alpha}{\sqrt{2}}\right\rangle_A\left\langle\frac{-\alpha}{\sqrt{2}}\right| \otimes \left|\frac{-\alpha}{\sqrt{2}}\right\rangle_B\left\langle\frac{-\alpha}{\sqrt{2}}\right|\right). \quad (3.21)$$

In this state, if mode B is in the state $|\alpha/\sqrt{2}\rangle$, then mode A must be in the same state. However since $|\alpha/\sqrt{2}\rangle$ and $-|\alpha/\sqrt{2}\rangle$ are non-orthogonal, it is impossible to deterministically identify the state of mode A with a measurement on mode B. Therefore the state possesses some discord. Intuitively, for high α the overlap of the states is small, so the discord must be small. Similarly, for $\alpha = 0$ there are no correlations between the states and the discord is zero.

Now consider the case where loss is applied to mode B, modelled here as a beamsplitter with transmission T. The new state is

$$\hat{\rho}'_{AB} = \frac{1}{2}\left(\left|\frac{\alpha}{\sqrt{2}}\right\rangle_A\left\langle\frac{\alpha}{\sqrt{2}}\right| \otimes \left|\frac{T\alpha}{\sqrt{2}}\right\rangle_B\left\langle\frac{T\alpha}{\sqrt{2}}\right| + \left|\frac{-\alpha}{\sqrt{2}}\right\rangle_A\left\langle\frac{-\alpha}{\sqrt{2}}\right| \otimes \left|\frac{-T\alpha}{\sqrt{2}}\right\rangle_B\left\langle\frac{-T\alpha}{\sqrt{2}}\right|\right). \quad (3.22)$$

As loss increases, the amplitude of the coherent states in mode B decreases, which means their overlap increases. If α is initially high enough this should mean that as the states of mode B become more non-orthogonal, the discord will grow, as in the Gaussian case. To

check if our intuition is correct, we need to be able to calculate the discord for this state. However, since the state is non-Gaussian, it doesn't make sense to use Gaussian discord; instead we need to use a different method to calculate discord.

3.6.1 Calculation of Discord

To calculate the discord of the state $\hat{\rho}'_{AB}$ in (3.22), I follow the method in [85] that gives a reliable method to calculate the quantum discord for an arbitrary two-qubit state, where the measurement on mode B is restricted to projective measurements. This method can also be used to calculate the discord present in the mixture of two coherent states considered here. For this method there are a number of operations on the expression for $\hat{\rho}'_{AB}$ in Eq. (3.22) that must be followed:

- calculate the Gram-Schmidt orthonormalisation of $\hat{\rho}'_{AB}$
- express the state in Bloch form
- convert to Bloch normal form
- use the method of [85] to get an expression for conditional entropy
- optimise the conditional entropy to calculate the discord

To get the Gram-Schmidt orthonormalisation of $\hat{\rho}'_{AB}$, we first need the orthonormal vectors. These are easily calculated to be

$$\begin{aligned} |u_1\rangle_A &= \left|\frac{\alpha}{\sqrt{2}}\right\rangle_A, \quad |u_2\rangle_A = N_A\left(\left|\frac{-\alpha}{\sqrt{2}}\right\rangle_A - \mathrm{e}^{-\alpha^2}\left|\frac{\alpha}{\sqrt{2}}\right\rangle_A\right), \\ |u_1\rangle_B &= \left|\frac{T\alpha}{\sqrt{2}}\right\rangle_B, \quad |u_2\rangle_B = N_B\left(\left|\frac{-T\alpha}{\sqrt{2}}\right\rangle_B - \mathrm{e}^{-T^2\alpha^2}\left|\frac{T\alpha}{\sqrt{2}}\right\rangle_B\right). \end{aligned} \tag{3.23}$$

where $N_A = (1-\exp(-2\alpha^2))^{-\frac{1}{2}}$, $N_B = (1-\exp(-2T^2\alpha^2))^{-\frac{1}{2}}$. Now the coherent states are expressed in terms of the orthonormal vectors as

$$\begin{aligned} \left|\frac{\alpha}{\sqrt{2}}\right\rangle_A &= |u_1\rangle_A, \quad \left|-\frac{\alpha}{\sqrt{2}}\right\rangle_A = \sqrt{1-\mathrm{e}^{-2\alpha^2}}|u_2\rangle_A + \mathrm{e}^{-\alpha^2}|u_1\rangle_A, \\ \left|\frac{T\alpha}{\sqrt{2}}\right\rangle_B &= |u_1\rangle_B, \quad \left|-\frac{T\alpha}{\sqrt{2}}\right\rangle_B = \sqrt{1-\mathrm{e}^{-2T^2\alpha^2}}|u_2\rangle_B + \mathrm{e}^{-T^2\alpha^2}|u_1\rangle_B. \end{aligned} \tag{3.24}$$

Inserting these expressions into Eq. (3.22) gives an expression for $\hat{\rho}'_{AB}$ in terms of orthonormal vectors. After doing this, the state can be written in matrix form as

$$\hat{\rho}'_{AB} = \frac{1}{2}\begin{pmatrix} 1+a^2c^2 & a^2cd & abc^2 & abcd \\ a^2cd & a^2d^2 & abcd & abd^2 \\ abc^2 & abcd & b^2c^2 & b^2cd \\ abcd & abd^2 & b^2cd & b^2d^2 \end{pmatrix}, \tag{3.25}$$

where the rows and columns are in the order $|u_1,u_1\rangle$, $|u_1,u_2\rangle$, $|u_2,u_1\rangle$, $|u_2,u_2\rangle$ and

$$a = \mathrm{e}^{-\alpha^2}, \quad b = \sqrt{1-a^2}, \quad c = \mathrm{e}^{-T^2\alpha^2}, \quad d = \sqrt{1-c^2}. \tag{3.26}$$

Now that I have calculated the Gram-Schmidt orthonormalisation, the next step is to express it in Bloch form. A state is in the Bloch form if it is expressed in the Bloch basis as [207]

$$\rho = \frac{1}{4}\sum_{i,j=0}^{3} R_{ij}\sigma_i \otimes \sigma_j, \tag{3.27}$$

where $R_{ij} = \mathrm{Tr}[\rho(\sigma_i \otimes \sigma_j)]$, $\sigma_0 = \mathbb{1}_2$ and $\sigma_i (i = 1, 2, 3)$ are the Pauli matrices. By careful inspection of the individual elements of Eq. (3.25) the state $\hat{\rho}'_{AB}$ is expressed in Bloch form with the Bloch matrix R given by

$$R = \begin{pmatrix} 1 & cd & 0 & c^2 \\ ab & 2abcd & 0 & ab(c^2 - d^2) \\ 0 & 0 & 0 & 0 \\ a^2 & cd(a^2 - b^2) & 0 & 1 + 2a^2c^2 - a^2 - c^2 \end{pmatrix}. \tag{3.28}$$

To calculate the discord of this state, it is necessary to convert it into the Bloch normal form [143]

$$\hat{\rho} = \frac{1}{4}\left(\mathbb{1}_4 + \sum_i a_i\sigma_i \otimes \mathbb{1}_2 + \sum_i b_i \mathbb{1}_2 \otimes \sigma_i + \sum_i c_i \sigma_i \otimes \sigma_i\right). \tag{3.29}$$

Any arbitrary two-qubit state can be converted into this form [143], and therefore any two-qubit state can be completely described by three three-dimensional column vectors $\vec{a} = \{a_i\}$, $\vec{b} = \{b_i\}$ and $\vec{c} = \{c_i\}$. It can be seen from Eqs. (3.27) and (3.29) that converting a state to Bloch normal form requires the lower $3 \otimes 3$ block matrix of the Bloch matrix R to be diagonalised. Since local unitary operations $\hat{\rho}' = (U_A \otimes U_B)\hat{\rho}(U_A \otimes U_B)^\dagger$ correspond to multiplication of the Bloch matrix R with orthogonal matrices,

$$R' = \begin{pmatrix} 1 & 0 \\ 0 & O_A^T \end{pmatrix} R \begin{pmatrix} 1 & 0 \\ 0 & O_B \end{pmatrix}, \tag{3.30}$$

the normal form can be found by calculating the singular value decomposition of the lower $3 \otimes 3$ block matrix T of R. From Eq. (3.28) it can be seen that the lower $3 \otimes 3$ block matrix is

$$T = \begin{pmatrix} 2abcd & 0 & ab(c^2 - d^2) \\ 0 & 0 & 0 \\ cd(a^2 - b^2) & 0 & 1 + 2a^2c^2 - a^2 - c^2 \end{pmatrix}. \tag{3.31}$$

The singular value decomposition for this matrix is found by expressing $T = O_A C O_B^T$, where $O_{A,B}$ are orthogonal matrices. The columns of O_A are the normalised eigenvectors of TT^T, and the columns of O_B are the normalised eigenvectors of $T^T T$. These are calculated to be

$$O_A = \begin{pmatrix} b & 0 & -a \\ 0 & 1 & 0 \\ a & 0 & b \end{pmatrix}, \quad O_B = \begin{pmatrix} d & 0 & -c \\ 0 & 1 & 0 \\ c & 0 & d \end{pmatrix}. \tag{3.32}$$

The Bloch normal form is now found by calculating R' as in Eq. (3.30), resulting in

$$R' = \begin{pmatrix} 1 & c & 0 & 0 \\ a & ac & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & bd \end{pmatrix}. \tag{3.33}$$

The three three-dimensional column vectors that define the state are thus $\vec{a} = (a, 0, 0)^T$, $\vec{b} = (c, 0, 0)^T$ and $\vec{c} = (ac, 0, bd)^T$. With these vectors, the discord in the state can now be calculated.

The entropies of $\hat{\rho}_B$ and $\hat{\rho}_{AB}$ are easily found from the eigenvalues of the density matrix but calculation of the conditional entropy of mode A after measurement on B is more difficult. An expression for conditional entropy was found in [85] by first introducing the vector $\vec{X} = (x, y, z)$ with $x = 2\cos(\theta)\sin(\theta)\cos(\phi)$, $y = 2\cos(\theta)\sin(\theta)\sin(\phi)$ and $z = 2\cos^2(\theta) - 1$. This vector describes the possible projective measurements on mode B and all possible measurements can be found by varying the angles θ and ϕ. To simplify the expression for $\tilde{S}$ the vectors $\vec{m}_\pm = \{a_i \pm c_i X_i\}$ are also introduced. With these vectors, the conditional entropy $\tilde{S}$ can be written in the form

$$\begin{aligned} \tilde{S} = -\frac{1}{4}\Bigg\{ (1 - \vec{b}\cdot\vec{X}) \Bigg[\left(1 - \frac{|\vec{m}_-|}{1 - \vec{b}\cdot\vec{X}}\right) \log_2 \left(1 - \frac{|\vec{m}_-|}{1 - \vec{b}\cdot\vec{X}}\right) \\ + \left(1 + \frac{|\vec{m}_-|}{1 - \vec{b}\cdot\vec{X}}\right) \log_2 \left(1 + \frac{|\vec{m}_-|}{1 - \vec{b}\cdot\vec{X}}\right) \Bigg] + (1 + \vec{b}\cdot\vec{X}) \times \\ \Bigg[\left(1 - \frac{|\vec{m}_+|}{1 + \vec{b}\cdot\vec{X}}\right) \log_2 \left(1 - \frac{|\vec{m}_+|}{1 + \vec{b}\cdot\vec{X}}\right) + \left(1 + \frac{|\vec{m}_+|}{1 + \vec{b}\cdot\vec{X}}\right) \log_2 \left(1 + \frac{|\vec{m}_+|}{1 + \vec{b}\cdot\vec{X}}\right) \Bigg] \Bigg\}. \end{aligned} \tag{3.34}$$

This expression depends on θ and ϕ and thus depends on the measurement performed on mode B. The last step for calculation of quantum discord is to minimise this term over all possible measurements. The final expression for quantum discord is therefore

$$D^{\leftarrow}(\hat{\rho}'_{AB}) = S(\hat{\rho}'_B) - S(\hat{\rho}'_{AB}) + \min_{\theta,\phi} \tilde{S}(\theta, \phi), \tag{3.35}$$

where $\hat{\rho}'_B = \mathrm{Tr}_A(\hat{\rho}'_{AB})$.

3.6.2 Behaviour of quantum discord

The expression for $\tilde{S}$ in Eq. (3.34) can be numerically minimised on Mathematica, which allows the behaviour of discord to be plotted for this state. The behaviour of discord is shown in Fig. 3.11 for varying levels of initial coherent state size and attenuation. The first thing to note is that for low α, there is no observable discord increase. This result is similar to that in the Gaussian case, where modulation had to be large enough to observe discord increase. When α reaches about 0.7, discord increase becomes observable. This effect is small at first but quickly becomes more pronounced. Note that discord increase is observed at a much smaller amplitude with two coherent states than with Gaussian-distributed coherent states, where a modulation of about 5.8 was required for discord increase. This is because for Gaussian distributed coherent states, even with a large modulation there are still many coherent states with small amplitude. This means

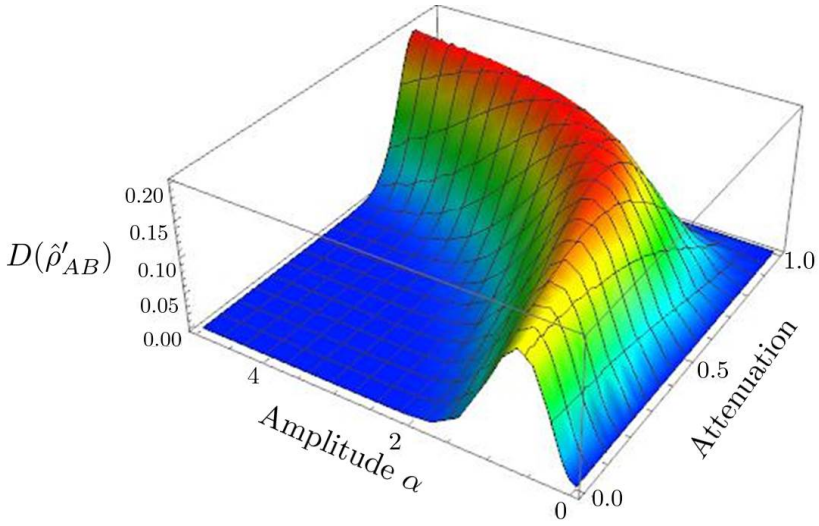


Figure 3.11: Discord behaviour for the split mixture of coherent states after loss on mode B as a function of coherent state amplitude and attenuation. There is a "ridge of discord" where discord reaches its maximum, outside of which the discord is close to zero.

the modulation has to be much higher to achieve the same "average non-orthogonality" as the two coherent state case.

For high α, the discord is very close to zero for low loss. This is because the states have very little overlap, so a measurement on B will have very little uncertainty about the state of mode B. Since mode A and B are either both $|\alpha\rangle$ or both $|-\alpha\rangle$, a measurement on mode B will gain almost all the shared information between the two modes, meaning the discord must be very small. As loss increases, the states of mode B become less distinguishable, so a measurement on mode B will leave more uncertainty about mode A, and the discord must increase. Note that increasing α only has a small influence on the maximum level of discord. This shows that the biggest influence on the total level of discord is the overlap of the measured states, rather than the amplitude of the states in the other mode.

The most striking feature of Fig. 3.11 is the "ridge of discord", the small area where discord increases rapidly from about zero to a maximum value, then drops rapidly to zero again. This ridge suggests there is an optimal non-orthogonality between the states making up the mixture in mode B. Again there is a balance; if the amplitude is too high, a measurement on mode B can reveal almost all the shared information, but if the amplitude is too low, there is not enough shared information between the modes. Just like Goldilocks, discord requires the conditions to be "just right" in order to reach its maximum value.

Since quantum key distribution (QKD) relies heavily on the non-orthogonality of states, it is interesting to ask whether this graph can give any information about the security of QKD. When there is no loss on mode B, this situation is similar to the case of QKD running at a loss level of 50%. In that scenario, mode B would be attributed to an eavesdropper, and mode A given to one of the participants in QKD. Interestingly, at a loss level of 50% the optimum amplitude that maximises the key rate in QKD has been found to be about $\alpha = 0.7$ [201], which is similar to the amplitude that gives the maximum discord as measured on mode B. This suggests that the amplitude for optimal key rate is similar to that which maximises the discord. The study of the role of discord in QKD is interesting, although it is likely that the efficiency of QKD protocols cannot be

explained by discord alone. It has been shown by Pirandola [169] that secret key rate is upper bounded by quantum discord.

By studying the behaviour of discord under loss for a discrete mixture of coherent states, we have gained greater understanding about what causes discord increase. With a mixture of two coherent states, rather than a continuous Gaussian mixture, the importance of the non-orthogonality of the constituent states is given greater clarity. The same phenomenon underlies the discord increase in both cases, but it is much easier to visualise when only two coherent states make up the mixture.

3.7 Summary of Chapter 3

In this chapter I have investigated the phenomenon of discord increase under loss using a variety of methods. I first described how loss can increase, or even introduce, discord in a discrete variable setting. I then studied under what conditions discord increase can occur, and what affects the size of the increase. By purifiying the state involved in discord increase, I discussed how discord increase could be related to the flow of correlations to the environment. I then gave an alternative viewpoint to study discord increase in terms of splitting a thermal state on an unbalanced beamsplitter. Finally I calculated discord increase for a discrete mixture of coherent states, rather than a Gaussian mixture. This brought greater focus on the non-orthogonality of the states making up the mixture, identifying it as the primary driver of discord increase. Non-orthogonality of states is one of the most important contributors to quantum correlations beyond entanglement, and has many applications, particularly in quantum cryptography.

4

Entangling Power of a Beamsplitter

A beamsplitter is an important optical device that has applications in many optics experiments. A beamsplitter superimposes incident light modes and can therefore be used to investigate interference effects, for example in the Hong-Ou-Mandel experiment [113]. Quadrature amplitudes are also superimposed by the action of a beamsplitter and therefore correlations can arise between the output modes. We have already seen in the previous chapter how a beamsplitter can be used to create discord between two modes, simply by inputting a thermal state to one port of the beamsplitter. More importantly, a beamsplitter is frequently used as a continuous variable entangler [75, 191], transforming a pair of input modes into an entangled state. This is most commonly achieved by mixing two modes that are squeezed in conjugate quadratures on a beamsplitter, resulting in an entangled state carring Einstein-Podolski-Rosen correlations [64]. States created in this way are used in many continuous variable experiments, including quantum teleportation [75, 94], dense coding [139] and quantum cryptography [175, 190, 62].

However, the beamsplitter is a passive operation [177] that doesn't affect the photon number of the input state, which means entanglement can only be created from Gaussian states if the incident modes carry some initial nonclassicality [226, 128]. If the states incident on a beamsplitter are statistical mixtures of coherent states, the output states are also classical [29]. Nonclassicality of Gaussian states is equivalent to squeezing [28, 216], and therefore the incident states must be squeezed in order to get entanglement at the output. While for pure states squeezing is a necessary and sufficient condition for entanglement, a stricter condition must be met if the input state is mixed [223].

In this chapter, I investigate counterintuitive situations where a beamsplitter can create entanglement even if the state input to the ports of the beamsplitter is completely classical. This is only possible if the input state is correlated to an additional mode or modes, and is most interesting when the full input state is completely separable. In the separable case the correlations are measured by quantum discord, and they perform a crucial role in the performance of the protocol. The work in this chapter is primarily based on work presented in [50].

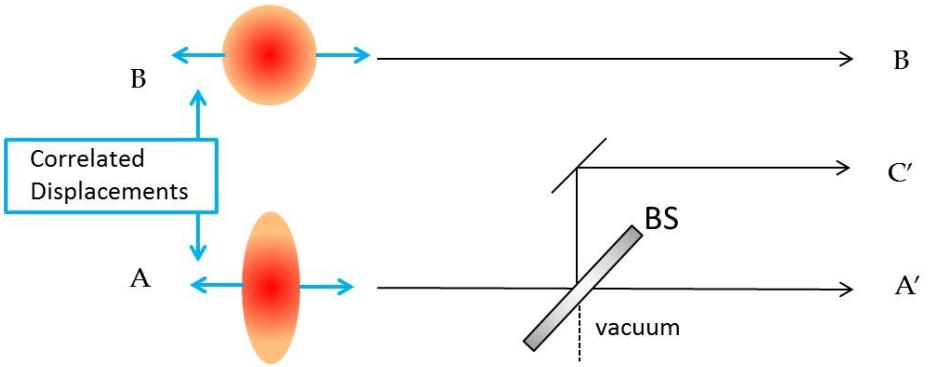


Figure 4.1: Mode A is prepared in a squeezed state and mode B is a coherent state. Correlated displacements are performed on the two modes to create a correlated mixed state. Mode A is mixed on a balanced beamsplitter with the vacuum resulting in a three-mode state.

4.1 Entanglement by splitting an individually classical mode on a beamsplitter

In the first protocol that demonstrates the entangling power of a beamsplitter, the initial separable state is two-mode and is prepared by correlated random displacements in one quadrature of a squeezed state and a vacuum state. After the displacements, assuming the displacements are large enough, the squeezed state is classical since it has a positive P-function, which means splitting it on a beamsplitter will not result in entanglement between the output modes [226, 128]. Instead it creates a three-mode state in which the output modes of the beamsplitter are individually separable, but each output mode is entangled with the remaining two modes. Therefore, even though the input mode to the beamsplitter is classical, entanglement has emerged at the output demonstrating the entangling power of a beamsplitter.

4.1.1 Theoretical description

The protocol is depicted in Fig. 4.1. Initially, Alice holds mode A squeezed in its position quadrature $\hat{x}_A$ and Bob holds mode B in the vacuum state. The respective covariance matrices read as $\gamma_B = \mathbb{1}$ and

$$\gamma_A^i = \begin{pmatrix} V_x & 0 \\ 0 & V_p \end{pmatrix}, \tag{4.1}$$

where $V_x = 2\langle(\Delta x_A)^2\rangle < 1$, $V_p = 2\langle(\Delta p_A)^2\rangle$, and $V_x V_p \geq 1$. Modes A and B are then displaced as

$$\hat{x}_A \to \hat{x}_A + \bar{x}, \quad \hat{x}_B \to \hat{x}_B + \bar{x}, \tag{4.2}$$

where the classical displacement $\bar{x}$ is distributed with a Gaussian distribution with zero mean and variance $\langle\bar{x}^2\rangle = \sigma^2$. After the displacements modes A and B are in a Gaussian state with covariance matrix

$$\gamma_{AB} = \begin{pmatrix} V_x + 2\sigma^2 & 0 & 2\sigma^2 & 0 \\ 0 & V_p & 0 & 0 \\ 2\sigma^2 & 0 & 1 + 2\sigma^2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{4.3}$$

The state was created by local operations and classical communication (LOCC) and therefore it is separable. The variance σ^2 is chosen such that the squeezing in mode A is destroyed, i.e., $V_x + 2\sigma^2 \geq 1$. In addition, the state has to be nonclassical because otherwise it would be a convex mixture of coherent states which cannot yield entanglement by splitting one of its parts on a beam splitter. A Gaussian state is nonclassical if and only if the lowest eigenvalue of its covariance matrix is less than one[223]. The eigenvalues of the covariance matrix (4.3) are $\lambda_1 = 1$, $\lambda_2 = V_p$,

$$\lambda_{3,4} = \frac{1}{2}\left(1 + 4\sigma^2 + V_x \pm \sqrt{1 + 16\sigma^4 - 2V_x + V_x^2}\right), \tag{4.4}$$

and therefore the state is nonclassical if and only if $\lambda_4 < 1$. Rearrangement of Eq. (4.4) for λ_4 shows that this condition is equivalent to $V_x < 1$. As long as mode A is initially squeezed, the state with covariance matrix (4.3) is nonclassical, and therefore suitable for the protocol.

Mode A is now mixed with a vacuum state $\gamma_C = \mathbb{1}$ on a balanced beamsplitter. Note that since mode A is no longer squeezed, it is impossible for the beamsplitter to create entanglement between the two output modes. The beamsplitter transforms the two-mode state into a three-mode state with covariance matrix

$$\gamma_{A'BC'} = \begin{pmatrix} \frac{1}{2}(\gamma_A + \mathbb{1}) & \frac{1}{\sqrt{2}}\gamma_{AB} & \frac{1}{2}(\gamma_A - \mathbb{1}) \\ \frac{1}{\sqrt{2}}\gamma_{AB} & \gamma_B & \frac{1}{\sqrt{2}}\gamma_{AB} \\ \frac{1}{2}(\gamma_A - \mathbb{1}) & \frac{1}{\sqrt{2}}\gamma_{AB} & \frac{1}{2}(\gamma_A + \mathbb{1}) \end{pmatrix}, \tag{4.5}$$

where $\gamma_A = \mathrm{diag}(V_x + 2\sigma^2, V_p)$, $\gamma_B = \mathrm{diag}(1 + 2\sigma^2, 1)$, and $\gamma_{AB} = \mathrm{diag}(2\sigma^2, 0)$.

To check whether the protocol has worked it is necessary to check whether the expected separability properties are observed in the final state. The first thing to note is that this state was prepared by LOCC across the $B|AC$ bipartition, and therefore mode B is separable from modes AC and also from each mode individually. Thus we just have to check the other bipartitions for their separability properties, which is done using the positive partial transpose (PPT) criterion described in Sec. 2.1.2. The separability of modes A' and C' after the beamsplitter is assessed by tracing out mode B and checking the physicality of the partially transposed state. The eigenvalues of $\gamma_{A'C'}^{T_A} + i\Omega_2$ are

$$\begin{aligned} \lambda_{1,2} &= \frac{1}{2}\left(V_x + 2\sigma^2 + 1 \pm \sqrt{(V_x + 2\sigma^2 - 1)^2 + 4}\right), \\ \lambda_{3,4} &= \frac{1}{2}\left(V_p + 1 \pm \sqrt{(V_p - 1)^2 + 4}\right). \end{aligned} \tag{4.6}$$

These two sets of eigenvalues are of the same form, and as long as $V_x + 2\sigma^2 \geq 1$ and $V_p \geq 1$, the minimum eigenvalue $\lambda_{\min} \geq 0$ and the state is separable. This agrees with what we would expect since a classical mode split on a beamsplitter cannot create entanglement.

The last cases to check are the $A|BC$ and $C|AB$ splittings, but since modes A and C are perfectly symmetric, it is only necessary to check one of these cases. Only two of the eigenvalues of $\gamma_{A'BC'}^{T_A} + i\Omega_3$ depend on V_p and they are always positive if $V_p > 1$ as it is in this case. The other four are solutions of a fourth-order polynomial equation so an analytic solution has not been found for them. However the minimum eigenvalue $\lambda_{\min} = 0$ when $V_x = 1$, and when $V_x < 1$, $\lambda_{\min} < 0$ no matter what value of $2\sigma^2$ is chosen.

Therefore, any state of the form (4.3) that has $V_x < 1$ will be entangled across both the $A|BC$ and $C|AB$ bipartitions after splitting mode A on a balanced beamsplitter. Note that in a realistic scenario when the correlations between modes A and B are not perfect, the squeezing of mode A will have to be suitably strong to account for any imperfections in order to observe entanglement creation.

In this section I have described the theoretical situation whereby entanglement can be created by splitting a fully classical state on a beamsplitter. The correlations between modes A and B before the beamsplitter make this possible. Since the two modes are individually classical, but form a nonclassical state when taken together, the correlations between the modes must carry some quantumness. This quantumness is captured by quantum discord, and is particularly interesting because the correlations are only present in one quadrature. This is in contrast to many previous experiments on quantum discord [146, 96, 210], and supports the work in [40] where it was found that correlations in one quadrature can lead to quantum behaviour.

A similar effect has been seen for discrete variables, where a CNOT gate can generate entanglement by acting on part of a three-qubit fully separable state [4]. The discord present between two of the initial modes (where the third mode is the control of the CNOT) determines how much entanglement can be activated in the process. In the continuous variable case, a beamsplitter can sometimes be used to activate entanglement. However not all discordant states are suitable for entanglement activation by a beamsplitter [152]; additional nonclassicality in the form of global squeezing is also necessary.

The fact that global squeezing before the beamsplitter is a vital component of the protocol relates to work by Ferraro and Paris [73], where different notions of nonclassicality were discussed. In quantum optics, negativity of the P-function is considered the indicator of nonclassicality, whereas in quantum information the most general indicator of nonclassicality is quantum discord. In [73], they showed that the two notions of classicality were maximally inequivalent. This means that the set of states without quantum discord that are also classical according to the P-function has zero measure. However for this scheme, the original state with covariance matrix (4.3) must possess both squeezing and discord, thus demonstrating the importance of both of these forms of nonclassicality to the performance of the protocol. In particular, it is the squeezing that is converted into entanglement; discord has to be present because there must be some correlation between the two modes prior to the beamsplitter so that the squeezing that is destroyed by the displacements can be recovered.

4.1.2 Experimental implementation

An experiment was carried out in [50] to demonstrate the principle of entanglement creation by splitting a classical state and verify that it is achievable under realistic conditions. The experimental setup for the protocol is shown in Fig. 4.2. The yellow circles and ellipses are the states for the entanglement from discord protocol and all the experimental methods are the same as for the discord increase experiment. The correlated displacements were realised by digitally mixing together differently displaced states in a correlated manner, as described in Section 1.5.3, resulting in a mixed state before the beamsplitter. After the experimental results were combined, the measured covariance matrix of the final state

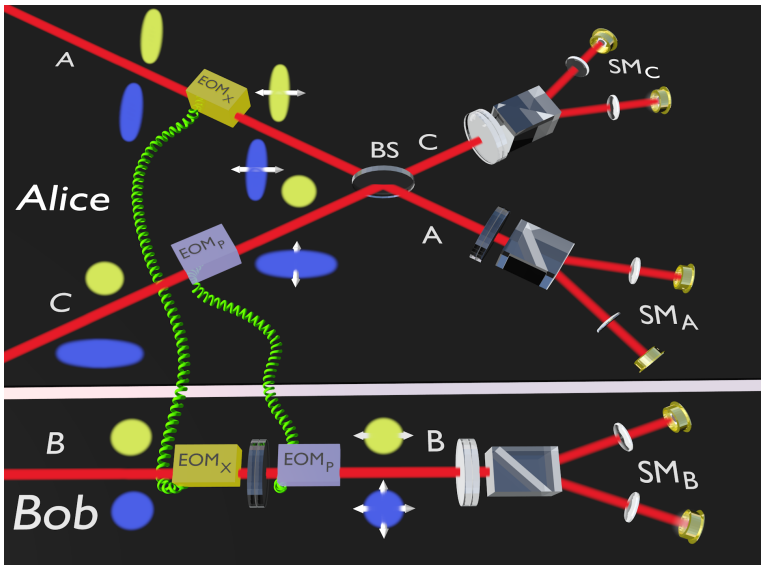


Figure 4.2: Experimental scheme. EOM_x and EOM_p: electro-optical modulators implementing displacement of quadratures $\hat{x}$ (white horizontal arrow) and $\hat{p}$ (white vertical arrow). BS: balanced beam splitter, SM_j: Stokes measurement on mode j. The yellow circles and ellipses represent the states of the entanglement from discord protocol, and the blue circles and ellipses are the states for the entanglement distribution protocol. The yellow (blue) modulators EOM_x (EOM_p) are applied to both protocols (only to the entanglement distribution protocol).

was found to be

$$\gamma_{ABC} = \begin{pmatrix} 5.42 & 0.23 & 3.34 & -0.73 & 4.06 & 0.04 \\ 0.23 & 19.28 & 0.00 & 0.00 & 0.45 & 17.29 \\ 3.34 & 0.00 & 3.43 & -0.54 & 3.06 & -0.03 \\ -0.73 & 0.00 & -0.54 & 1.12 & -0.67 & 0.01 \\ 4.06 & 0.45 & 3.06 & -0.67 & 4.73 & 0.55 \\ 0.04 & 17.29 & -0.03 & 0.01 & 0.55 & 17.70 \end{pmatrix}. \tag{4.7}$$

The measurement errors for the elements of the covariance matrix lie between 0.002 and 0.023. The approximate values used for the experiment were $V_x = 0.61$, $V_p = 38.4$ and $2\sigma^2 = 9.23$. There are a few things to note about this experimental covariance matrix. First, since $V_x V_p \gg 1$, the initial state of mode A is highly mixed. This is because of additional phase noise in the p-quadrature that comes from guided-acoustic-wave Brillouin scattering in optical fibres used during the squeezing process. Second, the correlations are not perfect between modes A and B before the beamsplitter, in contrast to the theoretical case. This can be seen in the (3,3) entry of γ_{ABC} since it is less than $1 + 2\sigma^2$.

To verify whether the required separability properties are present, even with these imperfections, it is necessary to check the PPT criterion [193] on the various bipartitions. To ease this discussion I will use the notation $\lambda_k^{T_j} \equiv \min[\mathrm{eig}(\gamma_k^{T_j} + i\Omega_3)]$. First the three-mode separability properties can be checked by taking the partial transpose with respect to each mode in turn and checking the PPT criterion. The results for this are shown in Table 4.1. From this table, it can be seen that the state is entangled across the $A|BC$ splitting as well as the $C|AB$ splitting, while it remains separable across the $B|AC$ splitting. Since mode B is separable from modes AC, this also implies that mode B is separable from modes A and C individually. The last thing to check is that modes A and C are separable from each other, which is true since for $\gamma_{AC} = \mathrm{Tr}_B(\gamma_{ABC})$ the minimum eigenvalue is

j	A	B	C
$\lambda_{ABC}^{T_j}$	-0.022 ± 0.001	0.069 ± 0.001	-0.022 ± 0.001

Table 4.1: Minimum eigenvalues for the three mode separability properties.

$\lambda_{AC}^{T_A} = 0.84 \pm 0.01 > 0$. Therefore the experimentally measured state with covariance matrix (4.7) fulfils all the required separability properties.

It is important to note that a beamsplitter can only create three-mode entanglement if there is some nonclassicality before the beamsplitter that remains throughout the whole procedure [223, 121]. In this case, the nonclassicality is global squeezing that is present at the end as evidenced by $\min[\mathrm{eig}(\gamma_{ABC})] = 0.91 \pm 0.01 < 1$. An interesting property of the covariance matrix (4.7) is that the minimum eigenvalue of γ_{AC} is $\min[\mathrm{eig}(\gamma_{AC})] = 0.91 \pm 0.01 < 1$. This suggests that the reduced state after the beamsplitter is squeezed, even though the state split on the beamsplitter has high variance in both the x- and p-quadratures. However this is just an artifact originating in imperfections in the experiment. Since the vacuum is input at one of the ports of the beamsplitter, it is very close to a squeezed state, so even small errors could make the output state appear squeezed.

This experiment has demonstrated that entanglement can be formed by splitting a classical state on a beamsplitter, as long as it is part of a larger state. The resultant entanglement does not occur between the outputs of the beamsplitter, but is instead three-mode entanglement between one output mode and the remaining two modes. These separability properties do not exist for pure states, and therefore require an initially mixed state. To get an idea about the degree of the mixedness of the experimental state, the purity of the covariance matrix (4.7) can be calculated. This is found to be $P = 1/\sqrt{\det(\gamma_{ABC})} = 0.01090$, which shows that the state is highly mixed, since $P = 1$ for pure states. This experiment has also shown that the effect is robust against noise and experimental imperfections.

4.1.3 Conditions for the scheme to work

In the previous sections I have described a particular protocol where entanglement can be created by splitting a classical part of a two-mode state on a beamsplitter. It is interesting to study whether this property is widespread, or if it takes a specific set of circumstances for this effect to take place. Consider a general two-mode state that possesses no $\hat{x}$-$\hat{p}$ correlations

$$\gamma_{AB} = \begin{pmatrix} a_1 & 0 & c_1 & 0 \\ 0 & a_2 & 0 & c_2 \\ c_1 & 0 & b_1 & 0 \\ 0 & c_2 & 0 & b_2 \end{pmatrix}. \tag{4.8}$$

To achieve the required separability criteria, the state must satisfy a number of conditions. It must be a physical state, a separable state and a nonclassical state. In addition, splitting mode A on a beamsplitter must result in entanglement. This must occur while modes A and B are individually classical, i.e., $a_{1,2} \geq 1$ and $b_{1,2} \geq 1$. A state is physical if its minimum symplectic eigenvalue is greater than or equal to one. A state with covariance matrix (4.8) has minimum symplectic eigenvalue

$$\nu_{\min} = \frac{1}{\sqrt{2}} \sqrt{\Delta_+ - \sqrt{\Delta_+^2 - 4(a_1 b_1 - c_1^2)(a_2 b_2 - c_2^2)}}, \tag{4.9}$$

where $\Delta_+ = a_1a_2 + b_1b_2 + 2c_1c_2$. A state is separable if the minimum eigenvalue of its partial transpose is greater than or equal to one. For a state with covariance matrix (4.8), its partial transpose has minimum symplectic eigenvalue

$$\tilde{\nu}_{\min} = \frac{1}{\sqrt{2}}\sqrt{\Delta_- - \sqrt{\Delta_-^2 - 4(a_1b_1 - c_1^2)(a_2b_2 - c_2^2)}}, \tag{4.10}$$

where $\Delta_- = a_1a_2 + b_1b_2 - 2c_1c_2$. A state is nonclassical if its minimum eigenvalue is less than one. The minimum eigenvalue of γ_{AB} is

$$\lambda_{\min} = \min_{i=1,2} \frac{1}{2}\left(a_i + b_i - \sqrt{(a_i - b_i)^2 + 4c_i^2}\right). \tag{4.11}$$

In addition to modes A and B being classical and physical, these three conditions must be satisfied if a state is to produce entanglement by splitting a classical part of a separable state. Now I will look at a number of frequently used states to see if it is common for these conditions to be simultaneously satisfied.

The first class of states I look at are isotropic states. An isotropic state has a covariance matrix of the form

$$\gamma_{\text{iso}} = \nu \begin{pmatrix} \cosh(2r)\mathbb{1} & \sinh(2r)\sigma_z \\ \sinh(2r)\sigma_z & \cosh(2r)\mathbb{1} \end{pmatrix}, \tag{4.12}$$

where $\nu \geq 1$. From Eq. (4.9) it can be seen that this state is physical for all $\nu \geq 1$. From Eq. (4.10), the minimum symplectic eigenvalue of the partial transpose is $\tilde{\nu}_{\min} = \nu e^{-2r}$. Therefore the state is separable if $\nu \geq e^{2r}$. The minimum eigenvalue is calculated using Eq. (4.11) to be νe^{-2r}, so for the state to be non-classical $\nu < e^{2r}$. Therefore no isotropic state can be both separable and non-classical, so isotropic states are not suitable for this scheme.

Symmetric two-mode squeezed thermal states can have a covariance matrix of the form

$$\gamma_{STS} = \begin{pmatrix} a\mathbb{1} & c\mathbb{1} \\ c\mathbb{1} & a\mathbb{1} \end{pmatrix}. \tag{4.13}$$

From Eq. (4.9), the minimum symplectic eigenvalue of the state is $\nu_{\min} = a - c$. Therefore for a physical state $c \leq a - 1$. Since $\text{Det}(\mathbf{C}) > 0$, where $\mathbf{C}$ is the off-diagonal block matrix describing the correlations, physical states of this form are always separable. From (4.11), the minimum eigenvalue is $\lambda_{\min} = a - c$. This coincides with the minimum symplectic eigenvalue which means physical states of this form are never non-classical.

The other form for symmetric two-mode squeezed thermal states is

$$\gamma_{STS} = \begin{pmatrix} a\mathbb{1} & c\sigma_z \\ c\sigma_z & a\mathbb{1} \end{pmatrix}. \tag{4.14}$$

Since taking the partial transpose is equivalent to flipping the sign of the momentum quadrature, we see that this covariance matrix is simply the partial transpose of the previous form for a squeezed thermal state. This means that the criteria for a physical state and a separable state have swapped for this class compared to the previous class of squeezed thermal states. Since the previous form of squeezed thermal states could never be both physical and nonclassical, a state of this form is never both separable and nonclassical. Therefore neither of the classes of symmetric squeezed thermal states can be

used to create entanglement by splitting a classical state.

Surprisingly, we have found that a number of commonly used states can never be suitable for this form of entanglement creation. Motivated by the state used in the previous section, I will now look at general states with no momentum correlations ($c_2 = 0$ in Eq. (4.8)) and try to find conditions that a state must satisfy to be suitable for the scheme. From Eq. (4.9), for the state to be physical we get the condition

$$c_1^2 \leq \left(a_1 - \frac{1}{a_2}\right)\left(b_1 - \frac{1}{b_2}\right). \tag{4.15}$$

Since $c_2 = 0$, Δ_+ and Δ_- are the same, and therefore the condition for separability is the same as that for physicality. From Eq. (4.11), for the state to be nonclassical we get the condition

$$c_1^2 > (a_1 - 1)(b_1 - 1). \tag{4.16}$$

These conditions can be satisfied simultaneously, as long as at least one of a_2 or b_2 is greater than 1. To check if the state can truly become entangled, we need to look at the symplectic eigenvalues of the partial transpose after mode A is passed through a balanced beamsplitter. The minimum symplectic eigenvalue of this state with mode A or C partially transposed is

$$\tilde{\nu}_{\min} = \frac{1}{\sqrt{2}}\sqrt{a_1 + b_1 b_2 - \sqrt{(a_1 - b_1 b_2)^2 + 4b_2 c_1^2}}. \tag{4.17}$$

For entanglement across the $A : BC$ and the $C : AB$ splitting $\tilde{\nu}_{\min} < 1$. This results in the criterion for entanglement

$$c_1^2 > (a_1 - 1)\left(b_1 - \frac{1}{b_2}\right). \tag{4.18}$$

Comparing this to the criterion for non-classicality, we see that this is a tighter criterion with the two coinciding when $b_2 = 1$. We already know $a_{1,2} \geq 1$ and $b_{1,2} \geq 1$. Combining Eqs. (4.15) and (4.18) we get the additional conditions $a_2 > 1$ and $b_1 > \frac{1}{b_2}$. The second of these means either $b_{1,2} > 1$. This gives us the final set of criteria for states with $c_2 = 0$ that become entangled after mode A is split on a balanced beamsplitter as

$$a_1 \geq 1, \;\; a_2 > 1, \;\; b_{1,2} \geq 1, \;\; b_1 > \frac{1}{b_2},$$

$$\left(a_1 - \frac{1}{a_2}\right)\left(b_1 - \frac{1}{b_2}\right) \geq c_1^2 > (a_1 - 1)\left(b_1 - \frac{1}{b_2}\right). \tag{4.19}$$

For particular values of $a_{1,2}$ and $b_{1,2}$, these equations give a range of values for c_1 that are both physical and give a state that can become entangled. The correlations have to be strong enough so that the state is nonclassical, but not so strong that it is entangled or unphysical. Note that increasing b_2 has no affect on the range of c_1 values consistent with the scheme, but it does mean that there are more nonclassical states that do not become entangled by a balanced beamsplitter. It is likely that alternative operations could create entanglement for such states. However any nonclassical state with $b_2 = 1$ becomes entangled if mode A is split on a beamsplitter. It is also interesting that the condition for entanglement is independent of a_2, so no matter how much excess noise exists in the p-quadrature of mode A, the state can still become entangled.

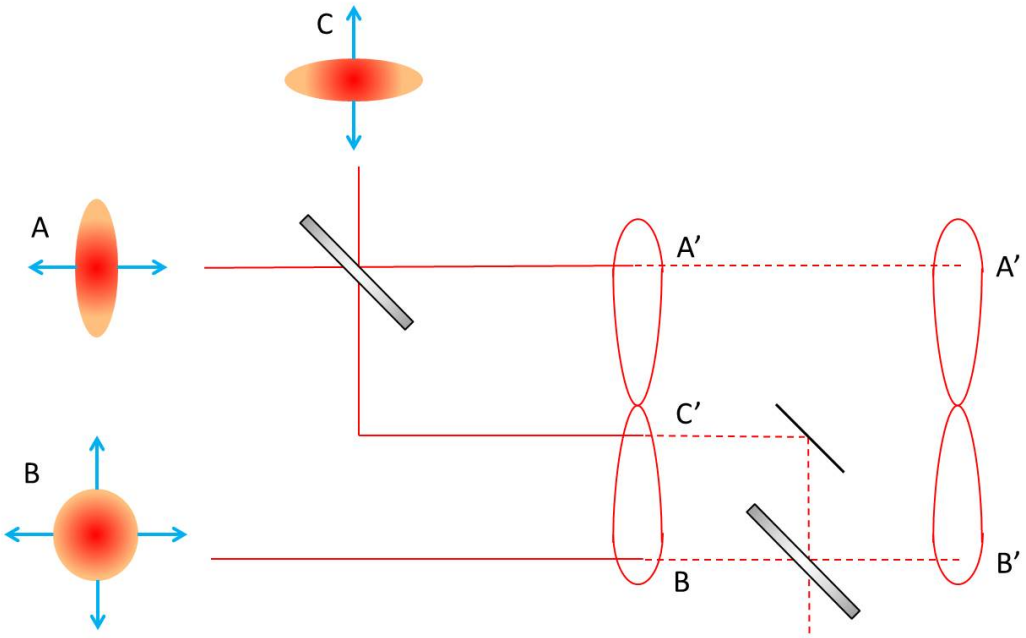


Figure 4.3: Depiction of the entanglement distribution protocol. Solid lines: The first two steps of the protocol considered here. Dotted lines: The final step of the protocol, described in [153], that localises the entanglement to two-mode entanglement. Initially, modes A and C are orthogonally squeezed states and mode B is the vacuum, then correlated displacements are added to the modes. Modes A and C are mixed on a beamsplitter resulting in a three-mode state that is entangled across the $A|BC$ splitting but separable otherwise. For the full protocol, modes B and C are mixed on a beamsplitter to localise the entanglement between modes A and B.

4.2 Entanglement distribution by separable states

The protocol described in the previous section is based on a similar principle as the protocol for entanglement distribution by separable states described in [151, 153], and implemented in [167]. Here, I briefly describe the first two steps of the protocol in order to draw comparisons with the scheme in the previous section and further highlight the entangling power of a beamsplitter. Entanglement distribution by separable states was first proposed for qubits in [51] and for CV in [151, 153]. It was experimentally demonstrated simultaneously for qubits [72] and for CV [167, 212].

4.2.1 Theoretical Scheme

Whereas in the previous scheme the initial state consisted of two modes, in this protocol the initial state is a three-mode state. The protocol is depicted in Fig. 4.3. Initially, mode A is in a position-squeezed state, mode C is a momentum-squeezed state and mode B is the vacuum. This means $2\langle\hat{x}_a^2\rangle = 2\langle\hat{p}_C^2\rangle = \exp(-2r)$ and $2\langle\hat{p}_a^2\rangle = 2\langle\hat{x}_C^2\rangle = \exp(2r)$ where $r > 0$ is the squeezing parameter. These modes are then displaced by

$$\hat{x}_A \to \hat{x}_A + \bar{x}, \quad \hat{p}_C \to \hat{p}_C - \bar{p}, \quad \hat{x}_B \to \hat{x}_B + \sqrt{2}\bar{x}, \quad \hat{p}_B \to \hat{p}_B + \sqrt{2}\bar{p}, \tag{4.20}$$

where $\bar{x}$ and $\bar{p}$ are uncorrelated classical displacements following Gaussian distributions with zero mean and variances $\langle\bar{x}^2\rangle = \langle\bar{p}^2\rangle = \sigma^2 \equiv (e^{2r} - 1)/2$. Note that the displacements add enough noise to destroy the initial squeezing present in modes A and C, meaning that each mode is individually classical. Next, modes A and C are mixed on a balanced

beamsplitter to create a new correlated three-mode state. Since modes A and C are classical and uncorrelated, the two output modes must be separable. The covariance matrix of the state after the beamsplitter is

$$\gamma_{ABC} = \begin{pmatrix} (\cosh(2r)+\sigma^2)\mathbb{1} & 2\sigma^2\sigma_z & (\sinh(2r)-\sigma^2)\sigma_z \\ 2\sigma^2\sigma_z & (1+4\sigma^2)\mathbb{1} & -2\sigma^2\mathbb{1} \\ (\sinh(2r)-\sigma^2)\sigma_z & -2\sigma^2\mathbb{1} & (\cosh(2r)+\sigma^2)\mathbb{1} \end{pmatrix}. \tag{4.21}$$

The separability properties of this state can be checked by the PPT criterion. The state is clearly separable across the $B|AC$ bipartition since it was created by LOCC across this splitting. The state is entangled across the $A|BC$ bipartition for $r > 0$ and $\sigma^2 \geq 0$. The state is separable across the $C|AB$ bipartition for $r > 0$ as long as $2\sigma^2 \geq \mathrm{e}^{2r} - 1$, which is why it was chosen as $2\sigma^2 \equiv (e^{2r} - 1)$ in this case. Therefore this scheme has demonstrated the effect where two uncorrelated classical states mixed together on a beamsplitter result in entanglement, as long as they are suitably correlated to a third mode. This is a similar effect to that discussed in the previous section and further demonstrates the entangling power of a beamsplitter.

4.2.2 Experimental Implementation

The full entanglement distribution scheme in this form was implemented experimentally in [167], and the first two steps were given greater focus in [50]. A schematic of the protocol implemented in [50] is shown by the blue circles and ellipses of Fig. 4.2. The steps of the experiment were carried out as described in the previous section. Measurement of the Stokes operators gave the covariance matrix of the final state as

$$\gamma_{ABC} = \begin{pmatrix} 20.90 & 1.10 & 5.17 & -8.59 & -7.80 & -1.68 \\ 1.10 & 25.31 & -5.04 & -6.76 & 1.00 & 14.64 \\ 5.17 & -5.04 & 11.87 & -0.45 & 4.95 & 4.49 \\ -8.59 & -6.76 & -0.45 & 18.88 & -8.61 & 6.04 \\ -7.80 & 1.00 & 4.95 & -8.61 & 20.68 & 0.80 \\ -1.68 & 14.64 & 4.49 & 6.04 & 0.80 & 24.65 \end{pmatrix}. \tag{4.22}$$

The required separability properties can be checked using the PPT criteria. The relevant eigenvalues needed to find the three-mode separability properties are shown in Table 4.2.

This shows that after the beamsplitter, the state is entangled across the $A|BC$ bipartition but separable across the $C|AB$ and $B|AC$ bipartitions, as predicted by the theory. Therefore the experiment has shown that entanglement can be generated by mixing two uncorrelated classical states on a beamsplitter, as long as they are suitably correlated to a third mode. Note that since there is only entanglement across one bipartition, it is impossible for there to be two-mode entanglement. For example if modes A and C were entangled, there would have to be entanglement across both the $A|BC$ and $C|AB$ splittings. This shows that the generated entanglement is genuine three-mode entanglement not caused by a nonclassical state entering one of the ports of the beamsplitter. Similarly to the previous protocol, there must be some global nonclassicality to allow entanglement to be created. In this case it is global squeezing, which is quantified by the eigenvalue $\min[(\mathrm{eig}(\gamma_{ABC})] = 0.609 \pm 0.003 < 1$.

Due to the specific entanglement properties of the state with covariance matrix (4.22), the state can be used for entanglement distribution by separable states. As was shown in

j	A	B	C
$\lambda_{ABC}^{T_j}$	-0.144 ± 0.001	0.351 ± 0.002	0.528 ± 0.003

Table 4.2: Minimum eigenvalues $\lambda_k^{T_j} \equiv \min[\text{eig}(\gamma_k^{T_j} + i\Omega_3)]$ for the three mode separability properties.

Section 2.2.2, the entanglement that can be generated in this way is upper-bounded by the relative entropy of discord between mode C and modes AB, as measured by mode C. This demonstrates the importance of discord to the performance of this scheme.

In both of the described protocols, the final states can be further processed to localise the entanglement into two-mode entanglement. This can be achieved by the action of a beamsplitter on two of the modes, thus further demonstrating the entangling power of a beamsplitter. This effect has been shown theoretically for the entanglement sharing protocol of [150], and experimentally demonstrated in the entanglement distribution protocol of [167].

The previous two protocols both demonstrate an important property of a beamsplitter. A beamsplitter can create entanglement even if the input modes are uncorrelated and classical, as long as the modes are suitably correlated to an additional mode. This brings into sharp focus the importance of global correlations when considering nonclassicality. To determine if a state is nonclassical, it is not sufficient to look at the individual mode; it is important to consider all the correlations the state possesses. States that at first appear unsuitable for quantum information processes, could actually be useful if they possess appropriate global correlations. This is an important area of research as the quest for quantum information protocols that are robust in open quantum systems continues.

4.2.3 Transformation between entanglement classes

The two protocols described also demonstrate the power of a beamsplitter to transform states between the entanglement classes described in Section 2.1.4. In both of the protocols, the states are initially in class 5, the class of three-mode fully separable states. In the first protocol, the first beamsplitter transforms the state into class 2, the class of one-mode biseparable states. A second beamsplitter can be used to localise the three-mode entanglement across $A|CB$ into two-mode entanglement between modes A and C. This property was demonstrated in the entanglement sharing protocol [150].

In the second protocol the first beamsplitter transforms the state from class 5 into class 3, the class of two-mode biseparable states. Similarly, a second beamsplitter can be used to localise the entanglement into two-mode entanglement between modes A and C. In this instance, the entanglement can't be localised by LOCC, thus demonstrating the advantage that a beamsplitter has for localising entanglement. This property was demonstrated in the entanglement distribution by separable states protocol [167].

4.3 Collaborative dense coding

The previous states have three-mode entanglement but no two-mode entanglement. This means that in order to make use of this entanglement one must have access to all three modes. This opens up the possibility of quantum information protocols that require three parties to collaborate. Here I investigate one such protocol called "collaborative dense coding" that requires three parties to work together to decode information more efficiently

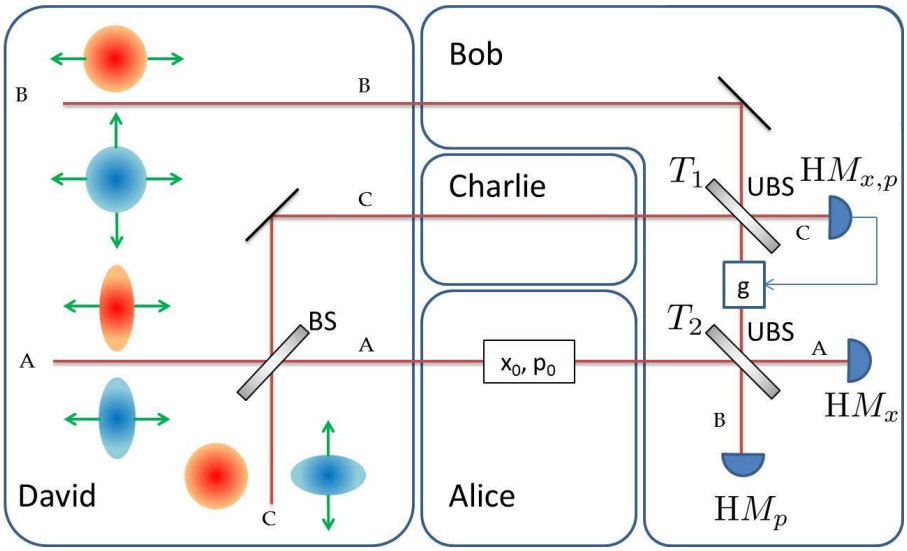


Figure 4.4: Collaborative dense coding schemes for a state from the entanglement from discord section (orange circles and ellipsis) and the entanglement distribution by separable states section (blue circle and ellipses). BS: balanced beam splitter, UBS: unbalanced beam splitters with transmissivities T_1 and T_2, HM_i:homodyne measurement on i-quadrature.

than classically possible.

Standard quantum dense coding [24, 27] involves only a sender Alice and a receiver Bob, who share a two-mode entangled state. Alice encodes a message on to her mode and sends it to Bob. The maximum amount of classical information that can be transmitted over this channel is well-established [111, 182]. However Bob is able to make use of the initial entanglement to gain more information about the message than is classically possible. In the qubit case [24, 148], during the messaging stage Bob receives two bits of information for every qubit Alice sent. This is twice as good as the classical limit of one bit of information per bit sent. The cost of this is that Alice and Bob have to share a quantum resource in the form of an entangled qubit pair, so overall they have shared two qubits and transferred two bits of information. However the entangled pair could have been distributed at any point in the past, and so at the time when the message was sent, two bits of information have been sent with the distribution of one qubit, thus demonstrating the advantage of quantum dense coding.

A similar result has been found for continuous variables [27, 139, 176], where the quantum resource Alice and Bob initially share is a pair of EPR beams. Some time later, Alice encodes a signal into each of the quadratures of her EPR beam and sends it to Bob. Bob interferes this beam with his EPR beam, and because of the EPR correlations can gain more information than classically possible. In the asympotic limit of high photon number, Bob can gain twice as much information as the classical limit [27], giving an analogous result to the qubit case.

A controlled dense coding scheme has been proposed [98] and experimentally demonstrated [125], in which a controller Charlie controls the rate at which Bob can receive information. In controlled dense coding Alice, Bob and Charlie hold a pure state that possesses genuine tripartite entanglement, for example a Greenberger-Horne-Zeilinger (GHZ) [93] state for discrete variables or an analogue of the GHZ state for continuous variables [205]. In these cases the control of information capacity is accomplished by a measurement

on Charlie's mode.

In the "collaborative dense coding" described here, the three parties share a mixed state that only has entanglement spread between three modes, as described in the previous sections. Charlie controls the capacity by interference of the collaborating mode with that of the receiver. If Charlie does not allow his mode to be used by the receiver Bob, it is impossible for the information transmission capacity to exceed the classical limit, so this is truly an example of collaborative dense coding.

The scheme for collaborative dense coding is shown in Fig. 4.4. One of the two states described in the previous sections is prepared by an additional party David to emphasise that none of the parties need to have control of the state preparation for the protocol to work. Modes A, B and C are then distributed to Alice, Bob and Charlie respectively. Alice encodes a signal x_0, p_0 chosen from a random Gaussian set to the $\hat{x}$- and $\hat{p}$-quadratures of mode A, where the variance of the signal is $2\langle x_0^2\rangle = 2\langle p_0^2\rangle = V_s$. She then sends mode A to Bob who is tasked with gaining as much information about the signal as possible. Assuming Charlie collaborates, Bob now has all three modes and can use them in any way to decode the signal with maximum efficiency. Bob's first step is to superimpose modes B and C on an unbalanced beamsplitter with transmission T_1 where $T_1 + R_1 = 1$. After this, the quadratures of the modes have been transformed as $\hat{\alpha}'_{B,C} = \sqrt{T_1}\hat{\alpha}_{B,C} \pm \sqrt{R_1}\hat{\alpha}_{C,B}$, where $\alpha = x, p$. This beamsplitter has the result of localising the three-mode entanglement between modes A and BC to two-mode entanglement between mode A and B. Bob then measures the $\hat{p}$-quadrature of mode C' with outcome $\bar{p}$ and displaces the mode B' by $\hat{p}'_B \to \hat{p}'_B + g\bar{p}$, where the gain g is chosen to maximise the capacity of the scheme. This measurement and displacement further strengthens the entanglement between modes A and B' to aid with the decoding capacity. Finally, Bob superimposes modes A and B' on a second unbalanced beamsplitter with transmissivity T_2 where $T_2 + R_2 = 1$, and measures the $\hat{x}$-quadrature of output mode A and the $\hat{p}$-quadrature of output mode B.

The capacity for this channel is calculated using the formula for channel capacity of a state with Gaussian distributed signal of power S, and Gaussian distributed noise of power N, $C = (1/2)\ln(1 + S/N)$ [187]. In this scheme there are two measurements giving information about different signals, so the channel capacity is

$$C = \frac{1}{2}\ln\left(1 + \frac{V_s}{N_x}\right)\left(1 + \frac{V_s}{N_p}\right), \tag{4.23}$$

where $N_{x,p}$ are the variances of the noises in the measured quadratures normalised by the attenuation the measured signal has experienced from the second beamsplitter. This noise can be calculated by calculating the quadratures at the end of the scheme. For the entanglement from discord scheme the normalised noises in the measured quadratures are found to be

$$\hat{x}_N = x_A^{(0)} e^{-r}\left(\frac{1}{\sqrt{2}} + \sqrt{\frac{R_1 R_2}{2T_2}}\right) + \bar{x}\left(\frac{1}{\sqrt{2}} + \sqrt{\frac{R_2}{T_2}}\left(\sqrt{\frac{R_1}{2}} - \sqrt{T_1}\right)\right)$$
$$-x_B^{(0)}\sqrt{\frac{T_1 R_2}{T_2}} + x_C^{(0)}\left(\frac{1}{\sqrt{2}} - \sqrt{\frac{R_1 R_2}{2T_2}}\right),$$

$$\hat{p}_N = p_A^{(0)} e^r \left(\frac{1}{\sqrt{2}} - \sqrt{\frac{T_2}{R_2}} \left(\sqrt{\frac{R_1}{2}} + g\sqrt{\frac{T_1}{2}} \right) \right) + p_B^{(0)} \sqrt{\frac{T_2}{R_2}} \left(\sqrt{T_1} - g\sqrt{R_1} \right) + p_C^{(0)} \left(\frac{1}{\sqrt{2}} + \sqrt{\frac{T_2}{R_2}} \left(\sqrt{\frac{R_1}{2}} + g\sqrt{\frac{T_1}{2}} \right) \right), \tag{4.24}$$

where r is the squeezing parameter, $\bar{x}$ is the correlated displacement and $x_i^{(0)}$, $p_i^{(0)}$ are the vacuum quadratures of mode i. These are connected to $N_{x,p}$ by $2\langle \hat{x}_N^2 \rangle = N_x$, $2\langle \hat{p}_N^2 \rangle = N_p$. Similar expressions for the noise can be found for the entanglement distribution by separable states scheme.

The behaviour of channel capacity against maximal average photon number is the quantity that is of most interest. In this case, mode A after the signal is encoded is the most intense mode travelling through the channel. The average photon number $\bar{n}$ of a beam is given by [176]

$$\bar{n} = \frac{V_+ + V_-}{4} - \frac{1}{2}, \tag{4.25}$$

where $V_{+,-}$ are the variances of the two quadratures. For the entanglement from discord scheme, called protocol 1 from now on, the noise from correlated displacements is chosen to be as small as possible while still retaining the relevant separability properties, so $2\langle \bar{x}^2 \rangle = 1 - \mathrm{e}^{-2r}$. For the entanglement distribution scheme I consider two cases for the noise from the correlated displacements. The first is the case where the noise is at its smallest value such that mode C is separable from modes AB after the first beamsplitter, $2\langle \bar{x}^2 \rangle = 2\langle \bar{p}^2 \rangle = \mathrm{e}^{2r} - 1$, called protocol 2 from now on. The second case is that where the noise is just large enough to destroy the squeezing before the first beamsplitter, $2\langle \bar{x}^2 \rangle = 2\langle \bar{p}^2 \rangle = 1 - \mathrm{e}^{-2r}$, called protocol 3. In this second case, the state after the first beamsplitter has the same entanglement properties as the state from the entanglement from discord scheme. This gives three different schemes that have average photon number

$$\bar{n}_1 = \frac{4V_s + \mathrm{e}^{2r} - 1}{8}, \quad \bar{n}_2 = \frac{2V_s + 2\mathrm{e}^{2r} + \mathrm{e}^{-2r} - 3}{4}, \quad \bar{n}_3 = \frac{2V_s + \mathrm{e}^{2r} - 1}{4}, \tag{4.26}$$

where $\bar{n}_1$ is the average photon number for protocol 1, $\bar{n}_2$ is the average photon number for protocol 2, and $\bar{n}_3$ is the average photon number for protocol 3.

The capacity of the different schemes is calculated by numerically maximising Eq. (4.23) at fixed average photon number for each of the schemes. The maximisation is carried out over r, V_s, $T_{1,2}$ and g, and the results are plotted for varying photon number in Fig. 4.5. The results for the different protocols are shown alongside the capacity for coherent state communication with heterodyne detection $C^{coh} = \log_2(1 + \bar{n})$ [227] and squeezed state communication with homodyne detection $C^{sq} = \log_2(1 + 2\bar{n})$ [227]. C^{coh} is the maximum information that can be decoded without any squeezing or nonclassicality, so anything above this line is evidence of dense coding. As can be seen, the capacity of each of the protocols exceeds the classical capacity for sufficiently high photon number. C^1 exceeds C^{coh} for $\bar{n} > 0.36$, and $C^{2,3}$ exceed C^{coh} for $\bar{n} > 0.44$; therefore each of these states is suitable for collaborative dense coding. In fact, C^3 even exceeds C^{sq} for sufficiently high photon number $\bar{n} > 11.28$, which is a similar result to the capacity of controlled dense coding in [125]. In that case the dense coding was achieved using a pure three-mode state. Here, I have shown that even if there is a lot of additional noise at the start of the protocol, the correct decoding procedure can still achieve a high channel capacity. Note

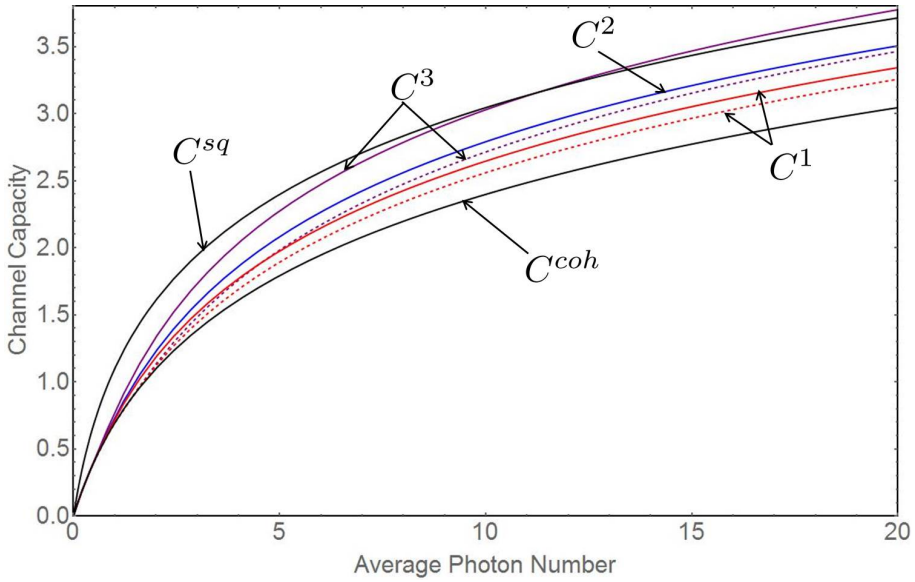


Figure 4.5: Solid coloured lines: channel capacities C^1, C^2 and C^3 for protocols 1, 2 and 3. Dashed lines: channel capacities for protocols 1 and 3 with no interference between modes B and C. Black lines: C^{sq}, C^{coh} are the capacities of squeezed and coherent state communication.

that to achieve a capacity beyond C^{coh} using this method, there must be entanglement between the two modes before the final beamsplitter (if the signal is ignored).

The dashed lines in Fig. 4.5 show the case where mode B is measured and the results fed forward, but modes B and C never interfere ($T_1 = 0$ in Fig. 4.4). For protocol 1, the capacity in this case exceeds C^{coh} when $\bar{n} > 1.38$, and for protocol 3 the capacity exceeds C^{coh} when $\bar{n} > 1.46$. However for protocol 2 measurement on mode B without interference can never exceed the classical capacity. This is because the state is separable across the $C|AB$ bipartition, and measurement and feed-forward of results on mode B is an LOCC operation that can never increase entanglement. This means modes A and C are separable, so the capacity can never exceed the coherent state capacity. The other two capacities do exceed C^{coh} because measurement and feed-forwarding can localise entanglement between two modes. This is only possible if there is entanglement across at least two of the three bipartitions.

From Fig. 4.5 it is clear that the capacities of the protocols obey the hierarchy $C^3 \geq C^2 \geq C^1$ for all values of $\bar{n}$. It is clear that C^3 exceeds C^2 because the added noise is lower in protocol 3 than in protocol 2. These capacities are both greater than C^1 because protocols 2 and 3 involve squeezing in both quadratures, whereas protocol 1 only has squeezing in a single quadrature. This additional squeezing increases the photon number of the state, but the benefit to the capacity of having squeezing in both quadratures exceeds this cost. In addition the squeezing in both quadratures means that measurement of the $\hat{x}$- and $\hat{p}$-quadratures reveals the same amount of information, whereas in protocol 1 more information is gained about the $\hat{x}$-quadrature. This symmetric decoding is more efficient, which contributes to the increased capacity of protocols 2 and 3.

It is also worth noting the importance of the first beamsplitter interaction for the performance of collaborative dense coding. If a signal was encoded into mode A before the first beamsplitter, the coherent capacity cannot be beaten. This is because the signal is not encoded on to part of an entangled state, so dense coding is not possible. Finally, it

is important to note that the absence of any of the modes in any of the protocols, makes it impossible to achieve a capacity greater than C^{coh} without any additional quantum resources. This is because all the entanglement is three-mode entanglement, and so it requires collaboration of all three parties to achieve dense coding.

4.4 Summary of Chapter 4

In this chapter I have discussed two protocols that demonstrate the entangling power of a beamsplitter. In each of them, entanglement has been created by mixing two uncorrelated classical beams on a beamsplitter, with entanglement emerging between at least one of the output modes and the remaining two. For the scheme to work, the state before the beamsplitter must have some global nonclassicality, quantified by global squeezing, and it must also possess quantum discord between the modes, while remaining fully separable. This shows the importance of each of these classifications of nonclassicality. Although it is global squeezing that is converted into entanglement, discord has to be there to ensure that the state possesses some correlations before the entangling beamsplitter. Interestingly, I have shown that there are some common classes of two-mode states that are never nonclassical and separable at the same time. However it seems likely that for states that are more mixed, the window in which states can be both nonclassical and separable is bigger. I also discussed how the beamsplitter is used in these protocols to transform between the different classes of three-mode entanglement.

Finally, I have demonstrated an application for these protocols in the form of collaborative dense coding. To use the three-mode entanglement for dense coding all three parties must work together. To do this the power of a beamsplitter is further demonstrated as it's used to localise the three-mode entanglement into two-mode entanglement that can be used for dense coding.

5

Quantum Digital Signatures

A signature provides a method that ensures the authorship of a message and guarantees the integrity of its content. There have been many examples throughout history, from the wax seal of the middle ages to the chip-and-pin system today. One obvious example of a signature is the one on the back of your credit card or in your chequebook. Ideally this can only be produced by you, so anything bearing this signature must have originated from you. However the obvious problem with this is that anyone can observe the exact signature, and so a skilled forger can recreate it almost exactly. Therefore the importance of securing signatures against forgery is clear to see.

Recently, as more and more communication occurs online, digital signatures have become prevalent. These are based on the same principle as other signatures but can be transmitted through the use of computers. However currently used classical digital signature schemes are only secure if one assumes that an adversary has limited computational power. At the moment, this assumption is probably safe, but with the advent of quantum computers many currently used schemes would become immediately insecure. This leads to the requirement for signature schemes that are unconditionally secure, and one possibility for this is a quantum digital signature (QDS). The security of QDS schemes is based on the fundamental principles of quantum mechanics and therefore provides unconditional security. The security of QDS is based on the same principles as security in quantum key distribution (QKD), in particular the non-orthogonality of quantum states.

In this chapter I introduce the properties of a signature scheme and briefly describe currently used classical digital signatures. I give an overview of work done so far on quantum digital signatures, focussing on the differences between schemes. I then introduce a protocol that provides a secure quantum digital signature through the use of homodyne detection, and describe its experimental implementation. Finally, I compare the performance of this scheme with previous work that uses discrete measurement techniques, showing that homodyne detection provides an advantage.

5.1 Introduction to signatures

Digital signature protocols, introduced by Diffie and Hellman in 1976 [58], aim to guarantee the author of a message and also its content. In addition, if one party accepts a signed message, he must be sure that a future party will also accept the message. To be considered secure a signature scheme must satisfy three properties [200]:

1. Unforgeability: Only the creator of the signature can send a message and have it successfully accepted as being genuine.
2. Non-repudiation: Once a message is signed, the signer cannot deny that the message originated from them.
3. Transferability: If someone accepts a signature, he must be confident that any future recipients will also accept the message. He must be sure of this without the need to interact with any other party.

In what follows, I restrict to the simplest case with three parties involved in the signature scheme, a distributor Alice and two recipients Bob and Charlie. Alice will send a signed message first to Bob, who then forwards the signed message to Charlie. In the three-party setting, the notions of non-repudiation and transferability are equivalent. In contrast to the case for QKD, where Alice and Bob are assumed to be honest, in a signature protocol any of the involved parties could be dishonest. In analogy to a signature on a cheque, Alice is the owner of the cheque and wishes to pay Bob, who wants to bring the cheque to Charlie, the bank. When Bob receives the cheque he must be sure that the bank will also accept it; this is transferability. When Charlie (the bank) receives the cheque from Bob, he must be sure that the cheque was signed by Alice; this is unforgeability. Recent work has began to extend QDS to more than three parties [12], but this adds additional complications, e.g. how to deal with colluding adversaries and dispute resolution.

In the case of a conventional handwritten signature, Alice has previously distributed her signature to the other parties before sending the message some time in the future. In both classical and quantum digital signature schemes, there are also two stages, a distribution and messaging stage. In both cases the distribution stage will often be in the form of public key distribution, where all parties are assumed to have access to the public key. In the messaging stage Alice sends her message along with a signature, or private key. All other parties can compare the private key to the public key to verify the signature, but it is impossible to determine the private key from the public key, so only Alice could have signed the message with the private key. Security of this form is often based on a one-way function that converts a private key to a public key. From the private key, the function can easily be used to calculate the public key, however given the public key it is almost impossible to determine the private key.

5.2 Previous digital signature protocols

5.2.1 Classical signature schemes

Most commonly used classical signature schemes are based on one-way functions. An example of a one-way function is prime factorisation; given two prime numbers it is easy to calculate their product, but it is computationally difficult to calculate the prime factors

from their product. This provides the idea behind the Rivest-Adleman-Shamir (RSA) encryption scheme [161], where the product of two prime numbers is the public key, and the prime factors are the private key. Any honest party with access to the correct public key will agree on the result, thus confirming transferability of the message. Only the author of the public key could have access to the private key, thus confirming that the signature cannot be forged. Other classical signature schemes that follow the same principle as the RSA scheme are the digital signature algorithm (DSA) [68] and the elliptic curve digital signature algorithm (ECDSA) [126]. Instead of using prime factorisation, these schemes make use of the assumed computational difficulty of finding discrete logarithms. Interestingly, it has been shown that RSA, DSA and ECDSA can all be efficiently broken by quantum computers [189]. This means that all these schemes will be insecure in a world with quantum computers, making it necessary to develop new signature schemes.

A similar cryptographic tool to one-way functions are hash functions, which can also be used for digital signature schemes. Hash functions are essentially functions that map a longer message x to a shorter string $h(x)$, called a hash. To be useful for a signature scheme, the hash function $h(x)$ must also satisfy the following properties [161]:

1. Given $h(x)$ it must be difficult to find x, i.e., the hash function is a one-way function.
2. Given x_1 it should be difficult to find x_2 such that $h(x_1) = h(x_2)$.
3. It should be difficult to find any distinct pair x_1, x_2 such that $h(x_1) = h(x_2)$.

These hash functions only provide computational security since there are no known one-way functions that are provably more difficult to invert than compute.

Currently existing quantum digital signature schemes are closely related to hash-based signature schemes. Lamport [135] introduced a one-time signature scheme that is computationally secure and uses a hash function that satisfies the above properties. Most importantly, for the chosen hash function there must be a sufficiently low probability that two different inputs will map to the same output. For example if Alice wants to send a signed bit in the future she can choose two random inputs k_0, k_1 and apply the suitable hash function f. The public key is $\{(0, f(k_0)), (1, f(k_1)\}$. Assuming the hash function has been correctly chosen to be one-way, it is impossible for a forger to identify k_0 or k_1 given the public key. If Alice wants to send a signed message b, she will send (b, k_b), and the recipient will apply f to k_b, accepting the message only if $f(k_b)$ matches the previously distributed public key. After the message, k_b is known so the public key has to be discarded, making this a one-time signature scheme. Merkle [149] extended the one-time signature scheme so it can be reused, however it can still only be used a limited number of times before it loses its security. Due to this inefficiency, hash functions have mostly been ignored in favour of ECDSA-based digital signature schemes. However hash based signature schemes are gaining popularity since a quantum algorithm has not yet been found to break them [8].

5.2.2 Quantum one-way function

All currently used classical digital signature schemes rely on computational security [8] and could therefore be broken by a quantum computer given enough time. However in quantum mechanics there are provably secure one-way functions, so signature schemes

based on such quantum one-way functions can have information-theoretic security and remain secure, even against attacks from quantum computers.

Gottesman and Chuang [92] proposed a signature scheme based on a quantum analogue of the Lamport-Diffie one-time signature scheme described in the previous section. This scheme makes use of a quantum one-way function f that converts classical information k into a quantum state $|\psi_k\rangle$. The $|\psi_k\rangle$ for different values of k must be non-orthogonal to each other for this to be a secure one-way function. The classical information k fully describes the quantum state $|\psi_k\rangle$, and it is easy to prepare $|\psi_k\rangle$ given k. However due to Holevo's theorem [110], it is impossible to determine the exact state of $|\psi_k\rangle$, and therefore k, given a copy of the quantum state $|\psi_k\rangle$. Therefore $f(k) = |\psi_k\rangle$ provides a one-way function that is provably secure due to the laws of quantum mechanics. The basis of the security against forgery comes from the fact that the possible $|\psi_k\rangle$ come from a non-orthogonal set. This makes it impossible to identify which state $|\psi_k\rangle$ was prepared without prior knowledge of k. By making the signature a long string of such states it can be made arbitrarily unlikely that a forger has sufficient knowledge about $\{k\}$ to successfully forge.

A signature scheme based on a quantum one-way function is therefore possible and most QDS schemes are based on this idea. They only differ in what states $|\psi_k\rangle$ they use, how they secure against repudiation, and how they verify the signature. In the next section I describe how QDS schemes have developed to where they are today. So far most work has focussed on QDS schemes that assume authenticated quantum channels between participants, however recently steps have been taken to loosen this assumption [9], and this is described in Section 6.1.1.

5.2.3 Quantum digital signature schemes

In this section I describe the most important developments in QDS in the last fifteen years. I leave a more complete description of a QDS protocol and security analysis for Section 5.3, here focussing on the differences between different schemes.

Original idea

In 2001, Gottesman and Chuang [92] introduced the idea of quantum digital signatures based on a one-way function that converts classical information into quantum states. The exact quantum states used to make up the signature are not overly important; as long as the chosen states are non-orthogonal, the signature will be secure against forgery. This is because Holevo's theorem [110] limits the amount of information an eavesdropper can gain about an n-qubit state, $|\psi_n\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$, to Tn bits, where T is the number of copies of $|\psi_n\rangle$ available. As long as the total amount of information needed to fully describe the state $L \gg Tn$, the scheme will be secure against forgery for a sufficiently long string of n-qubit states.

To secure against repudiation and transferability, Gottesman and Chuang use a SWAP test [30] to ensure that Bob and Charlie are given the same quantum states by Alice. A SWAP test is a way to compare two quantum states $|f_k\rangle$ and $|f_{k'}\rangle$ to test if they are the same. The states $|f_k\rangle$ are $|f_{k'}\rangle$ are prepared along with a single ancilla qubit in the state $(|0\rangle + |1\rangle)/\sqrt{2}$. These states are passed through a Fredkin gate that performs a controlled

swap on the states, where the ancilla is the control. This causes the transformation

$$\frac{1}{\sqrt{2}}|f_k\rangle|f_{k'}\rangle(|0\rangle + |1\rangle) \rightarrow \frac{1}{\sqrt{2}}\left(|f_k\rangle|f_{k'}\rangle|0\rangle + |f_{k'}\rangle|f_k\rangle|1\rangle\right). \tag{5.1}$$

The ancilla mode is then passed through a Hadamard gate. This transforms the state to

$$\frac{1}{2}\left((|f_k\rangle|f_{k'}\rangle + |f_{k'}\rangle|f_k\rangle)|0\rangle + (|f_k\rangle|f_{k'}\rangle - |f_{k'}\rangle|f_k\rangle)|1\rangle\right). \tag{5.2}$$

Clearly, if the two states are the same a measurement on the ancilla mode will never give the state $|1\rangle$, so a measurement of $|0\rangle$ is considered to pass the SWAP test. Given realistic imperfections, the SWAP test will fail sometimes even if the states are the same, so in reality some limit is set on the number of failures that can occur before the SWAP test is failed.

Bob and Charlie use this SWAP test to guard against repudiation in the following way. Alice distributes two copies of each public key to Bob and Charlie. Bob and Charlie each perform a SWAP test on their two keys to ensure that they are the same. If they both succeed, one of them (say Charlie) passes one of his keys to the other (Bob), who performs a SWAP on the received state and one of his copies. If the SWAP test passes Bob and Charlie know they have the same states. The crucial point is that Bob and Charlie's shared state is symmetric from the point of view of Alice, so there is nothing she can do to make it more likely for one to fail than the other. If the second recipient uses a looser criterion to accept the signature than the first recipient, this guards against repudiation by Alice, and guarantees transferability.

In the messaging stage, Alice sends the classical information about the public key along with a message to Bob. Bob uses this information to prepare the quantum state described by the classical information. To authenticate the message Bob uses a SWAP test to ensure it is the same as the original public key. If the number of discrepencies is below some threshold he accepts the message and forwards to Charlie, who uses a SWAP test to check the signature. This method has the obvious drawback that it requires a long-term quantum memory, especially since there will often be a long time between distributing the public key and signing the message. However it provides a template for a QDS scheme that future protocols have followed with only minor adjustments.

Quantum digital signatures with linear optics

Apart from the problem of quantum memory, the above signature scheme is complicated by the difficulty to implement the SWAP test. This was improved upon by Andersson *et al.* [10] who described a QDS protocol involving linear optics and coherent states. Rather than qubits, the public key is made up of phase-encoded coherent states, and the private key is the phases of the individual coherent states. Security against forgery follows from the fact that the coherent states are non-orthogonal so a forger can never perfectly identify the phases of the coherent states.

Verification of the signature is achieved by determining whether two coherent states are different from each other. In the messaging stage, Alice distributes her private key containing the phases of the coherent states in the public key. The recipient Bob can easily prepare the appropriate coherent states $|\beta\rangle$ and compare with the states $|\alpha\rangle$ he received during the distribution of the public key. This is done by passing the two states through

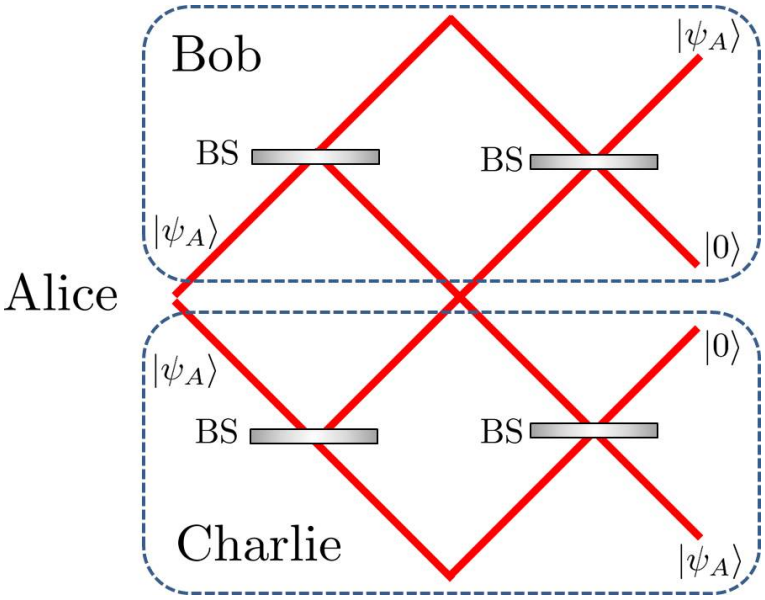


Figure 5.1: A multiport used to symmetrise the states received by Bob and Charlie. BS: balanced beamsplitter. Bob (Charlie) splits the state they received from Alice on a balanced beamsplitter, keeping one of the outputs and sending the other to Charlie (Bob). Bob (Charlie) compares the half he kept with the half he received from Charlie (Bob) to compare that they are the same.

a balanced beamsplitter, after which the outputs of the beamsplitter will be $|(\alpha+\beta)/\sqrt{2}\rangle$ and $|(\alpha-\beta)/\sqrt{2}\rangle$. Therefore if the states are the same there will be no photons present in the "dark" port, so any clicks in that output indicate that the states were not the same. As long as the number of mismatches is lower than a certain threshold, the signature is accepted.

Security against repudiation is again provided by symmetrising the states held by Bob and Charlie. Rather than a SWAP test, this is done using a multiport shown in Fig. 5.1. No matter what states Alice sends to Bob and Charlie, the output ports labelled $|\psi_A\rangle$ will have the same output. If Alice sends the same states (as in the figure), the other ports will be "dark" so any photons detected there indicate that the states were not the same or there has been some attack on the multiport. This guarantees that the state held by Bob and Charlie is symmetric from Alice's point of view so there is nothing she can do to make repudiation likely.

A proof-of-principle experiment was implemented to demonstrate this idea by Clarke *et al.* [45]. As signature states they used phase-encoded coherent states, and secured against repudiation using a multiport. The phase-encoded coherent states were chosen from a variety of sets, ranging from 2 to 32 possible phases. They got around the requirement for quantum memory by sending the state produced by the private key at the same time as the public key. However in a realistic signature protocol, there can often be weeks or even longer between distribution of a public key and signing of a message. It is clearly infeasible with current technology to achieve memories of this length, so a QDS protocol that doesn't require quantum memory is needed for a practical signature scheme.

Quantum digital signatures without quantum memory

Dunjko *et al.* [61] proposed a method that allows quantum digital signatures to be achieved without the need for quantum memory. Instead of storing the states making up the

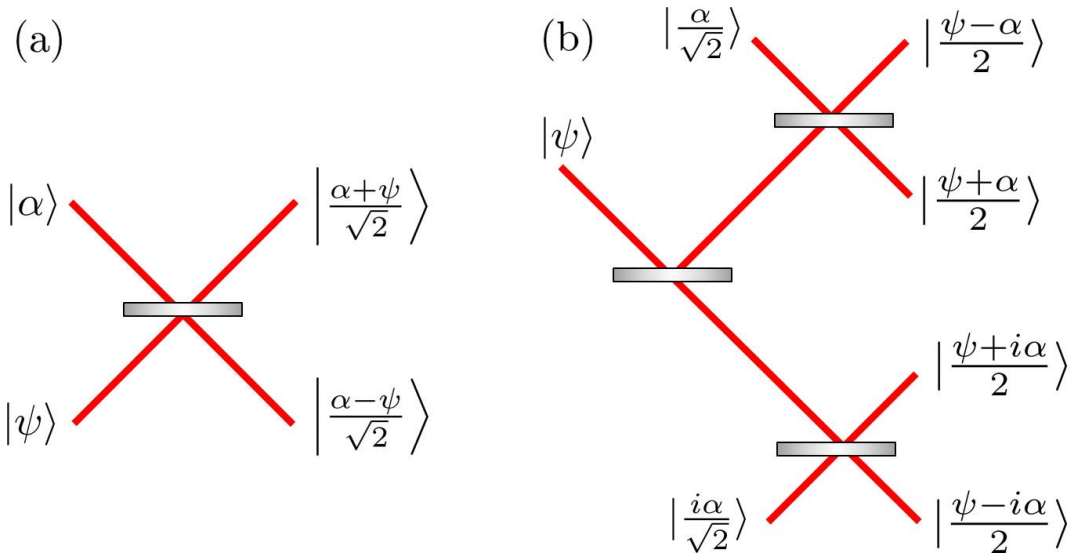


Figure 5.2: (a) Unambiguous state discrimination. The state $|\psi\rangle$ received from Alice is mixed on a balanced beamsplitter with the coherent state $|\alpha\rangle$. If a photon is detected in the upper arm, it is concluded that $|\psi\rangle$ is not $|\text{-}\alpha\rangle$, and if a photon is detected in the lower arm the state $|\psi\rangle$ is not $|\alpha\rangle$. (b) Unambiguous state elimination. The state $|\psi\rangle$ received from Alice is split on a balanced beamsplitter. One output is mixed on another balanced beamsplitter with $|\alpha\rangle$, and the other output is mixed on another balanced beamsplitter with $|i\alpha\rangle$. For each of the outputs at which a photon is detected, one of the states is eliminated.

public key, they suggested immediately measuring the states on receipt. In the messaging stage the measurement results are compared with the signature to determine whether the message is genuine. This works because a forger will inevitably have errors when he tries to forge a signature, so the measurement results will be better correlated with Alice's signature than it could ever be with a forger's. Security against repudiation is again achieved using a multiport.

The protocol involves two identical strings of coherent states, where each element is randomly chosen by Alice to be either $|\alpha\rangle$ or $|-\alpha\rangle$. They are sent through a multiport to Bob and Charlie who immediately measure the received states using unambiguous state discrimination (USD) [122, 57, 165]. In this case USD is performed as in Fig. 5.2 (a) [16] by mixing the received states $|\psi\rangle$ on a balanced beamsplitter with the state $|\alpha\rangle$. Using this method some elements of the public key can be determined perfectly. This comes at the cost of gaining no information about other elements. The elements for which a result is known are used to check the authenticity of a later received signature.

Collins *et al.* [48] implemented an experiment demonstrating a QDS scheme without quantum memory based on the above protocol. They used as the signature states the set $\{|\alpha\rangle, |\text{-}\alpha\rangle, |i\alpha\rangle, |\text{-}i\alpha\rangle\}$, and as a measurement procedure unambiguous state elimination (USE) [18, 17] rather than USD. A procedure for USE is shown in Fig. 5.2 (b) and works in much the same way as USD but not all incorrect states have to be eliminated to get a result. Every photon detection event allows one state to be eliminated, and this infromation can be used to check the signature. Using this method they were able to demonstrate a signature scheme that works without quantum memory, but the required signature length was about $L = 10^{14}$ to sign a single bit with a security level of 0.01%. Although this length is impractical, this experiment demonstrates that quantum signatures are realisable with current technology.

Quantum digital signatures without a multiport

In the protocol described above, one of the biggest sources of loss was the multiport used to symmetrise the state. These losses become particularly pronounced as the distance between the two recipients increases. Wallden *et al.* [215] have proposed a QDS procedure that removes the requirement for a multiport. They show that rather than symmetrising the quantum state between Bob and Charlie, it is sufficient to symmetrise the measurement results. Bob and Charlie achieve this by randomly forwarding half of their measurement results to the other party, secretly from Alice. This could be achieved, for example, using a standard QKD link. In this way, the measurement results they use to check the signature are symmetric from Alice's point of view so she cannot cause repudiation. They demonstrate this using BB84 states [20], however the same principle holds for phase-encoded coherent states.

Donaldson *et al.* [59] performed an experiment similar to the one in [48], but with the symmetrisation procedure carried out by swapping measurement results rather than using a multiport. Using this and some other improvements, the signature length required to sign a one-bit message at a security level of 0.01% is $L \approx 4 \times 10^9$. This length is much more practical and means that a one-bit message could be signed in about 40 seconds, however there is still a lot of progress to be made before quantum digital signatures can compete with their classical counterparts.

In [215], it was also shown that a QDS protocol can be realised using classical secret keys distributed over a QKD link. However this is unlikely to be the most efficient way to produce quantum signatures, because a QDS scheme is similar to a QKD scheme but without the requirement to perform reconciliation and privacy amplification. One effect of this is that QDS schemes can be implemented at loss levels where QKD can no longer be performed [9].

5.3 Quantum digital signatures with homodyne measurement

In previous quantum signature schemes, recipients use unambiguous quantum measurements, such as unambiguous state discrimination [61] or unambiguous state elimination [48], to obtain information about the distributed quantum state sequences. The measurement records are later, in the messaging stage, checked against the signature received with the message. In the ideal case, the unambiguous nature of the measurements means that any mismatches can be attributed to a malicious party, and the signature can be rejected. More realistically, however, there are always some errors, which means that messages will be accepted if the number of mismatches lies below some threshold. A disadvantage of unambiguous measurements is that a lot of the time they produce no result. Therefore, using some other type of measurement, which more often produces a result, could be advantageous. The increased detection rate, however, comes at the cost of an increased error rate. It is therefore of interest to investigate whether or not this leads to a more efficient scheme in practice.

In this section, I describe a quantum signature scheme that uses continuous variable (CV) quantum homodyne detection instead of single photon detectors. Similar to before, the measurement is performed as soon as the state is received, meaning no quantum memory is necessary, and the measurement results are used to eliminate some of the possible

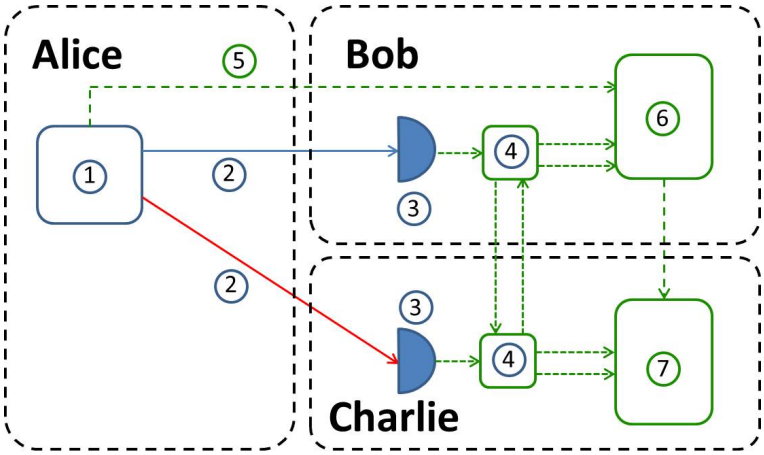


Figure 5.3: Depiction of the scheme. The numbered parts relate to the corresponding stages in the main text. Green dashed lines indicate classical communication. Red/blue lines indicate communication with quantum states.

states sent. In contrast to previous schemes, the continuous nature of homodyne detection makes it impossible to eliminate any state with certainty. Instead, it can only be said that it is less likely to be one state than another. For this reason, this measurement technique is called "ambiguous state elimination". Even with this ambiguity it is possible to perform a quantum signature scheme, because a forger will always have more mismatches with the measurement results than the author of the signature. Security against repudiation is guaranteed by swapping measurement results in the same way as in [215].

5.3.1 Description of the protocol

The protocol for quantum digital signatures using homodyne measurement is described below and represented in Fig. 5.3, and follows the template of the QDS protocol in [215]

Distribution stage: 1-4

1. For each possible future one-bit message $k = 0, 1$, Alice generates two identical copies of sequences of phase-encoded coherent states, $QuantSig_k = \otimes_{l=1}^{L} |\psi_l^k\rangle\langle\psi_l^k|$, where $|\psi_l^k\rangle$ is a randomly chosen phase-encoded coherent state, $|\psi_l^k\rangle = |\alpha e^{i\phi_l^k}\rangle$, $\phi_l^k \in \{0, \pi/2, \pi, 3\pi/2\}$, and L is a suitably chosen integer. The state $QuantSig_k$ is called the quantum signature, and the sequence of phases $PrivKey_k = (\phi_1^k, ...\phi_L^k)$ is called the private key.

2. Alice sends one copy of $QuantSig_k$ to Bob and one to Charlie, for each possible message $k = 0$ and $k = 1$.

3. Bob (Charlie) measures the states received from Alice by performing homodyne detection [137] in both the $\hat{x}$- and $\hat{p}$-quadrature. He records the result of the measurement and the associated position in the sequence l. For each quadrature, the sign of the measured result determines which state is eliminated. For example if a positive result is measured, then the state $|-\alpha\rangle$ or $|-i\alpha\rangle$ is eliminated, depending on the measured quadrature. In this way, Bob (Charlie) eliminates two states, one in each quadrature, for each signature element. The sequences of eliminated states will be used to verify a later message and is called the eliminated signature.

4. Symmetrisation: Bob (Charlie), for each element l of $QuantSig_k$, randomly chooses

with equal probability to either forward the measurement results and position to Charlie (Bob) or not, secret from Alice, who should not learn the positions of the forwarded results. The resulting sequences of measurement outcomes, after the forwarding procedure, form Bob's and Charlie's "eliminated signatures". Bob (Charlie) keeps the results obtained directly from Alice, and the results forwarded to him by Charlie (Bob) separate. Therefore, he has an eliminated signature in two parts, each of length $L/2$.

The homodyne measurement will, even in the ideal case, eliminate the sent state some of the time. If everybody follows the protocol, the probability that this happens depends on the overlap of the coherent states and thus on their amplitude, and is $p_{err} = \frac{1}{2}\mathrm{erfc}\left(\alpha/\sqrt{2}\right)$ in the ideal case with no loss or experimental imperfections, where $\mathrm{erfc}(x)$ is the complementary error function. For $\alpha = 0$, this probability equals one half, and as α increases, it quickly drops towards zero. Due to these fundamentally unavoidable errors, this measurement protocol is an example of "ambiguous state elimination". Since measurements are performed immediately on receipt of the states, no quantum memory is required, just as in [48, 61].

Messaging stage: 5-7

5. To send a signed one-bit message m, Alice sends $(m, PrivKey_m)$ to Bob.

6. Bob checks whether $(m, PrivKey_m)$ matches both parts of his stored eliminated signature by counting how many elements of Alice's private key were eliminated during the distribution stage. If there are fewer than $s_a L/2$ mismatches in each of the two parts of his eliminated signature, where s_a is the authentication threshold, Bob accepts the message and forwards it to Charlie.

7. Charlie tests for mismatches in the same way as Bob, but with a higher verification threshold s_v, to protect against repudiation. Charlie accepts the message if there are fewer than $s_v L/2$ mismatches in each of the two parts of his eliminated signature, with $p_{err} < s_a < s_v < \frac{1}{2}$.

Essentially, the security of this protocol comes from two main effects. First, it is impossible for a forger to perfectly determine the signature states since they come from a non-orthogonal set. Therefore the distributor Alice always has an advantage over any other party. Second, the forwarding of measurement results ensures that, from Alice's perspective, Bob's and Charlie's measurement records follow the same statistics. This means that if Charlie uses a higher verification threshold s_v than Bob's authentication threshold s_a, then Alice's probability to repudiate can be made arbitrarily small by choosing the signature length L large enough. A detailed security analysis for individual forging attacks and repudiation is found in the following section.

Note that it is important for Bob and Charlie to keep the two halves of their measurement results separate. If Bob tries to forge a message to Charlie, he can ensure that, for the measurement results he forwarded to Charlie, there are no errors between the forged signature and Charlie's measurement results. At some level of loss, the number of mismatches in a forged signature of length $L/2$ is less than for a genuine signature of length L, so the signature scheme would be insecure beyond that loss level. This is guarded against by testing each part of the signature separately, and the signature is only accepted if both halves pass the test. Essentially, the results Charlie received directly from Alice guard against forgery by Bob, and the measurement results he received from Bob guard against repudiation.

5.3.2 Security analysis

A quantum digital signature scheme must be secure against both repudiation and forgery. The scheme is secure if the probability that the signature can be repudiated or forged decays exponentially with the length of the key. In addition, the scheme should be robust, which means that if all parties behave as they should, the protocol runs as intended with high probability. The analysis below follows the same methods as in [59].

Security against repudiation: For successful repudiation, Charlie must reject a message that Bob has already accepted. Due to the random swapping of measurement results between Bob and Charlie, the measurement statistics they share are symmetric, which provides security against repudiation. No matter what cheating strategy Alice adopts, including strategies involving entangled states, Bob and Charlie will have the same probability p to observe a mismatch in the messaging stage. Alice has control over p, but cannot cause a difference between Bob's and Charlie's measurement statistics.

To achieve successful repudiation, Alice can manipulate the states sent to Bob and Charlie to try to cause a disagreement between them. Alice has full control over the probability of a mismatch between the private key and Bob's and Charlie's eliminated signatures. The probability of a mismatch is called p_B for states first sent to Bob, and p_C for states first sent to Charlie.

For successful repudiation, Bob must accept the message for both length $L/2$ parts of his signature and Charlie has to reject the message in at least one part of his signature. Since $P(A \cap B) \leq \min\{P(A), P(B)\}$ and $P(A \cup B) \leq P(A) + P(B)$, we can write

$$p_{rep} = P((A \cap B) \cap (C \cup D)) \leq \min\{\min\{P(A), P(B)\}, P(C) + P(D)\}, \tag{5.3}$$

where $P(A)$ ($P(B)$) is the probability that Bob will accept the message using the $L/2$ states received from Alice (Charlie), and $P(C)$ ($P(D)$) is the probability that Charlie will reject the message due to the $L/2$ states received from Bob (Alice).

Using Hoeffding's inequalities [107], which bound the probability that the empirical mean of L independent random variables deviates from their expected mean, the probabilities, $P(A)$ and $P(B)$, that Bob will accept the message, for the length $L/2$ parts of his eliminated signature received from Alice and Charlie respectively, are

$$P(A) \leq \exp[-(p_B - s_a)^2 L], \quad P(B) \leq \exp[-(p_C - s_a)^2 L], \tag{5.4}$$

where s_a is the authentication threshold. Similarly, the probabilities $P(C)$ and $P(D)$ that Charlie will reject the message for the length $L/2$ parts of his eliminated signature received from Bob and Alice respectively are

$$P(C) \leq \exp[-(s_v - p_B)^2 L], \quad P(D) \leq \exp[-(s_v - p_C)^2 L], \tag{5.5}$$

where s_v is the verification threshold and $s_v > s_a$.

Now we can take $p = \max\{p_B, p_C\}$. In that case $\exp[-(p - s_a)^2 L] = \min\{P(A), P(B)\}$. In addition, $2\exp[-(s_v - p)^2 L] \geq P(C) + P(D)$. Combining these two equations with Eq. (5.3), we get

$$p_{rep} \leq \min\{2\exp[-(p - s_a)^2 L], 2\exp[-(s_v - p)^2 L]\}, \tag{5.6}$$

where the first term in the minima has been doubled for simplicity, noting that this slightly

loosens the tightness of the bound on the repudiation probability.

Alice's optimal choice of p is the one that maximises the smaller of these two terms, that is, $p = \frac{s_a + s_v}{2}$. With this choice, her repudiation probability is bounded as

$$p_{rep} \leq 2 \exp\left[-\frac{(s_v - s_a)^2}{4} L\right]. \tag{5.7}$$

This decays exponentially with the length of the signature and thus the scheme is secure against repudiation.

Security against forging: Since $s_v > s_a$, it is easier to forge a message that is claimed to be forwarded, than one that is claimed to come directly from Alice. Bounding the probability for the former also bounds the probability for the latter. Therefore, we will consider the case where Bob attempts to forge a message that he is forwarding to Charlie, claiming he received it from Alice. Since the protocol is symmetric with respect to the two recipients Bob and Charlie, this also bounds Charlie's probability to forge messages.

To successfully forge, Bob must ensure that he doesn't, in the messaging stage, declare any of the states that Charlie has eliminated, with fewer than $s_v L/2$ errors in each length $L/2$ part of Charlie's eliminated signature. Since Bob can control what he forwards to Charlie in the distribution stage, Bob can completely control the number of mismatches for these positions. If he so wishes, he can cause no mismatches in those positions. Therefore it is the measurement results which Charlie did not forward to Bob that Bob has to try to guess. The measurement results Charlie received through Bob are used to protect against repudiation, whereas the measurement results Charlie obtained for states directly received from Alice are used to test for forgery by Bob, and vice versa.

Assuming that Bob cannot interfere with the quantum states which Alice sends to Charlie, Bob's best forging strategy will involve measurements on the copies of these states that Bob legitimately received from Alice. Based on this, Bob will make a best guess when later declaring to Charlie what these states supposedly were. The optimal measurement Bob should make to forge is limited only by what is possible in quantum mechanics, not by any considerations of what measurements are practical to realise, and is not the same measurement as he would make if honestly following the protocol.

The fact that the possible states Alice can send are non-orthogonal provides the basis of the security of the scheme. As in [48], the optimal individual measurement Bob can perform is a minimum-cost measurement, minimising Bob's "cost" associated with mismatches. Since the states sent by Alice are uncorrelated with each other, collective forging strategies, where measurements on successive signature states can depend on the results obtained in previous measurements, provide no advantage over individual forging strategies, where Bob simply repeats the same optimal measurement for each signature state [48]. The most general type of forging attack are coherent forging attacks, where Bob can measure any number of signature states in an entangled basis. While intuitively the protocol should remain secure also against coherent forging, this analysis is not in general straightforward. Proof of security against coherent forging attacks is therefore left for future work, noting that it has been shown that for BB84 signature states, coherent attacks provide no advantage [214].

To prove security against individual and collective forging, we need to bound Bob's minimum cost for a measurement on an individual signature state, which in this case is

identical to Bob's probability to cause a mismatch for a single signature element. This is done following the method in the supplemental material of [59], resulting in a lower bound on the minimum cost C_{min}, depending on the cost matrix, which can be determined either theoretically or from experimental data, and p_{min}, which is the minimum probability for a forger to incorrectly identify a state received from Alice. p_{min} depends on the overlap of the signature states and is calculated from the eigenvalues of their Gram matrix. For the states considered here, the minimum probability is [48]

$$p_{min} = 1 - \frac{1}{16}|\sum_{i=1}^{4}\sqrt{\lambda_i}|^2, \tag{5.8}$$

where $\lambda_{1,2} = 2\exp(-\alpha^2)[\cosh(\alpha^2) \pm \cos(\alpha^2)]$ and $\lambda_{3,4} = 2\exp(-\alpha^2)[\sinh(\alpha^2) \pm \sin(\alpha)^2]$ are the eigenvalues of the approptiate Gram matrix. Here, we are assuming that the forger Bob has access to the states Alice sends before any losses or imperfections have acted on them. This is not true for an honest Charlie, whose measurements on the states is subject to loss and imperfections.

To find the minimum cost for a forger, the cost matrix is required. In a cost matrix, the rows correspond to the state sent by Alice, and the columns correspond to the states eliminated. The entries of the matrix are the probabilities that a state is eliminated for a given signal state. The cost matrix in the ideal theoretical case where the signature states are sent through a lossy channel with transmission T is

$$C = \begin{pmatrix} p_{err} & 1/2 & 1-p_{err} & 1/2 \\ 1/2 & p_{err} & 1/2 & 1-p_{err} \\ 1-p_{err} & 1/2 & p_{err} & 1/2 \\ 1/2 & 1-p_{err} & 1/2 & p_{err} \end{pmatrix}, \tag{5.9}$$

where $p_{err} = \frac{1}{2}\text{erfc}\left(\sqrt{\frac{T}{2}}\alpha\right)$, and the rows and columns follow the ordering $|\alpha\rangle, |i\alpha\rangle, |-\alpha\rangle, |-i\alpha\rangle$. Each of the rows adds up to 2 because two states are eliminated every time a state is sent. A detailed calculation for the minimum cost of an experimental cost matrix is shown in Section 5.3.3. Essentially, the minimum cost is the probability that a forger will make an error p_{min}, multiplied by the minimum cost of an error, added to the probability that the correct state will be eliminated in the absence of a forger p_{err}. The cost of a declaration is the difference between the probability that the declared state is eliminated and the probability that the sent state is eliminated. Combining all this with the cost matrix in Eq. (5.9), the minimum cost is found to be

$$C_{min} = p_{err} + p_{min}\left(\frac{1}{2} - p_{err}\right). \tag{5.10}$$

The probability of a successful forgery is the probability that Charlie measures fewer than $s_v L/2$ errors in the results for the $L/2$ states received directly from Alice during forgery by Bob. Using Hoeffding's inequalities [107], the probability of a successful forgery is therefore

$$p_{forg} \leq \exp\left[-(C_{min} - s_v)^2 L\right]. \tag{5.11}$$

This probability decays exponentially with respect to signature length as long as $C_{min} > s_v$.

Robustness: A QDS scheme is only useful if it only fails with small probability. If all parties are honest, then Bob should accept the message as being genuine, except with small probability. The message is rejected if Bob detects more than $s_a L/2$ errors in either of the length $L/2$ parts of his eliminated signature, which using Hoeffding's inequalities occurs with probability

$$p_{fail} \leq 2\exp\left[-(s_a - p_{err})^2 L\right], \tag{5.12}$$

where p_{err} is the probability that an honest recipient, following the protocol, will eliminate the state actually sent by Alice. If, as is normally the case, p_{err} for the states sent to Charlie is different to that for those sent to Bob, then p_{err} should be taken as the maximum of those probabilities. Since Charlie's rejection threshold is less strict than Bob's, Charlie's rejection probability is much smaller than Bob's. For the protocol to be robust, we thus have to choose $s_v > s_a > p_{err}$.

Taking everything together, the protocol can be made secure and robust as long as an honest Charlie is able to distinguish a "fake" declaration by Bob from a declaration made by Alice, in terms of the average number of mismatches Charlie sees. This occurs when Bob's optimum probability to cause a mismatch, C_{min}, is greater than the probability p_{err} that Alice's true declaration will cause a mismatch. As long as $C_{min} > p_{err}$, the thresholds s_v, s_a and the signature length L can be chosen so that the scheme is as secure as desired against forging and repudiation for all displacement amplitudes.

If it is assumed that all parties are equally likely to be dishonest, then the level of security can be defined by setting the terms in the exponentials of Eqs. (5.7), (5.11) and (5.12) to be equal to each other. This is achieved when $s_a = p_{err} + (C_{min} - p_{err})/4$, and $s_v = p_{err} + 3(C_{min} - p_{err})/4$. Note that Bob and Charlie can each determine s_a and s_v only using their own experimental data. This gives an upper bound for the total probability for the scheme to fail in any one of these ways of

$$P(\text{failure}) \leq 2\exp\left(-\frac{g^2}{16}L\right), \tag{5.13}$$

where $g = C_{min} - p_{err}$ can be determined from experimental results. The figure of merit used to characterise the quality of a QDS scheme is the length $2L$ required to sign a one-bit message for a particular security level. In this thesis, to facilitate comparison with earlier realisations [48, 59], the security level chosen is that the probability of failure is $\leq 0.01\%$.

5.3.3 Experimental implementation

To show that the protocol is feasible with current technology, an experiment was carried out over a real free-space urban link [168, 102]. The experiment was performed using Stokes operators with a bright excitation in the $\hat{S}_3$ direction. Stokes operators were used because polarisation is maintained over a free-space channel and the $\hat{S}_3$ excitation provides an in-built local oscillator, which aids with homodyne detection. The signal states $|\pm\alpha\rangle$, $|\pm i\alpha\rangle$ were prepared using electro-optical modulators to displace the states in the "dark" ($\hat{S}_1$-$\hat{S}_2$) plane, then repeatedly transmitted through a free-space channel between the buildings of the Max Planck Institute and the University of Erlangen-Nürnberg [168, 102, 132]. The length of the channel was approximately 1.6 km. During the measurements the channel transmission fluctuated between 50 % and 85 % due to scintillation. At the receiver the signal was split on a balanced beam splitter to measure both the $\hat{S}_1$ and $\hat{S}_2$ operators. Simultaneously, the transmission was recorded for each state. The experiment was imple-

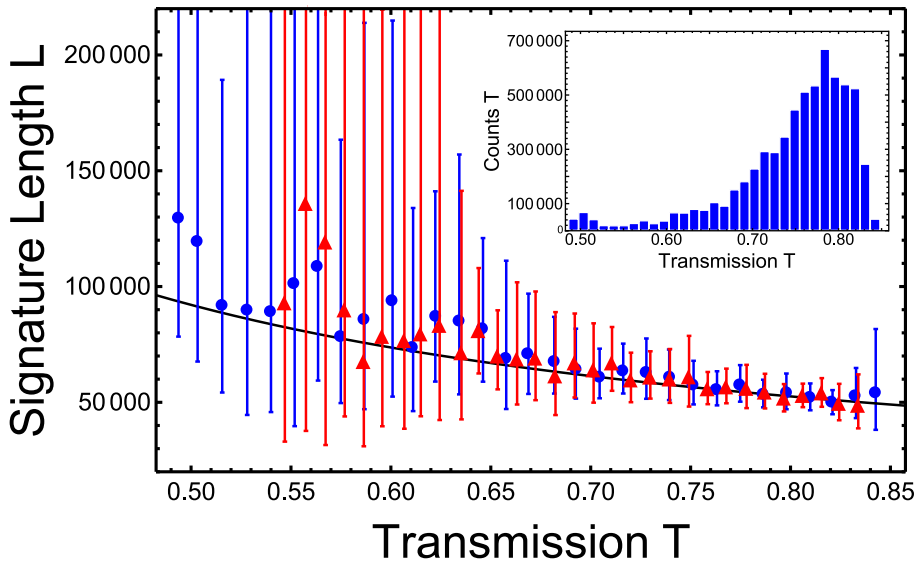


Figure 5.4: Signature length for $\alpha = 0.48$. Black curve: theoretical model. Blue dots/bars: results from the data attributed to Bob. Red triangles/bars: results from the data attributed to Charlie. The error bars calculated are statistical. The errors naturally increase with decreasing transmission since g from Eq. (5.13) decreases. In addition, less data was available at lower transmission values, as can be seen in the inset histogram, resulting in significantly larger errors. The data used for each point comes from a small range of transmissions, but horizontal error bars are omitted for clarity.

mented for three different signal amplitudes, $\alpha = 0.48$, $\alpha = 0.93$, and $\alpha = 1.63$, and the first (second) half of the measurement time is attributed to Bob (Charlie). To take into account the varying transmission, Bob's (Charlie's) measurement data was sorted into 32 subchannels according to the measured transmission [168, 102]. Depending on the sign of the quadrature measurement values, for each signal state, two of the possible sent states were eliminated.

For each set of data, the sequence of eliminated states was used to produce a cost matrix [214] that gives the probability that each state was eliminated for a particular signal state. For each cost matrix, the minimum difference between an off-diagonal element of the cost matrix (probability of eliminating a "wrong" state) and the diagonal element of that row (probability of eliminating the sent state) was calculated. This difference was multiplied by the appropriate p_{min} to obtain the parameter g from (5.13) for that cost matrix. The minimum probability that a forger will incorrectly identify the state is p_{min} from (5.8). For each g, the signature length $2L$ to sign a one-bit message with a failure probability of 0.01% was calculated. In Fig. 5.4, the length L is plotted against transmission T with $T+R=1$ for $\alpha = 0.48$.

An example of the measured cost matrix is shown with errors below. This matrix is Bob's data for $\alpha = 0.48$ at a transmission level of $T = 0.600$ ($T+R=1$) and is given by

$$C = \begin{pmatrix} 0.3767 & 0.5028 & 0.6233 & 0.4972 \\ 0.4929 & 0.3682 & 0.5071 & 0.6318 \\ 0.5979 & 0.496 & 0.4021 & 0.504 \\ 0.4957 & 0.6204 & 0.5043 & 0.3796 \end{pmatrix} \pm \begin{pmatrix} 0.015 & 0.019 & 0.015 & 0.019 \\ 0.008 & 0.013 & 0.008 & 0.013 \\ 0.013 & 0.019 & 0.013 & 0.019 \\ 0.014 & 0.020 & 0.014 & 0.020 \end{pmatrix}. \quad (5.14)$$

The above cost matrix can be used to bound the minimum cost of a minimum-cost mea-

surement performed by a forger, by following the method in the supplemental material of [48].

To find an analytical bound on the minimum cost, the cost matrix in Eq. (5.14) is manipulated to the form of an error-type cost matrix. This is done because the minimum cost of an error-type cost matrix is proportional to p_{min}, the minimum probability to incorrectly identify the state, with the proportionality given by the off-diagonal elements of the cost matrix. An error-type cost matrix has zeros on the diagonals of the cost matrix, and all the off-diagonal terms are equal. It is called error-type because a correct declaration has zero cost, and an incorrect declaration always has the same cost.

To get to this form, two properties of cost matrices are used. First, subtracting a constant row matrix from a cost matrix reduces the cost by a constant, while leaving the minimum-cost measurement unchanged. Second, the cost of a cost matrix $C_{i,j}$ is lower bound by the cost of a cost matrix $C^l_{i,j}$ that is strictly smaller than it $C^l_{i,j} \leq C_{i,j}$.

I define $C^h_{i,j} = C_{i,i}$, a constant row matrix for which the elements in each row are equal to the diagonal elements of the matrix $C_{i,j}$. I then define $C'_{i,j} = C_{i,j} - C^h_{i,j}$, which has the same minimum-cost measurement as $C_{i,j}$, but with the minimum cost reduced by $C^h = 1/4 \sum_i C_{i,i}$. Finally I define the cost matrix $C^l_{i,j}$ that is strictly smaller than $C'_{i,j}$ for all i, j such that $C^l_{i,j} = \min_{i \neq j} C'_{i,j}$ for all $i \neq j$, and with zeros on the diagonal. This final cost matrix $C^l_{i,j}$ is of error-type, for which the minimum cost C^l_{min} is proportional to the minimum error probability p_{min}. Using this argument the minimum cost of the cost matrix (5.14) can be lower bound as

$$C_{min} \geq C^h + C^l_{min}. \tag{5.15}$$

Starting from (5.14), the subsequent cost matrices are

$$C^h = \begin{pmatrix} 0.3767 & 0.3767 & 0.3767 & 0.3767 \\ 0.3682 & 0.3682 & 0.3682 & 0.3682 \\ 0.4021 & 0.4021 & 0.4021 & 0.4021 \\ 0.3796 & 0.3796 & 0.3796 & 0.3796 \end{pmatrix}, \tag{5.16}$$

$$C' = \begin{pmatrix} 0 & 0.1261 & 0.2466 & 0.1205 \\ 0.1247 & 0 & 0.1389 & 0.2636 \\ 0.1958 & 0.0939 & 0 & 0.1019 \\ 0.1161 & 0.2408 & 0.1247 & 0 \end{pmatrix}, \tag{5.17}$$

$$C^l = \begin{pmatrix} 0 & 0.0939 & 0.0939 & 0.0939 \\ 0.0939 & 0 & 0.0939 & 0.0939 \\ 0.0939 & 0.0939 & 0 & 0.0939 \\ 0.0939 & 0.0939 & 0.0939 & 0 \end{pmatrix}. \tag{5.18}$$

From (5.16), $C^h = 0.3817$. This is the cost for an honest scenario; it is the probability that Charlie will eliminate a state that Alice sent if all parties are honest. From (5.18), the minimum difference between the probability of eliminating the sent state, and the probability of eliminating another state is 0.0939. This difference therefore gives the advantage of declaring the sent state at the messaging stage. The minimum cost for matrix (5.18) is the product of that advantage and the minimum probability to incorrectly identify a state p_{min}. For this state $\alpha = 0.48$, so from Eq. (5.8), $p_{min} = 0.4373$. The

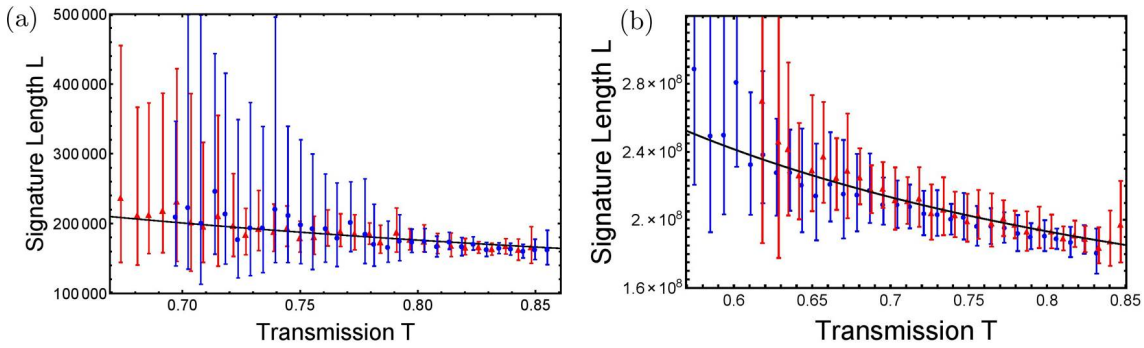


Figure 5.5: (a) Signature length for $\alpha = 0.93$. (b) Signature length for $\alpha = 1.63$. Black curve: theoretical model. Blue dots/bars: results from the data attributed to Bob. Red triangles/bars: results from the data attributed to Charlie. The error bars calculated are statistical.

minimum cost of the matrix $C_{i,j}$ is finally

$$C_{min} = 0.3817 + 0.0939 \times 0.4373 = 0.42276, \tag{5.19}$$

and the parameter g used to calculate the signature length is

$$g = C_{min} - C^h = 0.04106. \tag{5.20}$$

This corresponds to a required signature length of $L = 94000$ for a security level of 0.01%.

In all experimental graphs, errors in the signature length were calculated using the statistical errors of the elements in the cost matrices. The errors in the length were calculated by first adding the errors of the diagonal elements, and subtracting the errors of the off-diagonal elements. This gives a new cost matrix C' from which a new parameter g' can be calculated as above, with $g' < g$. This new g' is then used to calculate a new length $L' > L$, which is the worst-case scenario for the required signature length. The length L' gives the top of the error bar in Figs. 5.4 and 5.5.

Second, the error bars in the diagonal elements are subtracted, and the errors in the off-diagonal elements are added to give a new cost matrix C'' that has a new parameter $g'' > g$. This new g'' is then used to calculate a new length $L'' < L$, which gives a best-case scenario for the required signature length. The length L'' is used for the bottom of the error bar in Figs. 5.4 and 5.5.

Note that to ensure the required security when running a full signature protocol, the longest length L' should be used for the signature length, as this is the worst case scenario. This means it is important to minimise the errors in the cost matrix by taking a large number of measurements to calculate the cost matrix. In this experiment, insufficient data was available at some transmission levels, which led to the large error bars seen.

The experimental results for $\alpha = 0.93$ and $\alpha = 1.63$ are shown in Fig. 5.5. Increasing α gives a better cost matrix, but also makes a forger's guess easier. There is a balance between these two effects, with the optimal α found by maximising g in Eq. (5.13). This is theoretically predicted to be maximal when $\alpha \approx 0.5$, which is supported by the experimental results.

It is important to compare the performance of this scheme to previous results. The first realisation of a QDS scheme without quantum memory was in [48]. In that work

they found that a signature length of about $2L \approx 10^{14}$ was required to sign a one-bit message. Part of the reason this was so high is that there were significant losses in the multiport and they didn't use the optimum α. This experiment was improved upon in [59], where they swapped measurement results instead of using a multiport, and used an improved value of α, as well as a few other minor changes. With these improvements, the new signature length required was about $2L \approx 4 \times 10^9$, over four orders of magnitude better than the previous result. The channel producing this signature length was a 500 m optical fibre, corresponding to a loss level of about 35 %. However, even with this improved signature length, it would take about 40s to sign a one-bit message. Both of these previous experiments were implemented using single-photon detectors, and a large part of the reason for the high signature length is the inefficiency of such detectors, particularly for low amplitude states.

For the protocol involving homodyne detection described here, it can be seen from Fig. 5.4 that the signature length to sign a one-bit message at a similar loss level is $2L \approx 2 \times 10^5$. This is over four orders of magnitude shorter than for single photon measurements, demonstrating the great advantage of using homodyne detection. Part of the advantage comes from the improved efficiency of homodyne detection, but it is also interesting to ask whether there is also a fundamental advantage of this ambiguous measurement scheme. To answer this, a theoretical model is needed to compare both schemes in the ideal theoretical case, which is prvided in the next section.

The current experiment was run at a clock rate of 2.2 MHz, meaning that it takes approximately 0.1 s to sign a one-bit message, a large improvement on previous work. There is currently a plan to increase the clock rate into the GHz range, and this isn't expected to increase the required signature length. This means that about 10^4 one-bit messages could be signed in just 1 s, a vast improvement on previous results and one that could provide a practically useful signature protocol.

5.3.4 Theoretical models

The decisive factors that determine the required signature length are the minimum error probability of a forger p_{min}, and the cost matrix. Since the same states are used for the schemes based on unambiguous and ambiguous state elimination, any difference in performance is determined from the cost matrix. The cost matrix for the homodyne detection scheme is shown in Eq. (5.9) and the associated minimum cost given in Eq. (5.10). Therefore the parameter g used to calculate the signature length in Eq. (5.13) is $g = p_{min}(\frac{1}{2} - p_{err})$. Noting that $\mathrm{erfc}(x)$ is the complementary error function, and can be written as $\mathrm{erfc}(x) = 1 - \mathrm{erf}(x)$, where $\mathrm{erf}(x)$ is the error function, this can be written as

$$g = \frac{p_{\min}}{2} \operatorname{erf}\left(\sqrt{\frac{T}{2}}\alpha\right) \tag{5.21}$$

A higher g gives a shorter signature length and therefore the optimal α is the one that gives the highest g. In this case g is maximal when $\alpha \approx 0.5$. The black curve calculated in Fig. 5.6 is plotted by fixing $\alpha = 0.5$ and calculating L from the resulting g.

I now consider the case where single photon detection is used for unambiguous state elimination. With no experimental imperfections, the correct state will never be eliminated, and the other states will be eliminated with probability dependent on the overlap

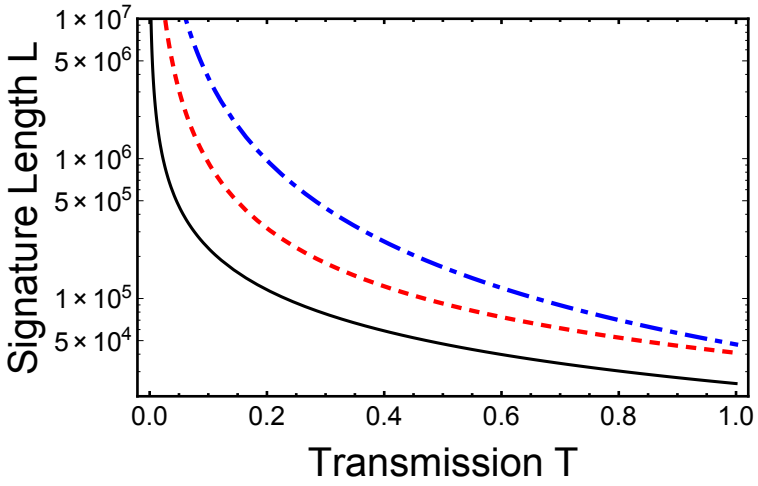


Figure 5.6: Black (solid) curve: Signature length for an ideal ambiguous measurement scheme. Red (dotted) curve: Signature length for an ambiguous measurement scheme with realistic imperfections. Blue (dot-dashed) curve: Signature length for an ideal unambiguous measurement scheme.

of the states. The ideal cost matrix is calculated to be

$$C = \begin{pmatrix} 0 & q & p & q \\ q & 0 & q & p \\ p & q & 0 & q \\ q & p & q & 0 \end{pmatrix}, \tag{5.22}$$

where $p = 1-\exp(-T\alpha^2)$, $q = 1-\exp(-T\alpha^2/2)$. From this, the minimum cost is bounded as before to be $C_{min} = p_{min}q$. Since the diagonal elements are 0, $C_{min} = g$, and g is used to calculate the required signature length. Since this protocol follows the same template as the one involving homodyne detection, the security analysis is the same, and the signature length can be calculated from g using Eq. (5.13). Again, a higher g gives a shorter signature length and therefore the optimal α is the one that gives the highest g. The blue curve in Fig. 5.6 is plotted by using the optimal α at each level of transmission, which in this case is $\alpha \approx 0.7$. As can be seen in Fig. 5.6, the signature length for homodyne measurements is less than that for single photon measurements. This is largely because the optimal α for homodyne measurements is smaller, which means a forger will necessarily make more errors. This shows that ambiguous measurements give a fundamental advantage over unambiguous state elimination in this case, even though they result from more errors. Approximately one order of magnitude of the advantage is due to fundamental reasons, and the remaining three orders of magnitude are due to the improved technical performance of homodyne detection.

In addition, a theoretical model can be created to take into account realistic experimental imperfections that occur in the homodyne detection scheme. The experimental imperfections included in the model are: imperfect detection efficiency, additional variance introduced by the electro-optical modulator, and electronic noise that increases the variance at the measurement stage. The probability for an operator to be measured with an opposite sign to its amplitude depends only on its amplitude and variance, and is given

by

$$p_{err} = \int_{-\infty}^{0} \psi(x)dx = \frac{1}{2}\text{erfc}\left(\frac{\langle\psi\rangle}{\sqrt{V(\psi)}}\right), \tag{5.23}$$

where $V(\psi) = \langle\psi^2\rangle - \langle\psi\rangle^2$. Ideally, under loss, the amplitude of a Stokes operator decreases linearly with T, and the variance decreases with $\sqrt{T}$. By using renormalised Stokes operators $\hat{S}'_i \equiv \hat{S}_i/\sqrt{|\langle\hat{S}_3\rangle|}$, this allows them to be used instead of quadrature operators, where the amplitude decreases with $\sqrt{T}$, and the variance remains constant. However, when imperfections are included, the amplitude and variance don't necessarily follow the ideal form, so their behaviour has to be calculated separately.

The effect of each imperfection can be included in Eq. 5.23 to create a model of the protocol with experimental imperfections. The additional variance introduced by the electro-optical modulator increases the variance of the states to $\epsilon \geq 1$. The imperfect transmission decreases the amplitude from $\alpha \to T\alpha$ and the variance from $\epsilon \to T\epsilon$. The imperfect detector efficiency effectively decreases the amplitude of the measured quadratures and the local oscillator. This means the measured amplitude is reduced to $\eta T\alpha$ and the variance is reduced to $\eta T\epsilon$, where $\eta \leq 1$ is the detection efficiency. The beamsplitter used for heterodyne detection also decreases the amplitude and variance by a half. Finally the electronic noise introduced by the measurement increases the variance, and this increase is independent of transmission. Therefore the final variance is $V = \frac{1}{2}\eta T\epsilon + elect$, where *elect* is the size of the electronic noise relative to the original variances $V_{1,2}$ at $T = 1$. Inserting all this information into Eq. 5.23, the probability of eliminating the distributed state is

$$p_{err} = \frac{1}{2}\text{erfc}\left(\frac{\frac{1}{2}\eta T\alpha}{\sqrt{\frac{1}{2}\eta T\epsilon + elect}}\right). \tag{5.24}$$

All of these parameters can be determined from experimental results, with *elect* measured by looking at the variance as a function of transmission and extrapolating to the point where $T = 0$. In all experiments, $\eta = 0.856$ and $\epsilon = 1.01$, and *elect* varies between 0.04 and 0.08. The theoretical model also takes into account the fact that the modulation of the Stokes operators $\hat{S}_1$ and $\hat{S}_2$ had a slightly different amplitude. The lower amplitude of $\hat{S}_1$ was used to calculate the guaranteed advantage from the cost matrix, and the higher amplitude of $\hat{S}_2$ was used to calculate p_{min}. The encoding always has some phase imperfections; however, since this only has a small effect on the signature length, it is not included in the model for simplicity.

The cost matrix including experimental imperfections is the same as that in Eq. (5.9) but with the new p_{err} above. With this new cost matrix the required signature length can be calculated. This model was used for the black curves in Figs. 5.4 and 5.5, and it can be seen that it fits the data well, at least for the measured transmission range. More data is required to determine whether there are other experimental effects that need to be included at lower transmission ranges. The theoretical model used for the data in Fig. 5.4 is also shown as the red curve in Fig. 5.6. This shows that even taking into account realistic experimental imperfections, the scheme based on heterodyne detection performs better than the one based on single photon detection could ever do. This advantage even increases for lower values of T where an actual signature scheme would likely be performed.

In this section, I have introduced a new quantum signature protocol based on ho-

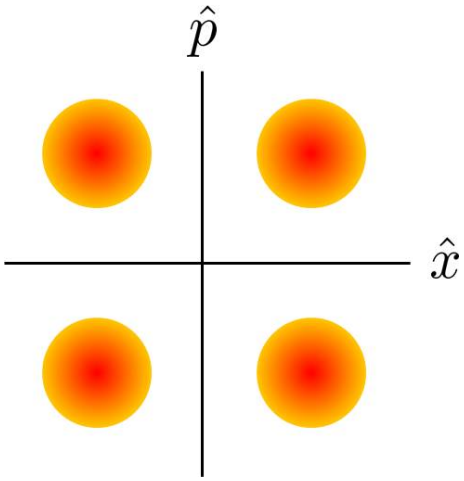


Figure 5.7: Four phase-encoded coherent states for alternative QDS protocol. $|\alpha \exp(i\phi)\rangle$, $\phi = \{\pi/4, 3\pi/4, 5\pi/4, 7\pi/4\}$.

modyne detection. This has been performed experimentally over a fluctuating free-space channel, and the required signature length is four orders of magnitude lower than previous work. I have shown that approximately one order of magnitude of the advantage comes from theoretical effects, and the rest comes from improved technical performance. This scheme provides a new avenue towards a practical quantum digital signature scheme, however more work is required to relax the assumption of authenticated quantum channels.

5.3.5 Alternative schemes based on homodyne measurement

The suggested QDS protocol based on homodyne detection used the coherent states $\{|\alpha\rangle, |\text{-}\alpha\rangle, |i\alpha\rangle, |\text{-}i\alpha\rangle\}$ as the state alphabet. These states were chosen to aid direct comparison with previous work, however it is possible that other state alphabets or elimination procedures could be useful. Here I consider a number of protocols that follow the same method as previously described, but with different states or elimination procedures.

The first procedure I consider uses the same states, but homodyne detection in a random quadrature is performed rather than heterodyne detection. The advantage of this is that the measured state has a higher amplitude than in the heterodyne case, but as a drawback only one state is eliminated at a time. The cost matrix for this case is

$$C = \begin{pmatrix} p_{err} & 1/4 & 1/4 - p_{err} & 1/4 \\ 1/4 & p_{err} & 1/4 & 1/2 - p_{err} \\ 1/2 - p_{err} & 1/4 & p_{err} & 1/4 \\ 1/4 & 1/2 - p_{err} & 1/4 & p_{err} \end{pmatrix}, \tag{5.25}$$

where $p_{err} = \frac{1}{4}\text{erfc}\left(\sqrt{T}\alpha\right)$. From this cost matrix, the parameter g used to calculate the signature length using Eq. (5.13) is $g = \frac{p_{\min}}{4}\left(1 - \text{erfc}\left(\sqrt{T}\alpha\right)\right)$, where $p_{\min}$ is defined in Eq. (5.8), which can be written in terms of the error function as

$$g = \frac{p_{\min}}{4}\,\text{erf}\left(\sqrt{T}\alpha\right). \tag{5.26}$$

I also consider a QDS scheme using the four phase-encoded coherent states in Fig.

5.7. Using these states, $p_{\min}$ is the same as in the previous case, because the states are the same, just rotated by $\pi/4$. However the elimination procedure can be different and I consider two scenarios here. The first is where measurement results in one quadrant eliminate the state in the opposite quadrant. Therefore only one state is eliminated at a time, but the correct state is rarely eliminated. The cost matrix in this case is

$$C = \begin{pmatrix} p_{err}^2 & p_{err}(1-p_{err}) & (1-p_{err})^2 & p_{err}(1-p_{err}) \\ p_{err}(1-p_{err}) & p_{err}^2 & p_{err}(1-p_{err}) & (1-p_{err})^2 \\ (1-p_{err})^2 & p_{err}(1-p_{err}) & p_{err}^2 & p_{err}(1-p_{err}) \\ p_{err}(1-p_{err}) & (1-p_{err})^2 & p_{err}(1-p_{err}) & p_{err}^2 \end{pmatrix}, \tag{5.27}$$

where $p_{err} = \frac{1}{2}\text{erfc}\left(\frac{\sqrt{T}}{2}\alpha\right)$. From this cost matrix, g from Eq. (5.13) is calculated to be $g = \frac{p_{\min}}{2}\text{erfc}\left(\frac{\sqrt{T}}{2}\alpha\right)\left(1-\text{erfc}\left(\frac{\sqrt{T}}{2}\alpha\right)\right)$, which is written in terms of the error function as

$$g = \frac{p_{\min}}{2}\text{erf}\left(\frac{\sqrt{T}}{2}\alpha\right)\left(1-\text{erf}\left(\frac{\sqrt{T}}{2}\alpha\right)\right). \tag{5.28}$$

Another possible elimination scheme is to eliminate all states that aren't in the quadrant of the measurement results. This is essentially the same as identifying the state as being the one in the measured quadrant. The advantage of this is that three states are eliminated per measurement, but the correct state is eliminated more often. The cost matrix for this scenario is

$$C = \begin{pmatrix} 1-(1-p_{err})^2 & 1-p_{err}(1-p_{err}) & 1-p_{err}^2 & 1-p_{err}(1-p_{err}) \\ 1-p_{err}(1-p_{err}) & (1-p_{err})^2 & 1-p_{err}(1-p_{err}) & 1-p_{err}^2 \\ 1-p_{err}^2 & 1-p_{err}(1-p_{err}) & (1-p_{err})^2 & 1-p_{err}(1-p_{err}) \\ 1-p_{err}(1-p_{err}) & 1-p_{err}^2 & 1-p_{err}(1-p_{err}) & (1-p_{err})^2 \end{pmatrix}, \tag{5.29}$$

where $p_{err} = \frac{1}{2}\text{erfc}\left(\frac{\sqrt{T}}{2}\alpha\right)$. From this cost matrix, g from Eq (5.13) is calculated to be $g = \frac{p_{\min}}{2}\left(2 - 3\ \text{erfc}\left(\frac{\sqrt{T}}{2}\alpha\right) + \text{erfc}\left(\frac{\sqrt{T}}{2}\alpha\right)^2\right)$. This can be more simply expressed in terms of the error function as

$$g = \frac{p_{\min}}{2}\text{erf}\left(\frac{\sqrt{T}}{2}\alpha\right)\left(1+\text{erf}\left(\frac{\sqrt{T}}{2}\alpha\right)\right). \tag{5.30}$$

Comparison with the expression for g in Eq. (5.28) shows that this is always larger than the case where one state is eliminated. Therefore it is better to eliminate three states in this case. This difference reduces as T reduces, since the error function tends towards zero.

The last signature scheme I consider here is one based on two signature states $\{|\alpha\rangle, |-\alpha\rangle\}$. Since these states are different to those in the previous schemes, the error probability for a forger is different. In this case the minimum error probability is

$$p_{\min,2} = 1 - \frac{1}{4}|\sum_{i=1}^{2}\sqrt{\lambda_i}|^2, \tag{5.31}$$

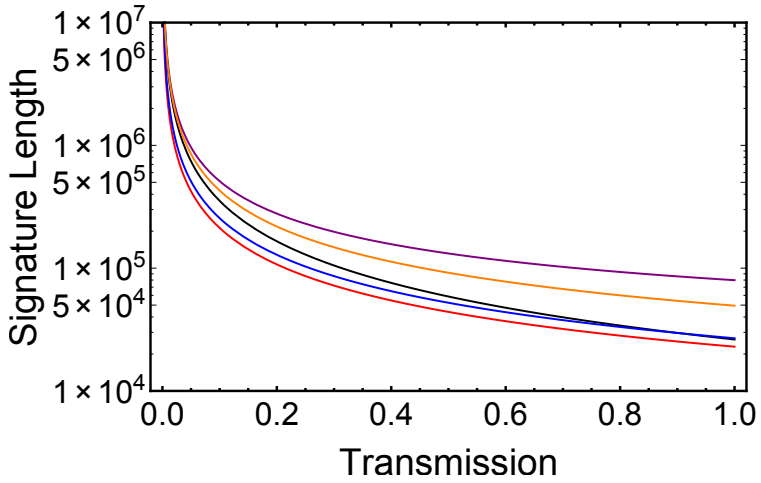


Figure 5.8: Red line: Original scheme based on heterodyne detection using g from Eq. (5.21). Orange line: Scheme using original states and homodyne detection in a random quadrature using g from Eq. (5.26). Purple line: Scheme based on new four state protocol, where one state is eliminated per measurement, calculated using g from Eq. (5.28). Black line: Scheme based on new four state protocol, where three states are eliminated per measurement, calculated using g from Eq. (5.30). Blue line: Scheme based on two coherent states using g from Eq. (5.33).

where $\lambda_{1,2} = 1 \pm \exp(-2\alpha^2)$ are the eigenvalues of the Gram matrix. The elimination scheme is to measure the x-quadrature, and eliminate the opposite state to the measured quadrature. This results in a cost matrix

$$C = \begin{pmatrix} p_{err} & 1 - p_{err} \\ 1 - p_{err} & p_{err} \end{pmatrix}, \tag{5.32}$$

where $p_{err} = \frac{1}{2}\text{erfc}(\sqrt{T}\alpha)$. From this cost matrix, g from Eq. (5.13) is calculated to be $g = p_{\min,2}(1 - \text{erfc}(\sqrt{T}\alpha))$, which written in terms of the error function is

$$g = p_{\min,2}\ \text{erf}(\sqrt{T}\alpha). \tag{5.33}$$

The expressions for g in Eqs. 5.21, 5.26, 5.28, 5.30, 5.33 are used to calculate the required signature length against transmission, and the results are shown in Fig. 5.8. As can be seen, the original QDS protocol (red curve) has the shortest signature length of them all, however the difference between the schemes is often small. With the original states, it is clearly better to perform heterodyne detection (red curve) rather than homodyne detection on a random quadrature (orange curve). Fortunately this is also easier to implement technically, since the measurement procedure remains constant.

For the new four-state protocol, eliminating three states (black curve) is always better than eliminating one state (purple curve), as expected, but this difference does reduce with reducing T. At high values of T, there is very little difference between eliminating three states and using the original scheme, but this difference increases with reducing T.

Interestingly, the two-state protocol (blue curve) only requires a slightly longer signature than the original protocol, at all values of transmission. Therefore the two-state protocol is a competitive alternative to the original four-state protocol, especially when technical difficulty is considered. For example, the signature length in the experiment described in Section 5.3.3 was increased because the displacement in the two Stokes pa-

rameters was different. This wouldn't be a problem in the two-state protocol, which could mean the two-state protocol would require a shorter signature length in a realistic environment.

The signature lengths of the different four-state protocols can be compared at low transmission levels, by using $\text{erf}(x) \approx 1.12x$ for small x. The optimal value of α for all the four-state protocols is $\alpha \approx 0.5$. Using this it can be seen that g for the original protocol is about $\sqrt{2}$ times bigger than g for the other four-state protocols. Since $L \propto 1/g^2$, the signature length at low levels of transmission is approximately half that of the other four-state protocols, which is supported numerically. Comparison with the two-state protocol is more difficult because the error probability of a forger is different, however by inserting the approximate optimal values for α, the schemes can be compared. Doing this it is found that g for the original four-state protocol is approximately 10% larger than for the two-state protocol. This means the required signature length is about 20% shorter for the original four-state protocol than for the two-state protocol. This is of course in the ideal case, and it may be that this difference reduces or even vanishes when technical considerations are included.

In this section I have calculated the signature lengths for a number of protocols to compare their efficiency. The original scheme requires the shortest signature length, but a protocol based on two phase-encoded coherent states provides a competitive alternative. It would be interesting to see how the two compare in realistic experimental conditions. It is possible that other schemes could outperform the proposed ones. For example, a scheme based on more phase-encoded coherent states, or even Gaussian distributed coherent states, could provide an advantage. However developing an elimination scheme for such states becomes complicated, and it would need to be shown that a minimum-cost measurement is the optimum measurement for a forger in order to use this security analysis.

5.4 Summary of Chapter 5

In this chapter, I have introduced the concept of quantum digital signatures and described the most important developments in the field. The most successful QDS protocols to date are based on coherent states and single photon detection, however these require a relatively long signature length to securely sign a message. Here I propose a new signature scheme based on coherent states and homodyne detection. The advantage of this scheme is that every measurement gives a usable result, but this comes at the cost of an increased error rate. I have shown that even with the increased error rate, this new quantum signature protocol outperforms old schemes. When technical considerations are included, the advantage reaches more than four orders of magnitude. This shows that QDS schemes based on homodyne detection provide a valuable area of research in the pursuit of improved signature protocols. Finally, I compared the proposed protocol to some alternative schemes based on homodyne detection. I found that the original scheme requires the shortest signature length, however the length required by a protocol based on two coherent states is comparable. Since the two-state protocol is simpler, it may even require a shorter length when technical considerations are included.

6

Conclusions and Outlook

Before concluding this thesis, I first provide some suggestions for future work.

6.1 Future work

6.1.1 Quantum digital signatures with unauthenticated quantum channels

The QDS protocol with homodyne detection described in the previous chapter assumed that Alice, Bob and Charlie possess authenticated quantum channels between them. This is the same as was done for most previous work, but it is an unrealistic assumption and should be replaced by a security analysis that allows unauthenticated channels. In previous protocols, Alice sent the same quantum signatures to Bob and Charlie, however this is not necessary. The assumption of authenticated quantum channels means that nobody can interfere with the quantum message, nor can they access any of the losses in the channel. This means that if different signatures are sent to Bob and Charlie, no other party can know anything about the signature. Therefore a forger's only strategy is to randomly guess each signature state, which gives a trivial security analysis. To account for this, the same states were sent to Bob and Charlie, which means that a forger could have a perfect copy of the quantum signature. By relaxing the assumption of authenticated channels, Alice can send different states to Bob and Charlie. This means no other party has a perfect copy of the signature; instead, a forger's ability to forge must be bound using parameter estimation of the quantum channel. Since a forger has a worse copy of the signature than with authenticated quantum channels, the signature length should decrease by relaxing this assumption. However with an unauthenticated quantum channel, a forger can also influence what is received by Bob or Charlie, using, for example, an intercept and resend attack. Further work is required to put a limit on how much a forger can achieve in this way.

Unauthenticated channels and discrete measurements

Amiri *et al.* [9] have recently shown that parameter estimation techniques similar to those used in quantum key distribution can be used to provide security for quantum digital signature schemes with unauthenticated quantum channels. In particular, they show that a forger's error probabillity can be lower bound using parameter estimation. Let the ith element of the private key be represented by the binary random variable X_i. Eve's auxiliary quantum system corresponding to each element of the key is denoted by E_i. Results from [221] show that

$$H(X_i|E_i) \leq H(X_i|E') \equiv \sum_r P(E' = r)H(X_i|E' = r) \tag{6.1}$$

The inequality is a result of the Holevo bound, and the equality follows from the definition of conditional entropy. $H(X_i|E_i)$ gives Eve's uncertainty about the element X_i given possession of the corresponding state E_i. Since the different elements of X are uncorrelated, the optimal collective attack is a collection of individual attacks, so $H(X_i|E_i)$ is Eve's uncertainty about X_i if she is limited to collective attacks.

If Eve's measurement returns an outcome $E' = r$, then $X_i = b$ with probability $1 - p_r \geq 1/2$. Eve's best guess is then $X_i = b$, which has an error probability of p_r. Eve's average error probability is therefore

$$p_e = \sum_r P(E' = r)p_r. \tag{6.2}$$

The concavity of the binary entropy shows that

$$h(p_e) = h\left(\sum_r P(E' = r)p_r\right) \geq \sum_r P(E' = r)h(p_r), \tag{6.3}$$

where $h(p) = -p\log p - (1-p)\log(1-p)$ is the binary entropy. Finally, since $X_i|E' = r$ is a classical random binary variable, there must be some $p_r \leq 1/2$ for which $H(X_i|E' = r) = h(p_r)$. Using Eqs. (6.1) and (6.3), this gives a bound on the error probability of a forger:

$$h(p_e) \geq \sum_r P(E' = r)H(X_i|E' = r) \geq H(X_i|E_i). \tag{6.4}$$

In [9], they use a parameter estimation protocol based on decoy states that has been used in QKD [141]. An expression for $H(X_i|E_i)$ is known for the protocol [133, 33], so a bound for the forger's error probability can be found. A bound for the error probability of an honest recipient must also be found using experimental data, for example using cost matrix analysis. As long as a forger has a higher erro probability than an honest party, a full signature scheme can be realised without the requirement of authenticated quantum channels.

Unauthenticated channels and homodyne measurements

An obvious next step is to extend QDS schemes using CV measurement to include unauthenticated quantum channels. For a signature protocol using unauthenticated quantum channels, Bob (Charlie) sends the quantum signature to Alice. This is because Eq. (6.4)

gives a bound on the error probability of a forger trying to determine the classical information encoded in a quantum state. The forger's task is to guess Bob's (Charlie's) classical information, so to use this method Bob (Charlie) must encode the classical information on the quantum states. In this way, Eq. (6.4) will give a forger's error probability about Bob's (Charlie's) classical information. Both the forger's error probability and Alice's error probability have to be calculated using parameter estimation. As long as the forger's error probability is higher than Alice's, the signature protocol is secure with unauthenticated quantum channels. The rest of the signature protocol and security analysis can proceed in the same way as previously. By using two phase-encoded coherent states $|\alpha\rangle, |-\alpha\rangle$ as the possible signature states, Eq. (6.4) is also applicable in the continuous variable case. A lower bound for $H(X_i|E_i)$ must be found using parameter estimation.

The bound in Eq. (6.4) can be rewritten in terms of accessible information by considering the definition of mutual information between a classical variable and quantum state:

$$I(X_i, E_i) = H(X_i) - H(X_i|E_i). \tag{6.5}$$

The accessible information I_{acc} gives an upper bound on the amount of information Eve can gain about the classical information X_i, $I(X_i, E_i) \leq I_{acc}$. Inserting this to the above equation and rearranging gives a lower bound for $H(X_i|E_i)$ and therefore a new lower bound on $h(p_e)$:

$$\begin{aligned} H(X_i) - H(X_i|E_i) &\leq I_{acc}, \\ H(X_i|E_i) &\geq H(X_i) - I_{acc}, \\ h(p_e) &\geq H(X_i) - I_{acc}. \end{aligned} \tag{6.6}$$

Note that since X_i is a classical random variable with two possible outcomes of equal probability, $H(X_i) = 1$. To find the error probability of a forger, an upper bound for I_{acc} has to be found using parameter estimation.

The accessible information in the case of a passive beamsplitter attack on the two coherent states $|\alpha\rangle, |-\alpha\rangle$ is known and presented in [192] as

$$I_{acc} = \frac{1}{2}\left(1+\sqrt{1-f^2}\right)\log\left(1+\sqrt{1-f^2}\right) + \frac{1}{2}\left(1-\sqrt{1-f^2}\right)\log\left(1-\sqrt{1-f^2}\right), \tag{6.7}$$

where f is the overlap between the states held by Eve after the beamsplitter:

$$f = \langle -\sqrt{1-\tau}\alpha | \sqrt{1-\tau}\alpha\rangle = \exp\left(-2(1-\tau)\alpha^2\right). \tag{6.8}$$

This expression for the overlap can easily be adapted to include excess noise $\epsilon \geq 1$ in the channel between Alice and Bob (Charlie) by making the change $\alpha \to \epsilon\alpha$.

This expression for the accessible information can be used to calculate the signature length required when Eve is restricted to a beamsplitter attack. However more work is required to extend to more general attacks. A few results for CV QKD that may be useful for this task are given below:

1. If Alice sends a mixture of coherent states with low amplitude, the state sent is very close to a Gaussian state, so it's acceptable to use results that apply for Gaussian states [138].

2. Gaussian attacks are the optimal collective attack in CV quantum cryptography if the channel is estimated using the covariance matrix[76, 156].

3. Gaussian channels are characterised by the channel transmission τ and the excess noise ϵ [95]. See also Pirandola *et al.* [170] for a complete characterisation of Gaussian attacks.

4. It has been shown that coherent attacks provide no advantage over collective attacks [178], as long as the measured states have low amplitude, as they do here.

If these results hold for quantum digital signatures, then Eq. (6.7) could be used to bound the error probability for a general attack by a forger.

In this section, I have outlined a possible path to provide security without authenticated channels for a two-state quantum signature protocol based on homodyne measurement. Beyond this, a security analysis for other signature alphabets is desirable, e.g. for the original four-state protocol. Further analysis of the most general attacks is also required. Signature protocols with unauthenticated quantum channels where Alice sends the signature to Bob (Charlie) should also be investigated, although a different method to find the error probabilities is required.

6.1.2 Other possibilities for quantum digital signatures

The field of quantum digital signatures is still in its early stages, especially when compared to the vast amount of research about quantum key distribution. Therefore, there remains significant progress to be made in both theoretical description and experimental implementation. Currently, Christoph Marquardt's group in Erlangen is performing an experiment that implements the quantum stages of a QDS protocol with a clock-rate in the GHz range. Assuming the technical performance of this experiment is as good as previously, this would allow messages of about 10^4 bits to be signed in a second over a quantum channel with a length of about 10 km. In future experiments, it would be interesting to extend the channel length to much further distances to investigate the behaviour of signature protocols at high loss.

The obvious next step on the theory side is to investigate how different attacks by Eve affect the security of a quantum signature scheme. In addition to this, it is important to consider different signature alphabets and measurement techniques to see what signature protocols have the best security under attacks from an eavesdropper. This could include extension to Gaussian state alphabets, in which case it would seem more natural to base security on mutual information rather than state elimination. So far efforts to base security on mutual information have been frustrated by the difficulty to find Eve's optimal strategy.

One advantage that QDS has over QKD is that signature protocols are possible at loss levels unsuitable for QKD [9]. This means that QDS could be tested on communication channels that are not yet suitable for QKD. For example, recently, quantum signals have been distibuted using satellites [69], and this channel could be used for a quantum signature scheme. Due to the low transmission level of this channel, a lot of data would be required to verify the security of the channel, however there is no fundamental reason why signatures could not be performed in this way. This could open up the possibility of a global quantum signature distribution channel.

It is important to note that currently classical digital signature schemes perform well,

so there is no need for quantum digital signatures. However, if a quantum computer was developed, classical signatures would become insecure. Due to the importance of signatures to global communication, it is important to have a practical quantum digital signature protocol prepared for such an eventuality.

6.1.3 Nonclassical correlations and multimode entanglement

Pure states are the fundamental class of states, with mixed states simply being a result of a lack of information about a globally pure state. In a pure state, entanglement and nonclassical correlations are equivalent notions, so this suggests that entanglement is the only truly fundamental measure of nonclassicality. However this does not mean that nonclassical correlations beyond entanglement are not a useful concept. Practically, we are usually dealing with mixed states, in which case nonclassical correlations, for example quantum discord, capture more of the quantum nature of the state. It is likely that a more complete understanding of nonclassical correlation measures, such as quantum discord, will lead to a greater ability to use quantum states in a dissipative environment to their full potential. Therefore it is important to continue studying these correlations to understand how they could be useful.

Similarly, although many quantum protocols rely on two-mode entanglement, multimode entanglement is an interesting area of research. As was seen in Chapter 4, states that locally appear classical or separable, can have their quantum or entangled nature revealed by considering additional states to which they are correlated. This demonstrates the importance of multimode correlations and multimode entanglement. In quantum experiments involving systems of many particles, entanglement can become distributed between many of the subsystems. Understanding how best to use these global correlations is an important area of study. In addition, whenever a quantum state is in an open quantum system, correlations between the state and the environment are established. Being able to exert some control over these correlations could lead to some exciting techniques in quantum information experiments.

6.1.4 Discord in quantum key distribution

Quantum key distribution relies on the distribution of nonorthogonal states to ensure that a forger cannot perfectly learn the secret key. Therefore discord between Alice and Bob is clearly necessary in a QKD protocol. This has been further developed by Pirandola *et al.* [169], who showed that the shared discord provides an upper bound for the secret key rate, following the equation

$$\begin{aligned} K^{\rightarrow} &\leq D^{\leftarrow}(\hat{\rho}_{AB}) - E_F(\hat{\rho}_{AE}), \\ K^{\leftarrow} &\leq D^{\rightarrow}(\hat{\rho}_{AB}) - E_F(\hat{\rho}_{BE}), \end{aligned} \tag{6.9}$$

where $K^{\rightarrow(\leftarrow)}$ is the secret key rate using forward (reverse) reconciliation. It would be interesting to investigate how tight this bound is, by calculating the discord present in QKD protocols where the secret key rate is known. This would determine how much increasing the discord shared between Alice and Bob improves the secret key rate, or whether it is necessary to consider other properties of the state when deciding how to optimise the rate.

6.2 Summary

This thesis involves two main topics of research. Chapters 3 and 4 focus on studying the behaviour of quantum correlations in continuous variable mixed states. In Chapter 5, I develop a quantum digital signature protocol that is implemented using coherent states and homodyne measurement.

In Chapter 3, I study the phenomenon of Gaussian discord increase under local loss. I look at the different properties that affect the degree of the increase, and focus on describing the increase in terms of non-orthogonality of states. I then show how considering the flow of correlations between the state and the environment can give more insight about discord increase. Finally, I show that discord increase under local loss also occurs for a discrete mixture of coherent states. This makes it easier to see how the non-orthogonality of the two states affects the discord increase, identifying it as the dominant factor.

In Chapter 4, I present two schemes that exhibits entanglement creation by mixing classical modes on a beamsplitter. The entanglement created is multimode entanglement between three modes. The correlations that the classical modes initially share with another mode allow the entanglement to be created by restoring the nonclassicality that had been destroyed by noise. This emphasises the importance of global correlations, and shows that to determine whether a state is nonclassical, one must consider all the states with which it shares correlations. Fully understanding the properties of this multimode entanglement could enhance our ability to utilise quantum states that exist in open quantum systems.

In Chapter 5, I introduce the field of quantum digital signatures and describe work carried out on this topic to this point. I propose a protocol that uses homodyne measurement to distribute the quantum signature. Unlike previous measurement schemes, this can be thought of as an ambiguous measurement, since there are necessarily errors caused by the measurement technique. Despite the increased error rate, I showed that this measurement scheme outperforms previous results, largely because the measurement always produces results. When experimental imperfections are taken into account, the advantage of this method is further amplified. This work provides an interesting route for future work on quantum digital signatures.

Bibliography

[1] G. L. Abbas, V. W. S. Chan, and T. K. Yee. Local-oscillator excess-noise suppression for homodyne and heterodyne detection. *Opt. Lett.*, 8(8):419–421, Aug 1983.

[2] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter. The mother of all protocols: restructuring quantum information's family tree. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 465(2108):2537–2563, 2009.

[3] G. Adesso. Gaussian interferometric power. *Physical Review A*, 90(2):022321, August 2014.

[4] G. Adesso, V. D'Ambrosio, E. Nagali, M. Piani, and F. Sciarrino. Experimental Entanglement Activation from Discord in a Programmable Quantum Measurement. *Physical Review Letters*, 112(14):140501, April 2014.

[5] G. Adesso and A. Datta. Quantum versus Classical Correlations in Gaussian States. *Physical Review Letters*, 105(3):030501, July 2010.

[6] G. Adesso and F. Illuminati. Gaussian measures of entanglement versus negativities: Ordering of two-mode Gaussian states. *Phys. Rev. A*, 72(3):032334, September 2005.

[7] G. H. Aguilar, O. Jiménez Farías, A. Valdés-Hernández, P. H. Souto Ribeiro, L. Davidovich, and S. P. Walborn. Flow of quantum correlations from a two-qubit system to its environment. *Phys. Rev. A*, 89:022339, Feb 2014.

[8] R. Amiri and E. Andersson. Unconditionally Secure Quantum Signatures. *Entropy*, 17:5635–5659, August 2015.

[9] R. Amiri, P. Wallden, A. Kent, and E. Andersson. Secure Quantum Signatures Using Insecure Quantum Channels. *ArXiv e-prints*, July 2015.

[10] E. Andersson, M. Curty, and I. Jex. Experimentally realizable quantum comparison of coherent states and its applications. *Phys. Rev. A*, 74:022304, Aug 2006.

[11] H. Araki and E. H. Lieb. Entropy inequalities. *Comm. Math. Phys.*, 18(2):160–170, 1970.

[12] J. M. Arrazola, P. Wallden, and E. Andersson. Multiparty Quantum Signature Schemes. *ArXiv e-prints*, May 2015.

[13] A. Aspect, P. Grangier, and G. Roger. Experimental tests of realistic local theories via Bell's theorem. *Phys. Rev. Lett.*, 47:460–463, Aug 1981.

[14] A. Aspect, P. Grangier, and G. Roger. Experimental realization of Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment* : A new violation of Bell's inequalities. *Phys. Rev. Lett.*, 49:91–94, Jul 1982.

[15] R. Auccaise, J. Maziero, L. C. Céleri, D. O. Soares-Pinto, E. R. deAzevedo, T. J. Bonagamba, R. S. Sarthour, I. S. Oliveira, and R. M. Serra. Experimentally witnessing the quantumness of correlations. *Phys. Rev. Lett.*, 107:070501, Aug 2011.

[16] K. Banaszek. Optimal receiver for quantum cryptography with two coherent states. *Physics Letters A*, 253(1-2):12 – 15, 1999.

[17] S. Bandyopadhyay, R. Jain, J. Oppenheim, and C. Perry. Conclusive exclusion of quantum states. *Phys. Rev. A*, 89:022336, Feb 2014.

[18] S. Barnett. *Quantum Information.* Oxford University Press, New York, 2009.

[19] J. S. Bell. On the Einstein Podolsky Rosen Paradox. *Physics*, 1:195–200, 1964.

[20] C. H. Bennett and G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. *G. Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[21] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[22] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76:722–725, Jan 1996.

[23] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824–3851, Nov 1996.

[24] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.*, 69:2881–2884, Nov 1992.

[25] J. Bertrand and P. Bertrand. A Tomographic Approach to Wigner's Function. *Foundations of Physics*, 17:397, 1987.

[26] L. J. Boya. The Thermal Radiation Formula of Planck (1900). *ArXiv Physics e-prints*, February 2004.

[27] S. L. Braunstein and H. J. Kimble. Dense coding for continuous variables. *Phys. Rev. A*, 61:042302, Mar 2000.

[28] S. L. Braunstein and P. van Loock. Quantum information with continuous variables. *Rev. Mod. Phys.*, 77:513–577, Jun 2005.

[29] M. Brunelli, C. Benedetti, S. Olivares, A. Ferraro, and M. G. A. Paris. Single- and two-mode quantumness at a beam splitter. *Physical Review A*, 91(6):062315, June 2015.

[30] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.*, 87:167902, Sep 2001.

[31] P. Busch, P. Lahti, and P. Mittelstaedt. *The Quantum Theory of Measurement.* Springer, 1996.

[32] H. Cable, M. Gu, and K. Modi. Power of One Bit of Quantum Information in Quantum Metrology. *ArXiv e-prints*, April 2015.

[33] R. Y. Q. Cai and V. Scarani. Finite-key analysis for practical implementations of quantum key distribution. *New Journal of Physics*, 11(4):045024, April 2009.

[34] S. Campbell, T. J. G. Apollaro, C. Di Franco, L. Banchi, A. Cuccoli, R. Vaia, F. Plastina, and M. Paternostro. Propagation of nonclassical correlations across a quantum spin chain. *Phys. Rev. A*, 84:052316, Nov 2011.

[35] F. Caruso, J. Eisert, V. Giovannetti, and A. S. Holevo. Optimal unitary dilation for bosonic gaussian channels. *Phys. Rev. A*, 84:022306, Aug 2011.

[36] C. G. H. Casimir. On the attraction between two perfectly conducting plates. *Proc. Kon. Nederland. Akad. Wetensch*, B51:793–795, 1948.

[37] N. J. Cerf and C. Adami. Negative entropy and information in quantum mechanics. *Phys. Rev. Lett.*, 79:5194–5197, Dec 1997.

[38] N. J. Cerf, G. Leuchs, and E. S. Polzik. *Quantum Information with Continuous Variables of Atoms and Light.* Imperial College Press, 2007.

[39] R. Y. Chiao and J. C. Garrison. *Quantum Optics.* Oxford University Press, 2008.

[40] V. Chille, N. Quinn, C. Peuntinger, C. Croal, L. Mišta, C. Marquardt, G. Leuchs, and N. Korolkova. Quantum nature of Gaussian discord: Experimental evidence and role of system-environment correlations. *Phys. Rev. A*, 91(5):050301, May 2015.

[41] T. K. Chuan, J. Maillard, K. Modi, T. Paterek, M. Paternostro, and M. Piani. Quantum discord bounds the amount of distributed entanglement. *Phys. Rev. Lett.*, 109:070501, Aug 2012.

[42] F. Ciccarello and V. Giovannetti. Creating quantum correlations through local nonunitary memoryless channels. *Phys. Rev. A*, 85:010102, Jan 2012.

[43] F. Ciccarello and V. Giovannetti. Local-channel-induced rise of quantum correlations in continuous-variable systems. *Phys. Rev. A*, 85:022108, Feb 2012.

[44] L. Clarisse. Entanglement Distillation; A Discourse on Bound Entanglement in Quantum Information Theory. *eprint arXiv:quant-ph/0612072*, December 2006.

[45] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller. Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. *Nat. Commun.*, 3:1174, Nov 2012.

[46] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.

[47] V. Coffman, J. Kundu, and W. K. Wootters. Distributed entanglement. *Phys. Rev. A*, 61:052306, Apr 2000.

[48] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller. Realization of Quantum Digital Signatures without the Requirement of Quantum Memory. *Physical Review Letters*, 113(4):040502, July 2014.

[49] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley-Interscience, New York, NY, USA, 1991.

[50] C. Croal, C. Peuntinger, V. Chille, C. Marquardt, G. Leuchs, N. Korolkova, and L. Mišta. Entangling the Whole by Beam Splitting a Part. *Physical Review Letters*, 115(19):190501, November 2015.

[51] T. S. Cubitt, F. Verstraete, W. Dür, and J. I. Cirac. Separable states can be used to distribute entanglement. *Phys. Rev. Lett.*, 91:037902, Jul 2003.

[52] M. Curty, M. Lewenstein, and N. Lütkenhaus. Entanglement as a precondition for secure quantum key distribution. *Phys. Rev. Lett.*, 92:217903, May 2004.

[53] A. Datta. A Condition for the Nullity of Quantum Discord. *ArXiv e-prints*, March 2010.

[54] A. Datta, S. T. Flammia, and C. M. Caves. Entanglement and the power of one qubit. *Physical Review A*, 72(4):042316, October 2005.

[55] A. Datta, A. Shaji, and C. M. Caves. Quantum discord and the power of one qubit. *Phys. Rev. Lett.*, 100:050502, Feb 2008.

[56] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society of London Series A*, 461:207–235, January 2005.

[57] D. Dieks. Overlap and distinguishability of quantum states. *Physics Letters A*, 126(5-6):303 – 306, 1988.

[58] W. Diffie and M.E. Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6):644–654, Nov 1976.

[59] R. J. Donaldson, R. J. Collins, K. Kleczkowska, R. Amiri, P. Wallden, V. Dunjko, J. Jeffers, E. Andersson, and G. S. Buller. Experimental demonstration of kilometer-range quantum digital signatures. *Phys. Rev. A*, 93:012329, Jan 2016.

[60] Lu-Ming Duan, G. Giedke, J. I. Cirac, and P. Zoller. Inseparability criterion for continuous variable systems. *Phys. Rev. Lett.*, 84:2722–2725, Mar 2000.

[61] V. Dunjko, P. Wallden, and E. Andersson. Quantum digital signatures without quantum memory. *Phys. Rev. Lett.*, 112:040502, Jan 2014.

[62] T. Eberle, V. Händchen, J. Duhme, T. Franz, F. Furrer, R. Schnabel, and R. F. Werner. Gaussian entanglement for quantum key distribution from a single-mode squeezing source. *New Journal of Physics*, 15(5):053049, 2013.

[63] A. Einstein. On a heuristic viewpoint concerning the production and transformation of light. *Annalen der Physik*, 17:132, 1905.

[64] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.

[65] J. Eisert, S. Scheel, and M. B. Plenio. Distilling Gaussian States with Gaussian Operations is Impossible. *Phys. Rev. Lett.*, 89:137903, Sep 2002.

[66] A. Ekert and R. Jozsa. Quantum algorithms: entanglement-enhanced information processing. *Philosophical Transactions of the Royal Society of London Series A*, 356:1769, August 1998.

[67] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[68] T. ElGamal. *Advances in Cryptology: Proceedings of CRYPTO 84*, chapter A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, pages 10–18. Springer Berlin Heidelberg, Berlin, Heidelberg, 1985.

[69] D. Elser, K. Günthner, I. Khan, B. Stiller, C. Marquardt, G. Leuchs, K. Saucke, D. Tröndle, F. Heine, S. Seel, P. Greulich, H. Zech, B. Gütlich, I. Richter, and R. Meyer. Satellite Quantum Communication via the Alphasat Laser Communication Terminal. *ArXiv e-prints*, October 2015.

[70] F. F. Fanchini, L. K. Castelano, M. F. Cornelio, and M. C. de Oliveira. Locally inaccessible information as a fundamental ingredient to quantum information. *New Journal of Physics*, 14(1):013027, January 2012.

[71] F. F. Fanchini, M. F. Cornelio, M. C. de Oliveira, and A. O. Caldeira. Conservation law for distributed entanglement of formation and quantum discord. *Phys. Rev. A*, 84:012313, Jul 2011.

[72] A. Fedrizzi, M. Zuppardo, G. G. Gillett, M. A. Broome, M. P. Almeida, M. Paternostro, A. G. White, and T. Paterek. Experimental distribution of entanglement with separable carriers. *Phys. Rev. Lett.*, 111:230504, Dec 2013.

[73] A. Ferraro and M. G. A. Paris. Nonclassicality Criteria from Phase-Space Representations and Information-Theoretical Constraints Are Maximally Inequivalent. *Physical Review Letters*, 108(26):260403, June 2012.

[74] J. Fiurášek. Gaussian Transformations and Distillation of Entangled Gaussian States. *Phys. Rev. Lett.*, 89:137904, Sep 2002.

[75] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik. Unconditional quantum teleportation. *Science*, 282(5389):706–709, 1998.

[76] R. García-Patrón and N. J. Cerf. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Phys. Rev. Lett.*, 97:190503, Nov 2006.

[77] C. Gerry and P. Knight. *Introductory Quantum Optics*. Cambridge University Press, 2005.

[78] G. Giedke and J. I. Cirac. Characterization of Gaussian operations and distillation of Gaussian states. *Phys. Rev. A*, 66:032316, Sep 2002.

[79] G. Giedke, L.-M. Duan, J. I. Cirac, and P. Zoller. All inseparable two-mode Gaussian continuous variable states are distillable. *eprint arXiv:quant-ph/0007061*, July 2000.

[80] G. Giedke, B. Kraus, M. Lewenstein, and J. I. Cirac. Separability properties of three-mode Gaussian states. *Phys. Rev. A*, 64:052303, Oct 2001.

[81] G. Giedke, M. M. Wolf, O. Krüger, R. F. Werner, and J. I. Cirac. Entanglement of Formation for Symmetric Gaussian States. *Phys. Rev. Lett.*, 91:107901, Sep 2003.

[82] P. Giorda, M. Allegra, and M. G. A. Paris. Quantum discord for Gaussian states with non-Gaussian measurements. *Phys. Rev. A*, 86:052328, Nov 2012.

[83] P. Giorda and M. G. A. Paris. Gaussian quantum discord. *Phys. Rev. Lett.*, 105:020503, Jul 2010.

[84] D. Girolami. Interpreting quantum discord in quantum metrology. *Journal of Physics Conference Series*, 626(1):012042, July 2015.

[85] D. Girolami and G. Adesso. Quantum discord for general two-qubit states: Analytical progress. *Phys. Rev. A*, 83(5):052108, May 2011.

[86] N. Gisin. Bell's inequality holds for all non-product states. *Physics Letters A*, 154(5):201 – 202, 1991.

[87] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger. Significant-loophole-free test of bell's theorem with entangled photons. *Phys. Rev. Lett.*, 115:250401, Dec 2015.

[88] R. J. Glauber. Coherent and incoherent states of the radiation field. *Physical Review*, 131:2766, 1963.

[89] R. J. Glauber. Photon correlations. *Phys. Rev. Lett.*, 10:84, 1963.

[90] R. J. Glauber. The quantum theory of optical coherence. *Physical Review*, 130:2529, 1963.

[91] O. Glöckl, J. Heersink, N. Korolkova, G. Leuchs, and S. Lorenz. A pulsed source of continuous variable polarization entanglement. *Journal of Optics B: Quantum and Semiclassical Optics*, 5(4):S492, 2003.

[92] D. Gottesman and I. Chuang. Quantum Digital Signatures. *eprint arXiv:quant-ph/0105032*, May 2001.

[93] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger. Bell's theorem without inequalities. *American Journal of Physics*, 58(12):1131–1143, 1990.

[94] F. Grosshans and P. Grangier. Quantum cloning and teleportation criteria for continuous quantum variables. *Phys. Rev. A*, 64:010301, Jun 2001.

[95] F. Grosshans and P. Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, Jan 2002.

[96] M. Gu, H. M. Chrzanowski, S. M. Assad, T. Symul, K. Modi, T. C. Ralph, V. Vedral, and P. K. Lam. Observing the operational significance of discord consumption. *Nature Physics*, 8:671–675, September 2012.

[97] K. Hammerer, A. S. Sørensen, and E. S. Polzik. Quantum interface between light and atomic ensembles. *Reviews of Modern Physics*, 82:1041–1093, April 2010.

[98] J. Hao, C. Li, and G. Guo. Controlled dense coding using the Greenberger-Horne-Zeilinger state. *Phys. Rev. A*, 63:054301, Apr 2001.

[99] P. M. Hayden, M. Horodecki, and B. M. Terhal. The asymptotic entanglement cost of preparing a quantum state. *Journal of Physics A Mathematical General*, 34:6891–6898, September 2001.

[100] J. Heersink, T. Gaber, S. Lorenz, O. Glöckl, N. Korolkova, and G. Leuchs. Polarization squeezing of intense pulses with a fiber-optic Sagnac interferometer. *Phys. Rev. A*, 68:013815, Jul 2003.

[101] J. Heersink, V. Josse, G. Leuchs, and U. L. Andersen. Efficient polarization squeezing in optical fibers. *Opt. Lett.*, 30(10):1192–1194, May 2005.

[102] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, C. Marquardt, and G. Leuchs. Atmospheric continuous-variable quantum communication. *New Journal of Physics*, 16(11):113018, November 2014.

[103] B. Heim, C. Peuntinger, C. Wittmann, C. Marquardt, and G. Leuchs. Free space quantum communication using continuous polarization variables. In *Imaging and Applied Optics*, page LWD3. Optical Society of America, 2011.

[104] W. Heisenberg. Über den Anschaulichen inhalt der Quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Physik*, 43:172–198, 1927.

[105] L. Henderson and V. Vedral. Classical, quantum and total correlations. *Journal of Physics A Mathematical General*, 34:6899–6905, September 2001.

[106] 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. Experimental loophole-free violation of a Bell inequality using entangled electron spins separated by 1.3 km. *Nature*, 526:682–686, August 2015.

[107] W. Hoeffding. Probability inequalities for sums of bounded random variables. *j-J-AM-STAT-ASSOC*, 58(301):13–30, March 1963.

[108] A. S. Holevo, M. Sohma, and O. Hirota. Capacity of quantum Gaussian channels. *Phys. Rev. A*, 59:1820–1828, Mar 1999.

[109] A. S. Holevo and R. F. Werner. Evaluating capacities of bosonic Gaussian channels. *Phys. Rev. A*, 63:032312, Feb 2001.

[110] A.S. Holevo. Problems in the mathematical theory of quantum communication channels. *Reports on Mathematical Physics*, 12(2):273 – 278, 1977.

[111] A.S. Holevo. The capacity of the quantum channel with general signal states. *Information Theory, IEEE Transactions on*, 44(1):269–273, Jan 1998.

[112] P. R. Holland. *The Quantum Theory of Motion*. Cambridge University Press, 1993. Cambridge Books Online.

[113] C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.*, 59:2044–2046, Nov 1987.

[114] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature? *Phys. Rev. Lett.*, 80:5239–5242, Jun 1998.

[115] M. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. Sen(De), U. Sen, and B. Synak-Radtke. Local versus nonlocal information in quantum-information theory: Formalism and phenomena. *Phys. Rev. A*, 71:062307, Jun 2005.

[116] R. Horodecki and M. Horodecki. Information-theoretic aspects of inseparability of mixed states. *Phys. Rev. A*, 54:1838–1843, Sep 1996.

[117] R. Horodecki and P. Horodecki. Quantum redundancies and local realism. *Physics Letters A*, 194(3):147 – 152, 1994.

[118] R. Horodecki, P. Horodecki, and K. Horodecki, M.and Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865–942, Jun 2009.

[119] X. Hu, H. Fan, D. L. Zhou, and W. Liu. Necessary and sufficient conditions for local creation of quantum correlation. *Phys. Rev. A*, 85:032102, Mar 2012.

[120] X. Hu, Y. Gu, Q. Gong, and G. Guo. Necessary and sufficient condition for Markovian-dissipative-dynamics-induced quantum discord. *Phys. Rev. A*, 84:022113, Aug 2011.

[121] J. Solomon Ivan, S. Chaturvedi, E. Ercolessi, G. Marmo, G. Morandi, N. Mukunda, and R. Simon. Entanglement and nonclassicality for multimode radiation-field states. *Phys. Rev. A*, 83:032118, Mar 2011.

[122] I.D. Ivanovic. How to differentiate between non-orthogonal states. *Physics Letters A*, 123(6):257 – 259, 1987.

[123] K. Jacobs and D. A. Steck. A straightforward introduction to continuous quantum measurement. *Contemporary Physics*, 47(5):279–303, 2006.

[124] L. Jakóbczyk. Entangling two qubits by dissipation. *Journal of Physics A: Mathematical and General*, 35(30):6383, 2002.

[125] J. Jing, J. Zhang, Y. Yan, F. Zhao, C. Xie, and K. Peng. Experimental demonstration of tripartite entanglement and controlled dense coding for continuous variables. *Phys. Rev. Lett.*, 90:167903, Apr 2003.

[126] D. Johnson, A. Menezes, and S. Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, 1(1):36–63, 2001.

[127] R. Jozsa. Entanglement and Quantum Computation. *eprint arXiv:quant-ph/9707034*, July 1997.

[128] M. S. Kim, W. Son, V. Bužek, and P. L. Knight. Entanglement by a beam splitter: Nonclassicality as a prerequisite for entanglement. *Phys. Rev. A*, 65:032323, Feb 2002.

[129] J. R. Klauder. Improved version of optical equivalence theorem. *Phys. Rev. Lett.*, 16:534–536, Mar 1966.

[130] E. Knill and R. Laflamme. Power of one bit of quantum information. *Phys. Rev. Lett.*, 81:5672–5675, Dec 1998.

[131] M. Koashi and A. Winter. Monogamy of quantum entanglement and other correlations. *Phys. Rev. A*, 69:022309, Feb 2004.

[132] N. Korolkova, G. Leuchs, R. Loudon, T. C. Ralph, and Ch. Silberhorn. Polarization squeezing and continuous-variable polarization entanglement. *Phys. Rev. A*, 65:052306, Apr 2002.

[133] B. Kraus, C. Branciard, and R. Renner. Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses. *Phys. Rev. A*, 75:012316, Jan 2007.

[134] R. Laflamme, D. Cory, C. Negrevergne, and L. Viola. NMR Quantum Information Processing and Entanglement. *Quantum Info. Comput.*, 2(2):166–176, February 2002.

[135] L. Lamport. Constructing digital signatures from a one-way function. Technical report, Oct 1979.

[136] B. P. Lanyon, M. Barbieri, M. P. Almeida, and A. G. White. Experimental Quantum Computing without Entanglement. *Physical Review Letters*, 101(20):200501, November 2008.

[137] U. Leonhardt. *Essential Quantum Optics*. Cambridge University Press, 2010.

[138] A. Leverrier and P. Grangier. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.*, 102:180504, May 2009.

[139] X. Li, Q. Pan, J. Jing, J. Zhang, C. Xie, and K. Peng. Quantum Dense Coding Exploiting a Bright Einstein-Podolsky-Rosen Beam. *Phys. Rev. Lett.*, 88:047904, Jan 2002.

[140] S. Lloyd. Enhanced sensitivity of photodetection via quantum illumination. *Science*, 321(5895):1463–1465, 2008.

[141] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields. Efficient decoy-state quantum key distribution with quantified security. *Opt. Express*, 21(21):24550–24565, Oct 2013.

[142] A. Luis and N. Korolkova. Polarization squeezing and nonclassical properties of light. *Phys. Rev. A*, 74:043817, Oct 2006.

[143] S. Luo. Quantum discord for two-qubit systems. *Phys. Rev. A*, 77:042303, Apr 2008.

[144] N. Lütkenhaus and Stephen M. Barnett. Nonclassical effects in phase space. *Phys. Rev. A*, 51:3340–3342, Apr 1995.

[145] V. Madhok and A. Datta. Quantum Discord as a Resource in Quantum Communication. *International Journal of Modern Physics B*, 27:1345041, June 2012.

[146] L. S. Madsen, A. Berni, M. Lassen, and U. L. Andersen. Experimental Investigation of the Evolution of Gaussian Quantum Discord in an Open System. *Phys. Rev. Lett.*, 109:030402, Jul 2012.

[147] L. Mandel and E. Wolf. *Optical Coherence and Quantum Optics*. Cambridge University Press, 1995.

[148] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger. Dense coding in experimental quantum communication. *Phys. Rev. Lett.*, 76:4656–4659, Jun 1996.

[149] R. C. Merkle. *Advances in Cryptology — CRYPTO' 89 Proceedings*, chapter A Certified Digital Signature, pages 218–238. Springer New York, New York, NY, 1990.

[150] L. Mišta. Entanglement sharing with separable states. *Phys. Rev. A*, 87:062326, Jun 2013.

[151] L. Mišta and N. Korolkova. Distribution of continuous-variable entanglement by separable Gaussian states. *Phys. Rev. A*, 77:050302, May 2008.

[152] L. Mišta, D. McNulty, and G. Adesso. No-activation theorem for Gaussian nonclassical correlations by Gaussian operations. *Phys. Rev. A*, 90:022328, Aug 2014.

[153] L. Mišta, Jr. and N. Korolkova. Improving continuous-variable entanglement distribution by separable states. *Phys. Rev. A*, 80(3):032310, September 2009.

[154] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral. The classical-quantum boundary for correlations: Discord and related measures. *Reviews of Modern Physics*, 84:1655–1707, October 2012.

[155] C. A. Muschik, E. S. Polzik, and J. I. Cirac. Dissipatively driven entanglement of two macroscopic atomic ensembles. *Phys. Rev. A*, 83:052312, May 2011.

[156] M. Navascués, F. Grosshans, and A. Acín. Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography. *Phys. Rev. Lett.*, 97:190502, Nov 2006.

[157] S. Olivares and M. G. A. Paris. The balance of quantum correlations for a class of feasible tripartite continuous variable states. *International Journal of Modern Physics B*, 27(01n03):1345024, 2013.

[158] H. Ollivier and W. H. Zurek. Quantum Discord: A Measure of the Quantumness of Correlations. *Physical Review Letters*, 88(1):017901, January 2002.

[159] T. Opatrný, G. Kurizki, and D.-G. Welsch. Improvement on teleportation of continuous variables by photon subtraction via conditional measurement. *Phys. Rev. A*, 61:032302, Feb 2000.

[160] J. Oppenheim, M. Horodecki, P. Horodecki, and R. Horodecki. Thermodynamical approach to quantifying quantum correlations. *Phys. Rev. Lett.*, 89:180402, Oct 2002.

[161] C. Paar and Pelzl. J. *Understanding Cryptography: A Textbook for Students and Practititioners*. Springer, Berlin, 2010.

[162] G. Passante, O. Moussa, D. A. Trottier, and R. Laflamme. Experimental detection of nonclassical correlations in mixed-state quantum computation. *Physical Review A*, 84(4):044302, October 2011.

[163] W. Pauli. *Die allgemeinen Prinzipien der Wellenmechanik, Handbuch der Physik*. Springer, Berlin, 1933.

[164] W. Pauli. *General Principles of Quantum Optics*. Springer, Berlin, 1980.

[165] A. Peres. How to differentiate between non-orthogonal states. *Physics Letters A*, 128(12):19 –, 1988.

[166] A. Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77:1413–1415, Aug 1996.

[167] C. Peuntinger, V. Chille, L. Mišta, Jr., N. Korolkova, M. Förtsch, J. Korger, C. Marquardt, and G. Leuchs. Distributing Entanglement with Separable States. *Physical Review Letters*, 111(23):230506, December 2013.

[168] C. Peuntinger, B. Heim, C. R. Müller, C. Gabriel, C. Marquardt, and G. Leuchs. Distribution of squeezed states through an atmospheric channel. *Phys. Rev. Lett.*, 113:060502, Aug 2014.

[169] S. Pirandola. Quantum discord as a resource for quantum cryptography. *Scientific Reports*, 4:6956, November 2014.

[170] S. Pirandola, S. L. Braunstein, and S. Lloyd. Characterization of Collective Gaussian Attacks and Security of Coherent-State Quantum Cryptography. *Phys. Rev. Lett.*, 101:200504, Nov 2008.

[171] S. Pirandola, A. Serafini, and S. Lloyd. Correlation matrices of two-mode bosonic systems. *Phys. Rev. A*, 79:052327, May 2009.

[172] S. Pirandola, G. Spedalieri, S. L. Braunstein, N. J. Cerf, and S. Lloyd. Optimality of Gaussian Discord. *Phys. Rev. Lett.*, 113:140405, Oct 2014.

[173] M. B. Plenio. Logarithmic negativity: A full entanglement monotone that is not convex. *Phys. Rev. Lett.*, 95:090503, Aug 2005.

[174] N. Quinn, C. Croal, and N. Korolkova. Quantum discord and entanglement distribution as the flow of correlations through a dissipative quantum system. *Journal of Russian Laser Research*, 36(6):550–561, 2015.

[175] T. C. Ralph. Security of continuous-variable quantum cryptography. *Phys. Rev. A*, 62:062306, Nov 2000.

[176] T. C. Ralph and E. H. Huntington. Unconditional continuous-variable dense coding. *Phys. Rev. A*, 66:042321, Oct 2002.

[177] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 73:58–61, Jul 1994.

[178] R. Renner and J. I. Cirac. de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography. *Phys. Rev. Lett.*, 102:110504, Mar 2009.

[179] E. Schrödinger. Der stetige Uebergang von der Mikro- zur Macromechanik. *Naturwiss*, 14:664, 1926.

[180] E. Schrödinger. Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften*, 23(48):807–812, 1935.

[181] E. Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31:555–563, 10 1935.

[182] B. Schumacher and M. D. Westmoreland. Sending classical information via noisy quantum channels. *Phys. Rev. A*, 56:131–138, Jul 1997.

[183] A. Serafini. Multimode uncertainty relations and separability of continuous variable states. *Phys. Rev. Lett.*, 96:110402, Mar 2006.

[184] A. Serafini, J. Eisert, and M. M. Wolf. Multiplicativity of maximal output purities of Gaussian channels under Gaussian inputs. *Phys. Rev. A*, 71:012320, Jan 2005.

[185] A. Serafini, F. Illuminati, and S. DeSiena. LETTER TO THE EDITOR: Symplectic invariants, entropic measures and correlations of Gaussian states. *Journal of Physics B Atomic Molecular Physics*, 37:L21–L28, January 2004.

[186] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam. Strong loophole-free test of local realism*. *Phys. Rev. Lett.*, 115:250402, Dec 2015.

[187] C.E. Shannon. A mathematical theory of communication. *Bell System Technical Journal, The*, 27(3):379–423, July 1948.

[188] R. M. Shelby, M. D. Levenson, S. H. Perlmutter, R. G. DeVoe, and D. F. Walls. Broad-band parametric deamplification of quantum noise in an optical fiber. *Phys. Rev. Lett.*, 57:691–694, Aug 1986.

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

[190] Ch. Silberhorn, N. Korolkova, and G. Leuchs. Quantum key distribution with bright entangled beams. *Phys. Rev. Lett.*, 88:167902, Apr 2002.

[191] Ch. Silberhorn, P. K. Lam, O. Weiß, F. König, N. Korolkova, and G. Leuchs. "generation of continuous variable Einstein-Podolsky-Rosen entanglement via the Kerr nonlinearity in an optical fiber". *Phys. Rev. Lett.*, 86:4267–4270, May 2001.

[192] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs. Continuous variable quantum cryptography: Beating the 3 db loss limit. *Phys. Rev. Lett.*, 89:167901, Sep 2002.

[193] R. Simon. Peres-Horodecki Separability Criterion for Continuous Variable Systems. *Phys. Rev. Lett.*, 84:2726–2729, Mar 2000.

[194] R. Simon, N. Mukunda, and B. Dutta. Quantum-noise matrix for multimode systems: U(n) invariance, squeezing, and normal forms. *Phys. Rev. A*, 49:1567–1583, Mar 1994.

[195] M. S. Stefszky, C. M. Mow-Lowry, S. S. Y Chua, D. A. Shaddock, B. C. Buchler, H. Vahlbruch, A. Khalaidovski, R. Schnabel, P. K. Lam, and D. E. McClelland. Balanced homodyne detection of optical quantum states at audio-band frequencies and below. *Classical and Quantum Gravity*, 29(14):145015, July 2012.

[196] G. G. Stokes. On the composition and resolution of streams of polarized light from different sources. *Trans. Cambridge Phil. Soc.*, 9:399, 1852.

[197] A. Streltsov, H. Kampermann, and D. Bruß. Behavior of Quantum Correlations under Local Noise. *Physical Review Letters*, 107(17):170502, October 2011.

[198] A. Streltsov, H. Kampermann, and D. Bruß. Quantum cost for sending entanglement. *Phys. Rev. Lett.*, 108:250501, Jun 2012.

[199] E. C. J. Sudarshan. Equivalence of semiclassical and quantum mechanical descriptions of statistical light beams. *Phys. Rev. Lett.*, 10:277, 1963.

[200] C. M. Swanson and D. R. Stinson. *Information Theoretic Security: 5th International Conference, ICITS 2011, Amsterdam, The Netherlands, May 21-24, 2011. Proceedings*, chapter Unconditionally Secure Signature Schemes Revisited, pages 100–116. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[201] D. Sych and G. Leuchs. Coherent state quantum key distribution with multi letter phase-shift keying. *New Journal of Physics*, 12(5):053019, May 2010.

[202] R. Tatham and N. Korolkova. Quantum discord from system-environment correlations. *Physica Scripta Volume T*, 160(1):014040, April 2014.

[203] B. M. Terhal and K. G. H. Vollbrecht. Entanglement of formation for isotropic states. *Phys. Rev. Lett.*, 85:2625–2628, Sep 2000.

[204] J. D. Trimmer. The present situation in quantum mechanics: a translation of Schrödinger's "Cat Paradox" paper. *Proceedings of the American Philisophical Society*, 124(323), 1980.

[205] P. van Loock and S. L. Braunstein. Multipartite Entanglement for Continuous Variables: A Quantum Teleportation Network. *Physical Review Letters*, 84:3482–3485, April 2000.

[206] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight. Quantifying entanglement. *Phys. Rev. Lett.*, 78:2275–2279, Mar 1997.

[207] F. Verstraete, J. Dehaene, and B. DeMoor. Local filtering operations on two qubits. *Phys. Rev. A*, 64:010101, Jun 2001.

[208] F. Verstraete, M. M. Wolf, and J. I. Cirac. Quantum computation, quantum state engineering, and quantum phase transitions driven by dissipation. *ArXiv e-prints*, March 2008.

[209] G. Vidal and R. F. Werner. Computable measure of entanglement. *Phys. Rev. A*, 65:032314, Feb 2002.

[210] U. Vogl, R. T. Glasser, Q. Glorieux, J. B. Clark, N. V. Corzo, and P. D. Lett. Experimental characterization of Gaussian quantum discord generated by four-wave mixing. *Phys. Rev. A*, 87:010101, Jan 2013.

[211] K. G. H. Vollbrecht and R. F. Werner. Entanglement measures under symmetry. *Phys. Rev. A*, 64:062307, Nov 2001.

[212] C. E. Vollmer, D. Schulze, T. Eberle, V. Händchen, J. Fiurášek, and R. Schnabel. Experimental Entanglement Distribution by Separable States. *Physical Review Letters*, 111(23):230505, December 2013.

[213] N.G. Walker and J.E. Carroll. Simultaneous phase and amplitude measurements on optical signals using a multiport junction. *Electronics Letters*, 20(23):981–983, November 1984.

[214] P. Wallden, V. Dunjko, and E. Andersson. Minimum-cost quantum measurements for quantum information. *Journal of Physics A Mathematical General*, 47(12):125303, March 2014.

[215] P. Wallden, V. Dunjko, A. Kent, and E. Andersson. Quantum digital signatures with quantum-key-distribution components. *Phys. Rev. A*, 91(4):042304, April 2015.

[216] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621–669, May 2012.

[217] C. Weedbrook, S. Pirandola, J. Thompson, V. Vedral, and M. Gu. Discord Empowered Quantum Illumination. *ArXiv e-prints*, December 2013.

[218] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277–4281, Oct 1989.

[219] R. F. Werner and M. M. Wolf. Bound Entangled Gaussian States. *Phys. Rev. Lett.*, 86:3658–3661, Apr 2001.

[220] E. Wigner. On the quantum correction for thermodynamic equilibrium. *Physical Review*, 177:1857, 1969.

[221] M. M. Wilde. From Classical to Quantum Shannon Theory. *ArXiv e-prints*, June 2011.

[222] J. Williamson. On the algebraic problem concerning the normal forms of linear dynamical systems. *American Journal of Mathematics*, 58(1):141–163, 1936.

[223] M. M. Wolf, J. Eisert, and M. B. Plenio. Entangling power of passive optical elements. *Phys. Rev. Lett.*, 90:047904, Jan 2003.

[224] M. M. Wolf, G. Giedke, O. Krüger, R. F. Werner, and J. I. Cirac. Gaussian entanglement of formation. *Phys. Rev. A*, 69:052320, May 2004.

[225] W. K. Wootters. Entanglement of Formation of an Arbitrary State of Two Qubits. *Physical Review Letters*, 80:2245–2248, March 1998.

[226] W. Xiang-bin. Theorem for the beam-splitter entangler. *Phys. Rev. A*, 66:024303, Aug 2002.

[227] Y. Yamamoto and H. A. Haus. Preparation, measurement and information capacity of optical quantum states. *Rev. Mod. Phys.*, 58:1001–1020, Oct 1986.

[228] H. P. Yuen and V. W. S. Chan. Noise in homodyne and heterodyne detection. *Opt. Lett.*, 8(3):177–179, Mar 1983.

[229] H. P. Yuen and J. H. Shapiro. Optical communication with two-photon coherent states–part iii: Quantum measurements realizable with photoemissive detectors. *Information Theory, IEEE Transactions on*, 26(1):78–92, Jan 1980.