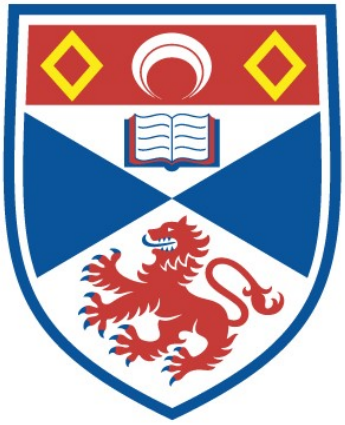
AGILE QUANTUM CRYPTOGRAPHY AND NON-CLASSICAL STATE GENERATION

Matthew Thornton

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



2020

Agile quantum cryptography and non-classical state generation

Matthew Thornton

University of
St Andrews

This thesis is submitted in partial fulfilment for the degree of

Doctor of Philosophy (PhD)

at the University of St Andrews

March 2020

Candidate's declaration

I, Matthew Thornton, do hereby certify that this thesis, submitted for the degree of PhD, which is approximately 72,000 words in length, has been written by me, and that it is the record of work carried out by me, or principally by myself in collaboration with others as acknowledged, and that it has not been submitted in any previous application for any degree.

I was admitted as a research student at the University of St Andrews in September 2016.

I received funding from an organisation or institution and have acknowledged the funder(s) in the full text of my thesis.

Date 26th October 2020 Signature of candidate

Supervisor's declaration

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

Permission for publication

In submitting this thesis to the University of St Andrews we understand that we are 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. We also understand, unless exempt by an award of an embargo as requested below, 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 this thesis will be electronically accessible for personal or research use and that the library has the right to migrate this thesis into new electronic forms as required to ensure continued access to the thesis.

I, Matthew Thornton, confirm that my thesis does not contain any third-party material that requires copyright clearance.

The following is an agreed request by candidate and supervisor regarding the publication of this thesis:

Printed copy

No embargo on print copy.

Electronic copy

No embargo on electronic copy.

Date 26th October 2020 Signature of candidate

Date Signature of supervisor

Underpinning Research Data or Digital Outputs

Candidate's declaration

I, Matthew Thornton, understand that by declaring that I have original research data or digital outputs, I should make every effort in meeting the University's and research funders' requirements on the deposit and sharing of research data or research digital outputs.

Date 26th October 2020 Signature of candidate

Permission for publication of underpinning research data or digital outputs

We understand that for any original research data or digital outputs which are deposited, we are giving permission for them to be made available for use in accordance with the requirements of the University and research funders, for the time being in force.

We also understand that the title and the description will be published, and that the underpinning research data or digital outputs will be electronically accessible for use in accordance with the license specified at the point of deposit, unless exempt by award of an embargo as requested below.

The following is an agreed request by candidate and supervisor regarding the publication of underpinning research data or digital outputs:

No embargo on underpinning research data or digital outputs.

Date 26th October 2020 Signature of candidate

Date Signature of supervisor

PUBLICATIONS

The following publications have resulted from the research contained in this Thesis:

M. Thornton, H. Scott, C. Croal and N. Korolkova:
Continuous-variable quantum digital signatures over insecure quantum channels,
Physical Review A **99**, 032341, (2019).

M. Thornton, A. Sakovich, A. Mikhalychev, J. D. Ferrer, P. de la Hoz, N. Korolkova and D. Mogilevtsev:
Coherent diffusive photon gun for generating nonclassical states,
Physical Review Applied **12**, 064051, (2019).

S. Richter, M. Thornton, I. Khan, H. Scott, K. Jaksch, U. Vogl, B. Stiller, G. Leuchs, C. Marquardt and N. Korolkova:
Agile quantum communication: signatures and secrets,
arXiv:2001.10089 [quant-ph].

CONFERENCE PRESENTATIONS

I have had the privilege to present at the following conferences:

1. QCrypt 2016, Washington DC, USA. Poster presentation: "Continuous variable quantum digital signatures."
2. 6th International Conference on New Frontiers in Physics (ICNFP 2017), Kolymbari, Crete. Oral presentation: "Gigahertz quantum signatures compatible with telecommunication technologies."
3. QCrypt 2017, Cambridge, UK. Poster presentation: "Gigahertz quantum signatures compatible with telecommunication technologies."
4. WE-Heraeus-Seminar on "Quantum Correlations in Space and Time," 2017, Bad Honnef, Germany. Poster presentation: "Gigahertz quantum signatures compatible with telecommunication technologies."
5. 25th Central European Workshop on Quantum Optics (CEWQO 2018), Palma de Mallorca, Spain. Poster presentation: "Gigahertz quantum signatures compatible with telecommunication technologies."
6. 24th Young Atom Opticians (YAO 2018), Glasgow, Scotland. Poster presentation: "Coherent quantum networks for non-classical state generation."
7. Quantum Roundabout 2018, Nottingham, UK. Poster presentation: "Efficient generation of sub-Poissonian light via coherent diffusive photonics."
8. 1st European Quantum Technologies Conference (EQTC 2019), Grenoble, France. Poster presentation: "Efficient generation of sub-Poissonian light via coherent diffusive photonics."
9. ICQOQI 2019, Minsk, Belarus. Oral presentation: "Continuous-variable quantum digital signatures over insecure channels."
10. Quantum Information Scotland (QUISCO) September 2019, St Andrews, Scotland. Oral presentation: "Agile quantum communication: quantum signatures and quantum secrets."

COLLABORATION STATEMENT

This Thesis is the result of work which I carried out at the University of St Andrews between September 2016 and March 2020. Much of the work contained here has been published in (or submitted to) refereed scientific journals. All text in this Thesis has been written entirely by me. Unless otherwise stated, all figures have been created entirely by me.

Content in Chapter 3 and Appendix C is also contained in M. Thornton *et. al.*, Phys. Rev. A **99**, 032341 (2019). Theoretical work was conducted in collaboration with H. Scott. All numerics used to generate results and figures in Ch. 3 were created by me.

Chapters 4 and 5 are extensions of work contained in S. Richter *et. al.*, arXiv:2001.10089 [quant-ph]. The original ideas and framework underpinning Ch. 5 were formulated during discussions I partook in at the Max-Planck-Institute für die Physik des Lichts (MPL) in Erlangen, Germany in May 2017. The work was completed in collaboration with S. Richter, I. Khan and C. Marquardt. My contribution was the theoretical analysis and security proofs which underpin the chapters, while the experiment discussed in Sec. 5.5 was performed at MPL by S. Richter and I. Khan, with assistance from K. Jaksch, U. Vogl, B. Stiller, G. Leuchs and C. Marquardt. I analysed experimental data with additional assistance from S. Richter and I. Khan.

Chapter 6 is an expansion on content contained in M. Thornton *et. al.*, Phys. Rev. Applied **12**, 064051, (2019). N. Korolkova and D. Mogilevtsev provided the direction and original ideas for the work. The work contained in Ch. 6 was carried out by myself in collaboration with D. Mogilevtsev and P. de la Hoz, and with assistance from A. Sakovich for the numerics.

All work in this Thesis has been supported by my supervisor, Professor N. Korolkova.

In the first half of this Thesis, we introduce a framework of "quantum cryptographic agility," which allows for a resource-efficient swap of an underlying cryptographic protocol. Specifically, we introduce several schemes which perform the tasks of Digital Signatures and Secret Sharing. Our first achievement is an investigation of Quantum Digital Signatures (QDS) over a continuous-variables platform, consisting of phase-encoded coherent states and heterodyne phase detection. QDS allows for secure authentication of a classical message, while guaranteeing message transferability. For the first time, we prove security of CV QDS in the presence of an eavesdropper on the quantum channels.

We then introduce a continuous variable (CV) Quantum Secret Sharing (QSS) protocol. Our security proof allows for classical information to be split and shared between multiple potentially dishonest recipients, while retaining security against collective beamsplitter and entangling-cloner attacks. In the last chapter of this half, we introduce another QDS scheme which runs over identical hardware setup to our QSS protocol. We analyse experimental data in which quantum coherent states were distributed at a rate of 1 GHz, which for QDS allows us to securely sign a message in less than 0.05 ms.

In the second half of this Thesis we suggest and discuss a deterministic source of nonclassical light, which we call "PhoG". Our source is based on the coherent diffusive photonics, relying on both coherent and dissipative evolution of the quantum state, and may be realised in an array of dissipatively-coupled laser-inscribed waveguides in a $\chi^{(3)}$ glass. We analyse the PhoG device with several analytical and numerical models and demonstrate that a coherent state input leads to a bright output state with strong photon-number squeezing. With minor reconfiguration our system can generate entangelement between spatially separated modes via a process analogous to four-wave mixing.

General acknowledgements

I would like to first thank my supervisor, Professor Natalia Korolkova, for her support and help over the past four years. My PhD has been fun, long, thrilling, difficult, enjoyable, frustrating, brilliant and always sinusoidal, and I am grateful to Natalia for her guidance and help in navigating each of these aspects. I should thank the many colleagues (and now friends) within the School of Physics and Astronomy who have contributed fun conversation and probing questions, and who have helped make the last four years so much fun. I have deeply appreciated these opportunities to grow in self-management and self-leadership, in scientific ability, in public speaking, in teaching, in writing, and in understanding and appreciation for our wonderful universe. Thank you to every undergraduate student I have taught or interacted with - you have reminded me that “yes I actually do quite enjoy physics, let me tell you why”. Thanks, Anton, for helping me understand Mathematica and Git. Thank you also to Hamish, to Jesús and to Cailean for giving me the privilege to work with you and explore fun aspects of quantum physics. I enjoyed it and I hope you did too.

I acknowledge deep support from my family. Thanks for listening to me trying to explain my research time and time again, and thanks especially to my parents for instilling in me a love and an appreciation for science and mathematics. I am grateful to Dad for convincing me to pursue physics (instead of Chemistry), and to both Mum and Dad for working so hard to support me financially through my first degree, and emotionally during this one. And thanks to my siblings Peter, Naomi, Annalise, Abigail and Andy for many years of friendship and encouragement.

I could not have survived without a little help from my friends. I am grateful, in particular, to those at St Andrews Baptist Church, who have put up with my potent combination of too-little-sleep and too-much-coffee for the last nine years. You have reminded me that there are bigger things to focus on and enjoy than the PhD, and more important places to find my self-worth and satisfaction than in my own productivity and scientific output. Thank you to Jesus for making (quantum) light in the first place. Thanks to everyone in the “Commune”. Thanks especially to James and Belinda, David, Daffyd, Jordan and Tamara, Emily, Gavin, the Milkman, the Irregulars, and so many more. I should say “thank you” to Andrew Rollinson for encouraging me towards a PhD in the first place (though he's probably forgotten about it) and say “hello” to Jason Isaacs.

Finally, I am deeply indebted for the love and support I have received from my wife Hannah. She has encouraged me when the PhD has just been plain annoying and rejoiced with me when it has just been plain brilliant. Thank you for allowing me to lock myself away to write for the last few months, and for being a source of fun, food and caffeine for the last few years.

Funding

This work was supported by the EPSRC [grant number 1798331].

Research Data/Digital Outputs access statement

Research data underpinning this thesis are available at https://doi.org/10.17630/6ba10862-4bdd-478f-8bd7-4f4b4d383374

CONTENTS

1 INTRODUCTION

1.1 INTRODUCTION TO THESIS

This Thesis consists of two halves. In the first half, we consider several related cryptographic protocols which securely perform the tasks of Quantum Digital Signatures (QDS) and Quantum Secret Sharing (QSS). Our goals here are, firstly: to remove an assumption of secure quantum channels from continuous-variable (CV) QDS, and provide a security proof when an eavesdropping attack is permitted; and secondly: to demonstrate that several CV quantum cryptographic protocols may be performed over identical hardware setups, while the hardware at the quantum level is agnostic to the protocol being implemented. This so-called "agile" approach illustrates a translation of cryptographic agility from classical (conventional) cryptography to quantum cryptography, and allows for a move towards secure and practical quantum cryptosystems which can perform multiple tasks.

In the second half we consider the task of quantum state generation. We design and analyse a system which is capable to deterministically produce highly non-classical states at the output, from a coherent state input. Using methods from the fields of nonlinear pulse propagation in fibers and of open quantum systems, we analytically and numerically analyse a large multimode system and reduce it, step-by-step, to a single-mode system which is much more numerically tangible. The device, which we denote PhoG (Photon Gun), will soon be implemented in a waveguide array structure and will provide a practical and cheap source of nonclassicality for quantum enhanced imaging and metrology, and may even improve the performance of quantum cryptographic systems.

The two halves of this thesis can be interpreted as studying different aspects of quantum networked systems, in which both the individual systems, and the geometry of coupling between them, play an important role. The first half considers quantum communications networks and cryptographic tasks which are inherently multipartite. By studying the simplest networks of just three players (in two different configurations) we move towards cryptosystems which can be implemented entirely agnostic to the network structure. In the second half we consider large structures of waveguide arrays, where the dynamics are intimately connected to the underlying geometry. We focus on quantum correlation flow and coherent signal propagation in this device of connected bosonic modes, which will soon be created in laser-inscribed waveguides.

Detailed overview

This Thesis is structured as follows. In the remainder of this Chapter we will introduce and outline several of the theoretical and analytical tools which we make extensive use of in the rest of the Thesis. We will show how the electromagnetic field may be quantized, discuss several common and useful quantum states of the field, and examine some methods for their description and visualization. In Chapter 2 we outline some of the developments in conventional cryptography which underpin our modern communications infrastructure, and discuss how two cryptographic tasks – digital signatures and secret sharing – may be translated to the quantum realm. In particular we will look at several recent and historic attempts to build such quantum protocols.

PART ONE: In Chapter 3 we introduce our own QDS protocol, and prove its security against several classes of attack. Ours is the first CV QDS protocol to allow for an eavesdropper on the channels, and we show that despite this we attain very short signature lengths over practical distances. In Chapter 4 we introduce our QSS protocol, prove its security, and analyse its performance. Crucially, unlike several recent QSS protocols, our protocol does not require generation and distribution of large-scale entangled states, nor does it require dedicated hardware for a sequential "round-robin" style of approach. In the last chapter of Part One, Chapter 5, we introduce and discuss the concept of quantum cryptographic agility, and demonstrate how it may apply to the protocols discussed in earlier chapters. We additionally introduce a new QDS protocol which runs in a modified configuration, and discuss how a quantum key distribution (QKD) protocol which already exists in the literature may be adopted into our agile system. We finish with a figure-of-merit graph which demonstrates that our QDS scheme, in addition to being practical and compatible with commercial telecommunications hardware, is also the fastest QDS protocol over comparable distances.

PART TWO: In Chapter 6 we motivate and introduce the PhoG device which will be the focus of the second half of this Thesis. We demonstrate that dissipation, far from being a hindrance to the desired evolution of our quantum system, is actually an asset and the main driver towards target nonclassicality. We introduce an exotic form of dissipation, called Nonlinear Coherent Loss, and show that in the ideal limit it will deterministically lead to single photons at the output. We then introduce progressively more complex models involving additional bosonic system modes, and demonstrate that a realistic full multi-mode model of the system can be used to effectively simulate the Nonlinear Coherent Loss decay channel. Finally, we end the chapter by demonstrating that in addition to generating highly sub-Poissonian

states, a slight modification to the PhoG device will lead to generation of entanglement at the output.

PART THREE: We finish the Thesis with the inclusion of several appendices containing results which are used at multiple points throughout the Thesis. Appendix A contains results describing the output state of a channel in which an initial coherent state is mixed with thermal noise. This result is used multiple times throughout Part One. Appendix B contains the forms of quantum states which are used under various channel attacks in Chapter 3, and a description of how the states may be numerically modelled. Appendix C contains a generalization of the QDS protocol from Chapter 3 to allow for larger alphabets of coherent states. Appendix D provides a tool which is used multiple times in Chapter 6 to reduce the complexity of a model by effectively ignoring a mode which reaches its steady state much quicker than the typical decay time of the system. Finally, in Appendix E we describe several numerical methods which may be applied to model the PhoG device. We compare them for speed, memory usage and accuracy, and then explicitly display several systems of coupled differential equations which approximate the PhoG device.

1.2 INTRODUCTION TO QUANTUM PHYSICS

In this Thesis we are primarily interested in the quantum properties of single- or few- mode states of light. This Chapter will serve as a short introduction to several of the key concepts which we deal with, and some of their main properties. We first introduce the state vector and density matrix formalisms for description of quantum modes, in which the physical state is completely described by sums and outer products of vectors chosen from a countably infinite Hilbert space. We introduce single-mode operators and several single-mode states, and visualise them using a quantum analogue of a classical phase-space probability distribution known as the Wigner function. Multi-mode quantum states are introduced as states on larger vector spaces which are formed via a tensor product operation.

We introduce a third description of the quantum state which captures the second moments (co-variances) of multi-mode states, the so-called covariance matrix. This allows for a complete description of properties of a state which is Gaussian in phase-space, otherwise it offers a partial description which is nonetheless useful.

Evolution of the quantum state is described by the von Neumann equation (no dissipation) or the Lindblad master equation (including dissipation). The latter allows for us to model the dynamics of a few modes chosen from much larger multi-mode system, provided that the two are weakly coupled and the larger system (environment/reservoir) is effectively unchanged by the system evolution.

Finally, we display several selected entropic and probabilistic relations and quantities which we use in this Thesis. In particular, the notion of conditional probability, and the intimately related Bayes' theorem, will prove useful both as helpful quantities in their own right, and as foundational building blocks for conditional classical and quantum entropies.

1.2.1 *State vectors and density matrices*

An ideal quantum state is denoted in the Dirac notation by $|\psi\rangle$. This state has been perfectly prepared with no noise, loss, or additional uncertainty due to the preparation. The $|\psi\rangle$ is a vector living in a vector space denoted $\mathcal{H}$, which we call a Hilbert space. The space has dimension $|\mathcal{H}|$, typically taken to be countably infinite, but there will be several points in this Thesis where we consider a finite $|\mathcal{H}|$.

Since $|\psi\rangle$ is a vector it can be written in terms of a set $\{|e_j\rangle\}$ of basis vectors,

$$|\psi\rangle = \sum_j c_j |e_j\rangle , \tag{1.1}$$

where the number of basis vectors typically equals $|\mathcal{H}|$.

The state $|\psi\rangle$ should be normalized, that is

$$\langle\psi|\psi\rangle = 1. \tag{1.2}$$

The notation $\langle\psi|\psi\rangle$ means

$$\sum_j |c_j|^2 . \tag{1.3}$$

We define an eigenstate of an arbitrary quantum operator $\hat{r}$ to be the state $|r\rangle$ such that

$$\hat{r}|r\rangle = r|r\rangle \tag{1.4}$$

with eigenvalue $r \in \mathbb{C}$.

The basis we choose for vector $|\psi\rangle$ is not unique and we may similarly have expanded $|\psi\rangle$ in terms of eigenstates of $\hat{r}$, as

$$|\psi\rangle = \sum_j |r\rangle \langle r|\psi\rangle , \tag{1.5}$$

where the $\langle r|\psi\rangle \in \mathbb{C}$ is such that its square modulus $|\langle r|\psi\rangle|^2$ is the probability that a measurement of r on $|\psi\rangle$ will give outcome r.

For convenience any basis vectors we use are chosen to be orthonormal, that is

$$\langle \hat{e}_j | \hat{e}_k \rangle = \delta_{j,k} \tag{1.6}$$

where $\delta_{j,k}$ is the Kronecker δ function.

The fact that a state $|\psi\rangle$ may be written as a sum of basis vectors corresponding to different possible measurement outcomes is a curious one, and is a key feature of quantum mechanics known as the *superposition principle*. A superposition state is one of the form

$$|\psi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{1.7}$$

where the constant factor $1/\sqrt{2}$ ensures normalization. We have chosen an abstract orthonormal basis set $\{|0\rangle, |1\rangle\}$, and here $|\mathcal{H}| = 2$. The superposition state possesses a fundamental uncertainty about its measurement outcomes, that is to say, if many identical copies of $|\psi\rangle$ are created, and on each copy a measurement which distinguishes between $|0\rangle$ and $|1\rangle$ is performed, then the measurement will output 0 half of the time, and 1 the other half of the time. If, however, we are able to perform a measurement which distinguishes between $(|0\rangle \pm |1\rangle)/\sqrt{2}$, then we will find the output $(|0\rangle + |1\rangle)/\sqrt{2}$ 100% of the time. This is markedly different from a statistical mixture, involving classical ignorance about whether the state is $|0\rangle$ or $|1\rangle$.

The density operator corresponding to a quantum state is

$$\hat{\rho} = \sum_{i,j} p_{i,j} |i\rangle\langle j| \tag{1.8}$$

where $\langle i| \in \mathcal{H}^*$ is dual to $|i\rangle$ ($\mathcal{H}^*$ is the dual space to $\mathcal{H}$). We shall often use the terms *density operator* and *density matrix* interchangeably.

Any state vector $|\psi\rangle$ can be described as a density operator. For example, the state $|\psi\rangle$ in Eq. 1.7 may equivalently be described as

$$\rho_\psi = |\psi\rangle\langle\psi| = \frac{1}{2}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|). \tag{1.9}$$

However, there are density operators which do not correspond to a state vector. For example, there exists no vector $|\phi\rangle$ such that

$$\rho_\varphi := \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = |\phi\rangle\langle\phi|. \tag{1.10}$$

The density operator formalism may be interpreted as encoding two distinct forms of uncertainty: quantum and classical. The quantum uncertainty arises from states which may be written as superposition state vectors, while the classical uncertainty arises from states which cannot. We refer to the first type of summation as superposition, and the second type of summation as classical mixing (or a statistical mixture). The classical mixing represents classical uncertainty about which state the system is in, and may in principle be removed by building better equipment.

In the $\{|0\rangle, |1\rangle\}$ basis, these states ρ_ψ and ρ_φ may be written as

$$\rho_\psi = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad \rho_\varphi = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{1.11}$$

The quantum nature of a state ρ is therefore intimately connected to the off-diagonal elements of its density matrix, which are often referred to as *coherences*. The density matrix ρ will be our primary tool for describing a quantum state in this Thesis.

1.2.2 *Introduction to quantum optics*

In the absence of currents or charge, classical electromagnetic fields obey Maxwell's equations:

$$\nabla \cdot \boldsymbol{B} = 0, \qquad \nabla \times \boldsymbol{E} = -\frac{\partial \boldsymbol{B}}{\partial t}, \qquad \nabla \cdot \boldsymbol{D} = 0 \quad \text{and} \quad \nabla \times \boldsymbol{H} = \frac{\partial \boldsymbol{D}}{\partial t}.$$

We may quantize these electric and magnetic fields by replacing the vectors $\boldsymbol{B}, \boldsymbol{E}, \boldsymbol{D}, \boldsymbol{H}$ with the corresponding operators $\hat{\boldsymbol{B}}, \hat{\boldsymbol{E}}, \hat{\boldsymbol{D}}, \hat{\boldsymbol{H}}$, and imposing that the classical fields should be regarded as expected values of these quantum operators:

$$\boldsymbol{E} = \langle \psi | \hat{\boldsymbol{E}} | \psi \rangle \quad \text{etc.} \tag{1.12}$$

By analogy with the classical vector potential, let us introduce the quantum vector potential $\hat{\boldsymbol{A}}$, and impose

$$\hat{\boldsymbol{E}} = -\frac{\partial \hat{\boldsymbol{A}}}{\partial t}, \qquad \hat{\boldsymbol{B}} = \nabla \times \hat{\boldsymbol{A}}, \quad \text{and} \quad \nabla \cdot \hat{\boldsymbol{A}} = 0. \tag{1.13}$$

As in classical electromagnetism, the first two of these requirements automatically imply that the first two of Maxwell's equations are satisfied, while the third requirement ("coulomb gauge") is merely a convenient choice which immediately satisfies the third Maxwell equation[1]. The final Maxwell equation is then equivalent to the following wave equation

$$\epsilon^{-1}\mu^{-1}\nabla \times \nabla \times \hat{\boldsymbol{A}} = -c^{-2}\frac{\partial^2 \hat{\boldsymbol{A}}}{\partial t^2}. \tag{1.14}$$

These equations contain all of the same information as Maxwell's equations, just involving the quantized vector potential. This $\hat{\boldsymbol{A}}$ contains all information about our light wave.

The Hamiltonian of our electromagnetic field takes the same form as the classical total energy, i.e.

$$\hat{H} = \int_V d^3V \, \frac{\hat{\boldsymbol{E}} \cdot \hat{\boldsymbol{D}} + \hat{\boldsymbol{B}} \cdot \hat{\boldsymbol{H}}}{2}. \tag{1.15}$$

1 Since light in linear media behaves as $\hat{\boldsymbol{D}} = \epsilon_0 \epsilon \hat{\boldsymbol{E}}$, where ϵ_0 is the vacuum permittivity and ϵ is the electric permittivity of the medium in question. The other "constitutive equation" is $\hat{\boldsymbol{H}} = \mu_0^{-1}\mu^{-1}\hat{\boldsymbol{B}}$, for permeability μ of the medium, and vacuum permeability μ_0.

The electromagnetic wave equation, Eq. 1.14, is a linear differential equation, and so we may sum any two solutions together to form a new solution. Let us define a set of monochromatic classical waves

$$\boldsymbol{A}_j\left(\overrightarrow{r},t\right)=\boldsymbol{A}_j\left(\overrightarrow{r}\right)\exp^{-i\omega_j t} \tag{1.16}$$

oscillating at frequency ω_j. We have assumed that the temporal and spatial aspects of the wave can be separated, and let the vector $\boldsymbol{A}_j\left(\overrightarrow{r}\right)$ contain all spatial information. We expand the quantum vector potential $\hat{\boldsymbol{A}}$ as

$$\hat{\boldsymbol{A}}\left(\overrightarrow{r},t\right)=\sum_k\left[\boldsymbol{A}_j\left(\overrightarrow{r},t\right)\hat{a}_j+\boldsymbol{A}_j^*\left(\overrightarrow{r},t\right)\hat{a}_j^\dagger\right], \tag{1.17}$$

where we have introduced single-mode quantum operators $\hat{a}_j, \hat{a}_j^\dagger$.

Substituting this $\hat{\boldsymbol{A}}\left(\overrightarrow{r},t\right)$, expanded in a basis of monochromatic waves, into the Hamiltonian Eq. 1.15, we arrive at

$$\hat{H}=\sum_j\hbar\omega_j\left(\hat{a}_j^\dagger\hat{a}_j+\frac{1}{2}\right), \tag{1.18}$$

where we have used the commutator $\left[\hat{a}_j\hat{a}_k^\dagger\right]=\delta_{j,k}$. We are thus led to identify the $\hat{a}_j, \hat{a}_j^\dagger$ as the raising and lowering operators of a simple harmonic oscillator which obeys the Hamiltonian Eq. 1.18.

We have effectively split the full quantum description of light into two parts, classical and quantum. The classical quantities $\boldsymbol{A}_j\left(\overrightarrow{r},t\right)$ fully describe all wave properties of the light, while the quantum operators $\hat{a}_j$ describe the quanta present in a single mode. For this Thesis we will focus on these quantum systems and ignore the wave nature of light. That is to say, we will regard the mode operators $\hat{a}_j$ as accurately describing the full system of interest, irrelevant of its classical properties. This proves to be a helpful distinction as it allows for us to make general quantum statements which are true for any bosonic system of quantum modes, regardless of their physical implementation.

In Sec. 6.8 we will briefly return to the classical $\boldsymbol{A}\left(\overrightarrow{r},t\right)$ in a $1+1$D system (one spatial dimension plus time). The $A\left(z,t\right)$ are discussed there in the context of light pulse propagation in waveguides where, with physical implementation in mind, we must pay great attention to the wave properties. We discuss there some methods to efficiently model such classical behaviour, and then mention as outlook several strategies which may be used to model the full propagation of a quantum pulse, taking into account both classical and quantum effects.

For a more detailed discussion of the derivation presented here, we refer the reader to the textbooks Refs. [1–3].

1.2.3 *Single-mode operators*

The bosonic operators $\hat{a}, \hat{a}^\dagger$ create and destroy a quantum of energy in the light mode. These operators obey the bosonic commutation relation

$$\left[\hat{a}, \hat{a}^\dagger\right] = 1, \tag{1.19}$$

and are crucial for modelling the quantum properties of our light.

We define the photon-number operator $\hat{n}$ as

$$\hat{n} = \hat{a}^\dagger \hat{a}, \tag{1.20}$$

which counts the number of photons in our mode. Letting ω denote the mode frequency, we may construct the following two operators

$$\hat{q} = \sqrt{\frac{\hbar}{2\omega}}\left(\hat{a}^\dagger + \hat{a}\right) \quad \text{and} \quad \hat{p} = i\sqrt{\frac{\hbar\omega}{2}}\left(\hat{a}^\dagger - \hat{a}\right) \tag{1.21}$$

which are known as the "quadrature operators", and can be shown to obey the commutator

$$[\hat{q}, \hat{p}] = i\hbar. \tag{1.22}$$

The quadrature operators $\hat{q}$ and $\hat{p}$ correspond to field amplitudes which are $\pi/2$ out of phase with each other. The annihilation operator can then be written

$$\hat{a} = \frac{1}{\sqrt{2\hbar\omega}}\left(\omega\hat{q} + i\hat{p}\right). \tag{1.23}$$

The quadrature operator for a general quadrature $\hat{q}_\theta$ is given by

$$\hat{q}_\theta = \hat{q}\cos\theta + \hat{p}\sin\theta, \tag{1.24}$$

and the operators $\hat{q}$, $\hat{p}$ are recovered as special cases with $\theta = 0$ and $\pi/2$, respectively. The quadrature operators $\hat{q}, \hat{p}$ may be used to write the well known Heisenberg uncertainty principle as

$$\mathrm{Var}\left(\hat{q}\right)\mathrm{Var}\left(\hat{p}\right) \geqslant \hbar^2/4, \tag{1.25}$$

where the variances in a general quantum state $|\psi\rangle$ are defined as

$$\begin{aligned}\mathrm{Var}\left(\hat{q}\right) &= \langle\psi|\hat{q}^2|\psi\rangle - \langle\psi|\hat{q}|\psi\rangle^2, \\ \mathrm{Var}\left(\hat{p}\right) &= \langle\psi|\hat{p}^2|\psi\rangle - \langle\psi|\hat{p}|\psi\rangle^2.\end{aligned} \tag{1.26}$$

The uncertainty principle Eq. 1.25 implies that we cannot simultaneously measure $\hat{q}$ and $\hat{p}$ with arbitrary precision - in other words q and p are conjugate variables.

The $\langle\psi|\hat{q}|\psi\rangle$ denote the expectation value of $\hat{q}$ in state $|\psi\rangle$. We may equivalently write this as $\langle\hat{q}\rangle_\psi$, or simply just $\langle\hat{q}\rangle$ when the corresponding state is obvious or irrelevant. The expectation value of an operator corresponds to the average measurement outcome when many measurements of that operator is performed on the given state.

The commutator Eq. 1.22 is equivalent to the commutator between operators which describe position and momentum of a quantum particle, and so we identify $\hat{q}$ as the position operator and $\hat{p}$ as the momentum operator (thus corroborating Eq. 1.25). Indeed, it is easy to show from the definitions that

$$\hat{H} = \omega^2 \frac{\hat{q}^2}{2} + \frac{\hat{p}^2}{2} = \hbar\omega \left(\hat{n} + \frac{1}{2} \right), \tag{1.27}$$

the middle terms of which describes the energy of a simple harmonic oscillator in what follows we will set $\hbar = 1$ for convenience.

1.2.4 *Wigner function*

An equivalent way to describe the quantum state ρ is to use a (*quasi*)-probability distribution known as the Wigner function. The Wigner function, $W(q,p)$, allows operator expectation values to be calculated using an averaging method similar to classical mechanics in phase space.

One immediate observation is that a *quantum phase space* must behave qualitatively very differently to the classical one. Because of Heisenberg's principle, we cannot accurately define a joint probability distribution of position q and momentum p as this would require precise knowledge of both quantities. This leads to interesting behaviours of the phase space "probability" distribution, such as becoming negative (for Wigner functions) or highly singular (for "P-functions"). Indeed, one may even measure the "quantumness" of a given state by checking for these properties.

We define the Wigner function corresponding to density operator $\hat{\rho}$ as [1]

$$W(q,p) = \frac{1}{2\pi} \int_{-\infty}^{\infty} dx \, \exp(ipx) \left\langle q - \frac{x}{2} \middle| \hat{\rho} \middle| q + \frac{x}{2} \right\rangle. \tag{1.28}$$

The marginal distributions of W are genuine probability distributions, and are given by tracing out the conjugate quadrature:

$$P(q) = \int_{-\infty}^{\infty} dp \, W(q,p) \quad \text{and} \quad P(p) = \int_{-\infty}^{\infty} dq \, W(q,p). \tag{1.29}$$

A useful feature of the Wigner function is that traces over operators may be calculated as

$$\mathrm{tr}\left[\hat{O}_1 \hat{O}_2\right] = 2\pi \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} dq \, dp \, W_1(q,p) \, W_2(q,p) \tag{1.30}$$

where $W_i(q,p)$ is the Wigner function corresponding to operator $\hat{O}_i$. Operator expectation values with respect a given state $\hat{\rho}$ may be calculated using Eq. 1.30.

The Heisenberg uncertainty relation further expresses itself in the Wigner function picture by imposing a minimum area which a quantum state must occupy. In the following sections we will see some examples of quantum states and their corresponding Wigner functions. In all plots of Wigner functions, the colour blue denotes $W(q,p) > 0$ while red denotes $W(q,p) < 0$. Negativity (red, in this Thesis) of the Wigner function is a clear sign that the underlying state is nonclassical[2].

Finally, we must note that the Wigner function is not the only quasi-probability distribution which one could define on the phase space, and because in general quantum operators do not commute there are multiple ways to consistently define a phase space description. Other common quasi-probability distributions are: the Hussimi Q function [4], which is intimately related to heterodyne measurement; Glauber-Sudarshan [5] P function, which is often used to describe mixtures of coherent states and becomes highly singular in all other cases; and the positive-P function, which is a generalization to the P function and is defined to be non-diagonal in the coherent state basis, and which allows quantum effects such as squeezing to be described [2]. One may also use these quasi-probability distributions to predict dynamics of the system using a Fokker-Planck diffusion equation [6], analogously to a classical stochastic process.

We use the Wigner function in Appendix A to simplify a calculation which is analytically difficult in the density matrix picture, and the Wigner functions offer an excellent visualization tool in the following few sections.

1.2.5 *Fock states*

Fock states (also called photon-number states) are defined as eigenstates of the photon-number operator $\hat{n} = \hat{a}^\dagger \hat{a}$:

$$\hat{n}\,|n\rangle = n\,|n\rangle\,. \tag{1.31}$$

In other words, $\hat{n}$ measures the number of photons in $|n\rangle$. The states have perfectly defined photon-number and find many applications in quantum information processing [7, 8]. The creation and annihilation operators $\hat{a}^\dagger, \hat{a}$ act on $|n\rangle$ as

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

2 Indeed, the only pure quantum states with non-negative Wigner functions are those with Gaussian Wigner function, i.e. the Glauber coherent states and the quadrature squeezed states.

The Fock states form an orthogonal basis for $\mathcal{H}$:

$$\langle m|n\rangle = \delta_{n,m}, \tag{1.32}$$

and so we will often seek an expansion of other states in the Fock-state basis. In particular, our density matrix ρ is written in a Fock state expansion as

$$\rho_{m,n} = \langle m|\hat{\rho}|n\rangle . \tag{1.33}$$

Wigner functions corresponding to some example Fock states are displayed in Fig. 1.1.

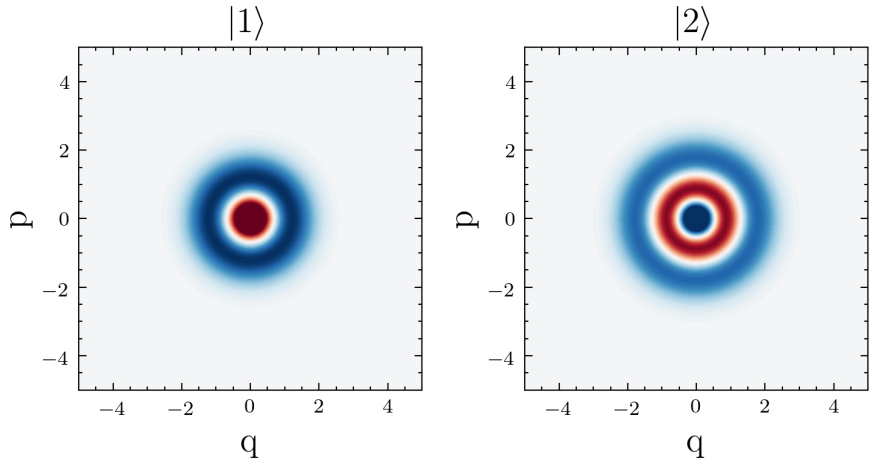


Figure 1.1: Wigner functions for Fock states $|1\rangle$ and $|2\rangle$. Blue signifies that the Wigner function is positive, while red signifies that the Wigner function is negative.

1.2.6 *Quadrature states*

We define the eigenstates of quadrature operators $\hat{q}$ and $\hat{p}$ as

$$\hat{q}\,|q\rangle = q\,|q\rangle \quad \text{and} \quad \hat{p}\,|p\rangle = p\,|p\rangle . \tag{1.34}$$

These $|q\rangle, |p\rangle$ are known as quadrature states. Although they are not normalizable, the quadrature states are a useful tool in quantum optics. For example, we will use them to describe ideal homodyne detection, Sec. 1.4.1, and they are also required for the definition of the Wigner function in Eq. 1.28.

1.2.7 *Coherent states*

Coherent states[3] are among the most important quantum states which we discuss in this Thesis. The coherent state $|\alpha\rangle$ is defined as the eigenstate of annihilation operator $\hat{a}$:

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle . \tag{1.35}$$

3 Also known as Glauber coherent states [5].

This coherent state has amplitude $\alpha \in \mathbb{C}$, and we display an example of a coherent state Wigner function in Fig. 1.2. It can be shown that the area occupied by the coherent state is the smallest allowable area of phase space for a Wigner function to cover. In other words, the coherent state saturates the Heisenberg bound and is a minimum uncertainty state.

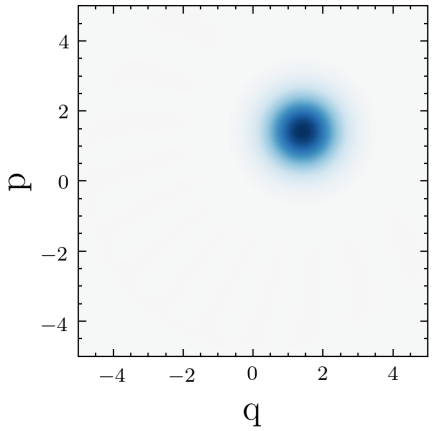


Figure 1.2: Wigner function for coherent state $|\alpha\rangle$ with $\alpha = 1 + 1i$.

The coherent states are non-orthogonal:

$$\langle\alpha|\beta\rangle = \exp\left(-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2} + \alpha^*\beta\right), \tag{1.36}$$

where α^* denotes the complex conjugate of α, and so we will regularly make use of an expansion of $|\alpha\rangle$ in the orthogonal Fock basis:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0} \frac{\alpha^n}{\sqrt{n!}} |n\rangle . \tag{1.37}$$

In the first part of this Thesis we will consider several quantum cryptographic protocols involving distribution of coherent states. We will regularly use an alphabet of coherent states known as the QPSK (Quadrature Phase-Shift Keying) alphabet,

$$\text{QPSK alphabet:} \quad \{|\alpha\rangle, |i\alpha\rangle, |-\alpha\rangle, |-i\alpha\rangle\}, \tag{1.38}$$

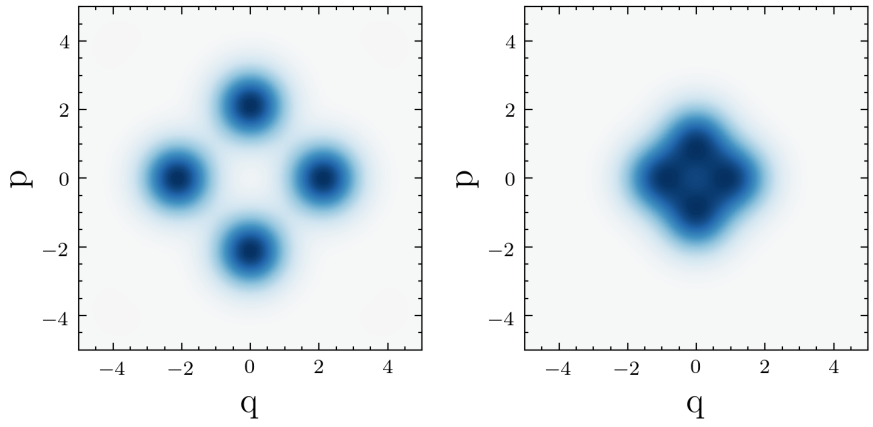
and we display a mixture over the QPSK alphabet in Fig. 1.3. We will not explicitly distinguish between whether we refer to the set of quantum states $\{|\alpha\rangle, |i\alpha\rangle, |-\alpha\rangle, |-i\alpha\rangle\}$ or the corresponding set of complex amplitudes $\{\alpha, i\alpha, -\alpha, -i\alpha\}$, since it should always be obvious which is meant.

A special case of the coherent states is that with eigenvalue 0,

$$\hat{a}\,|0\rangle = 0\,|0\rangle . \tag{1.39}$$

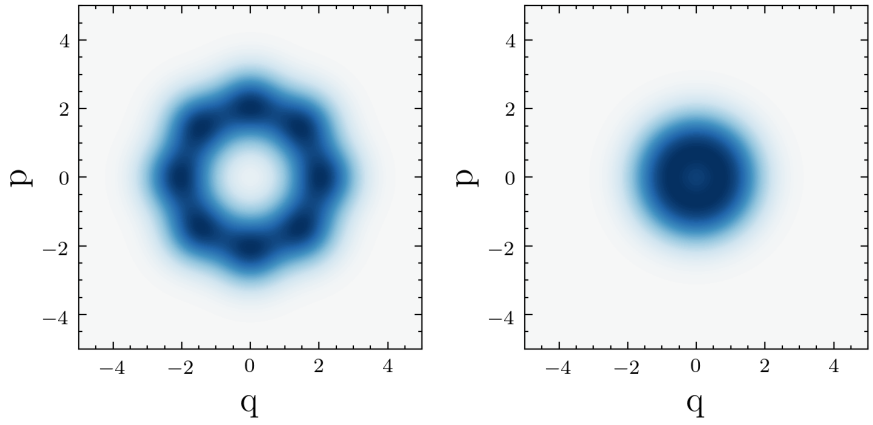
This state is known as the "vacuum" state, and is a special example of a quantum state, since $|0\rangle$ is also an eigenstate of $\hat{n}$, and is thus a Fock

state[4] with a photon number 0. The coherent state possesses the same uncertainty properties as the vacuum state.



(a) (b)

Figure 1.3: The Wigner function for a mixture over the QPSK alphabet is a sum of individual Wigner functions for each of the coherent states. QPSK alphabet with (a) $\alpha = 1.5$; (b) $\alpha = 0.8$.



(a) (b)

Figure 1.4: NPSK coherent state alphabet with $N = 8$. (a) $|\alpha| = 1.5$. (b) $|\alpha|$=0.8.

A generalization to QPSK is the so-called NPSK alphabet, in which N coherent states are chosen. The states are again equally distributed around the origin of phase space, and we note that QPSK is the special case $N = 4$. We display an example in Fig. 1.4.

1.2.8 *Thermal states*

The thermal state is defined as

$$\rho_{\text{thermal}} = \left(1 - e^{-\beta}\right) \sum_{n=0}^{\infty} e^{-n\beta} \, |n\rangle\langle n| \,, \tag{1.40}$$

4 It can also be viewed as a thermal state with $\bar{n} = 0$, c.f. Sec. 1.2.8.

with $\beta = (\hbar\omega)/(k_B T)$, reduced Planck's constant $\hbar$, angular frequency ω, Boltzmann's constant k_B and thermal equilibrium temperature T. As we see from the form of Eq. 1.40, the thermal state is a classical mixture of Fock states (c.f. Eq. 1.10). Typically we will parametrise the thermal state using the average thermal photon number $\bar{n}$, defined as

$$\bar{n} = \frac{1}{e^{\beta} - 1}, \tag{1.41}$$

which measures the average number of photons in the thermal state. We display the Wigner function of a thermal state in Fig. 1.5, where we have also displayed the vacuum state variance, for comparison.

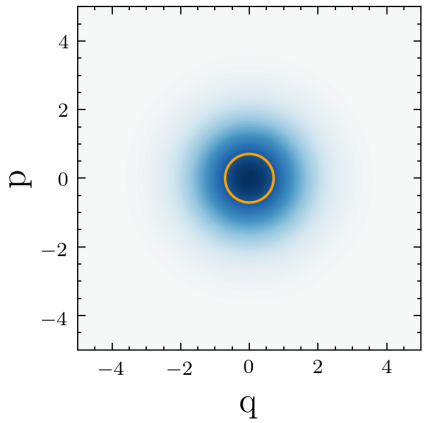


Figure 1.5: The thermal state Wigner function is Gaussian, with variance greater than the vacuum state variance, which is depicted in orange.

1.2.9 *Squeezed states (quadrature)*

We have already encountered the Heisenberg relation, which imposes a minimum phase space area which a state can occupy. The coherent state was a minimum uncertainty state and so occupied the minimum possible area while possessing symmetry: $\mathrm{Var}(\hat{q}) = \mathrm{Var}(\hat{p})$. Of course, it is possible to satisfy the Heisenberg relation while also taking $\mathrm{Var}(\hat{q}) \neq \mathrm{Var}(\hat{p})$, and this is precisely what (quadrature) squeezed states do. We display some examples of quadrature squeezed states in Fig. 1.6. In the limit of infinite squeezing one obtains quadrature states $|q\rangle$ and $|p\rangle$.

Quadrature squeezing is generated by application of the squeezing operator

$$\hat{S}(\zeta) = \exp\left(\frac{\zeta}{2}\left(\hat{a}^2 - \hat{a}^{\dagger 2}\right)\right), \tag{1.42}$$

which may be realised, for example, by degenerate parametric amplification [9].

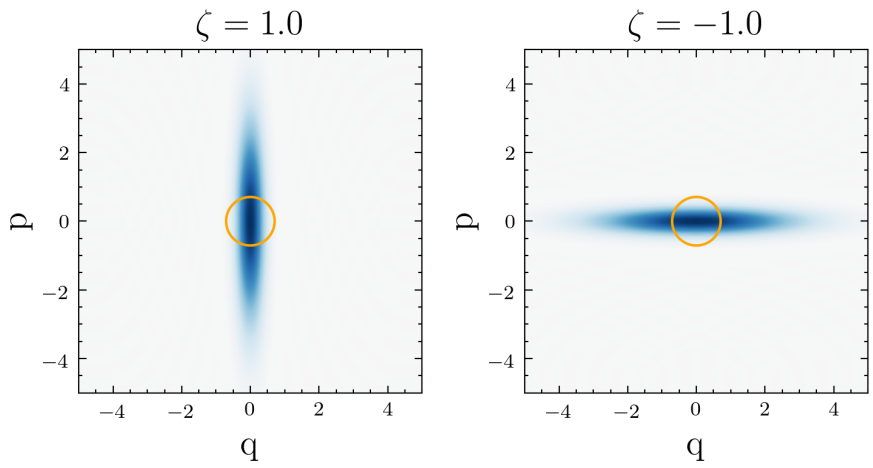


Figure 1.6: Quadrature squeezed states. Squeezing operator $\hat{S}(\zeta)$ has been applied to vacuum. (a) $\zeta = 1.0$. (b) $\zeta = -1.0$. Orange circles denote vacuum variance. Squeezed states allow for reduced uncertainty in one quadrature, at the expense of increased uncertainty in the conjugate quadrature.

1.2.10 *Squeezed states (photon-number)*

We have seen that the coherent state $|\alpha\rangle$ may be expanded in Fock basis as Eq. 1.37. From this equation it may be shown that the photon-number distribution of $|\alpha\rangle$ is

$$\mathcal{P}_n[|\alpha\rangle] = |\langle n|\alpha\rangle|^2 = \frac{|\alpha|^{2n}}{n!} e^{-|\alpha|^2} \tag{1.43}$$

which obeys Poissonian statistics, i.e. its mean is equal to its variance. The thermal state can be shown to possess super-Poissonian photon statistics, with variance larger than its mean. Conversely, a sub-Poissonian state has reduced photon-number variance, with a variance smaller than its mean. The Fock state, with zero photon-number uncertainty, is the limiting example of a sub-Poissonian state.

In addition to the quadrature squeezing discussed above, in which the variance in one quadrature was reduced at the expense of the other, we may think of a photon-number squeezed state in which the photon-number variance is reduced, at the expense of an increase in the phase variance[5]. We display the Wigner function of a photon-number squeezed state in Fig. 1.7.

5 Note that quantifying such a statement is tricky, and we refer the reader to Ref. [10] for discussion.

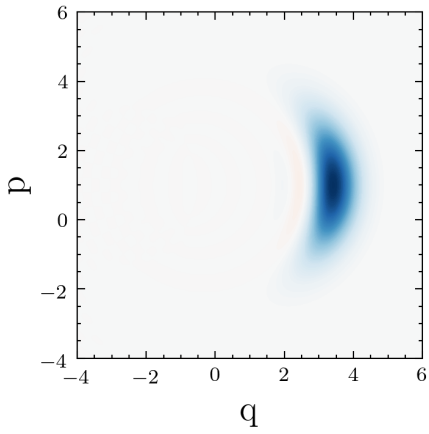


Figure 1.7: A photon-number squeezed state has reduced photon number uncertainty, at the expense of increased uncertainty in phase. In the limit of zero photon number uncertainty one obtains a Fock state, Fig. 1.1. This state displayed here is only slightly photon-number squeezed, but more closely represents a Fock state Wigner function than a quadrature squeezed state does.

1.2.11 *Mixing, purity, and entanglement*

Purity

We have already seen in Sec. 1.2.1 that the density matrix ρ can encode two types of uncertainty, quantum and classical. The quantum uncertainty is related to superpositions of basis states and is insurmountable, while the classical uncertainty represents ignorance of which quantum state was prepared, and can in principle always be reduced. A state possessing only the first type of ignorance may in general be written as

$$\rho = |\psi\rangle\langle\psi| \quad \text{with} \quad |\psi\rangle = \sum_n c_n |n\rangle \tag{1.44}$$

where without loss of generality we have used the Fock basis, and the c_n are complex coefficients. We call the the state Eq. 1.44 a "pure" state. Any state which is not pure is "mixed". A state with *only* the second type of ignorance may in general be written as

$$\rho = \sum_n d_n |n\rangle\langle n| \tag{1.45}$$

where without loss of generality we have used the Fock basis, and d_n are real coefficients. The state Eq. 1.45 only has diagonal elements in its density matrix, and if there are two or more nonzero d_n then the state is completely mixed.

Given a density matrix ρ, it is time consuming and difficult to check by hand which of these forms it takes, and in most situations it will not fit neatly into either form. We therefore desire a function which

will identify and quantify which type of ignorance the state possesses, and which may be easily computed on ρ. To do this, we first introduce the trace of ρ as

$$\mathrm{tr}\left[\rho\right] := \sum_{m} \langle m|\rho|m\rangle \,, \tag{1.46}$$

where without loss of generality we have used the Fock basis, but we note that we may instead sum over any orthonormal basis for $\mathcal{H}$. By definition, the trace of a normalized state must be 1. We introduce the notion of *purity* of a quantum state as a measure of how close to Eq. 1.44 our state is. This may be measured by

$$\mathrm{tr}\left[\rho^2\right], \tag{1.47}$$

which we will simply call the purity. It can easily be shown that state Eq. 1.44 has purity 1 while state Eq. 1.45 has purity 0.

Entanglement

Let us now turn to consider two-mode quantum states. We have already seen that a single-mode quantum state exists as a vector on Hilbert space $\mathcal{H}$. To describe two modes, we introduce an additional Hilbert space and write $\mathcal{H}_{tot} = \mathcal{H}_1 \otimes \mathcal{H}_2$, where $\mathcal{H}_{1,2}$ are Hilbert spaces of the individual modes, $\otimes$ represents the tensor-product, and $\mathcal{H}_{tot}$ is the total Hilbert space. We may tensor product any two single-mode quantum states together to form a state on $\mathcal{H}_{tot}$, for example

$$|\alpha\rangle_1 \otimes |n\rangle_2 \tag{1.48}$$

represents a state on $\mathcal{H}_{tot}$, consisting of a coherent state with amplitude α on $\mathcal{H}_1$, and an n photon Fock state on $\mathcal{H}_2$. For convenience we will often write $|\alpha, n\rangle$ instead of $|\alpha\rangle_1 \otimes |n\rangle_2$.

Now, there are many states which we can write in the form Eq. 1.48. The general form of this type of "product-state" is

$$\rho_{\text{product}} = |\Psi\rangle\langle\Psi| \quad \text{with} \quad |\Psi\rangle = |\psi\rangle_1 \otimes |\phi\rangle_2 \,. \tag{1.49}$$

A general "separable state" may be written

$$\rho_{\text{separable}} = \sum_{i,j} c_{i,j} \, |\psi_i\rangle\langle\psi_i|_1 \otimes \left|\phi_j\right\rangle\!\left\langle\phi_j\right|_2 \,, \tag{1.50}$$

called "separable" because the total two-mode state can be separated out into distinct single-mode density operators of modes 1 and 2 individually. The separable state may be interpreted as a classical mixture of product states.

Any state which cannot be written in the form Eq. 1.50 is known as a "non-separable" or "entangled" state. Entangled states cannot be written as a classical mixture over single-mode density operators, and so even full information about each individual mode is not sufficient

to fully describe the total system. Such a remarkable feature is one of the key departures of the quantum world from the classical one, and entanglement is itself a fundamental resource to accomplish quantum tasks [11, 12].

Partial trace

Let $\rho = \sum_{i,j,k,l} c_{i,j,k,l} |i,j\rangle \langle k,l|$ be a general two-mode density operator. We define the partial trace over mode 1 as

$$\begin{aligned} \mathrm{tr}_1[\rho] = \sum_n \langle n|\rho|n\rangle &= \sum_n \langle n| \left[\sum_{i,j,k,l} (|i\rangle\langle j|) \otimes (|j\rangle\langle l|) \right] |n\rangle \\ &= \sum_n \sum_{i,j,k,l} c_{i,j,k,l} \left(\langle n|l\rangle \langle k|n\rangle \right) |j\rangle\langle l| \\ &=: \rho_2 . \end{aligned}$$

The partial trace over mode 2 (yielding state ρ_1) is defined analogously.

In the specific case that the total state ρ is pure, it can be shown that if ρ is separable, then ρ_2 must be pure, i.e. $\mathrm{tr}\left[\rho_2^2\right] = 1$. Conversely, if $\mathrm{tr}\left[\rho_2^2\right] < 1$ then the total state ρ must be entangled.

1.2.12 *Two-mode squeezed vacuum (TMSV)*

Each of the states we have seen so far are single-mode states. Here we meet our first specific example of a two-mode state, the two-mode squeezed vacuum, which is written in a Fock-basis expansion as

$$|\mathrm{TMSV}\rangle = \frac{1}{\cosh\zeta} \sum_n (\tanh\zeta)^n |n,n\rangle . \tag{1.51}$$

The parameter ζ controls the level of two-mode squeezing of the state, and thus parametrises both its energy and its level of entanglement. The reduced states of $|\mathrm{TMSV}\rangle$ are thermal states with thermal photon number $\bar{n} = \sinh^2\zeta$, which we display in Fig.1.8. Remarkably, the state has strong quadrature correlations between modes:

$$\begin{aligned} q_1 &\sim q_2, \\ p_1 &\sim -p_2, \end{aligned}$$

where the position quadratures are correlated and the momentum quadratures are anticorrelated. We explicitly show this in the two-mode squeezed vacuum wavefunction in Fig. 1.9. The correlations between modes are a direct consequence of entanglement, making the two-mode squeezed vacuum a canonical resource state for quantum information processing. We shall use the TMSV extensively in the first part of this Thesis, since possession of one of its modes allows information about its second mode to be gained.

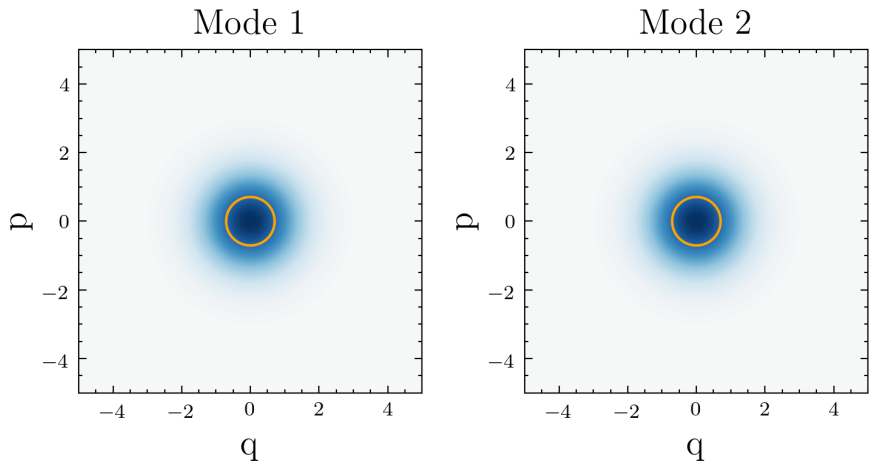


Figure 1.8: Wigner functions of reduced states of a TMSV with $\zeta = 0.65$. The corresponding quadrature wavefunctions are displayed in Fig. 1.9. Locally the modes look like thermal states with $\bar{n} = 0.5$, c.f. Fig. 1.5. The vacuum variance is depicted in orange.

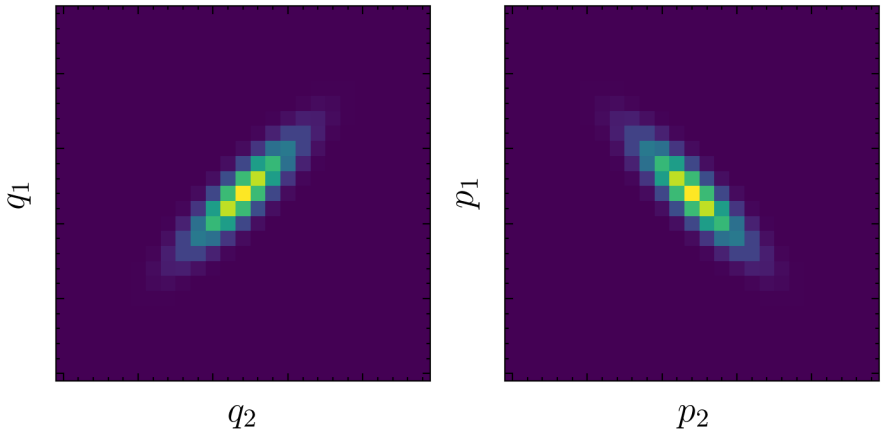


Figure 1.9: Quadrature wavefunction of the TMSV with $\zeta = 0.65$, with corresponding reduced state Wigner functions in Fig. 1.8. (a) Position representation. (b) Momentum representation. We see that position quadratures are strongly correlated, $q_1 \sim q_2$, while momentum quadratures are strongly anticorrelated, $p_1 \sim -p_2$.

1.3 MODELLING THE QUANTUM STATE

Let us introduce some additional tools which will help us to describe the quantum state and its dynamics.

1.3.1 *Covariance matrix*

We define a "Gaussian" state as one with a Gaussian Wigner function. A Gaussian function can be entirely described by its first and second moments; the first moment is its mean, and the second moment is its (co)-variance. We introduce the "covariance matrix" of a multi-mode Gaussian state as a quantity which contains all information about the state's second moments. Then, for a Gaussian state, the covariance matrix offers a description of the quantum state which is equivalent to the Wigner function or density matrix descriptions.

Let two modes be labelled 1 and 2. Then the covariance matrix element $\sigma_{j,k}$ is constructed as

$$\sigma_{j,k} = \frac{1}{2}\left[\left\langle d_j d_k \right\rangle + \left\langle d_k d_j \right\rangle\right] - \left\langle d_j \right\rangle \left\langle d_k \right\rangle \tag{1.52}$$

where vector $\overrightarrow{d} = [\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2]$, with the natural generalization to N modes. The covariance matrix σ is thus a 4×4 (or $2N \times 2N$) matrix .

A key quantity of the covariance matrix is its "symplectic eigenvalues," which are defined as the absolute values of the eigenspectrum of the matrix

$$i\Omega\sigma, \tag{1.53}$$

where

$$\Omega = \oplus_{k=1}^{2} \omega, \quad \text{and} \quad \omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{1.54}$$

We use the symplectic eigenvalues in Chapter 6 to quantify the entanglement between two modes described by their covariance matrix. Additional properties of the covariance matrix which we require will be introduced as needed, and we refer the reader to classic texts such as Refs. [13, 14] for further information.

1.3.2 *Beamsplitter relations*

The beamsplitter is one of the most important devices in quantum optics. On an ideal beamsplitter, two input quantum states interfere to produce two output states. The beamsplitter always requires four beams (two input and two output). We depict the beamsplitter in Fig. 1.10.

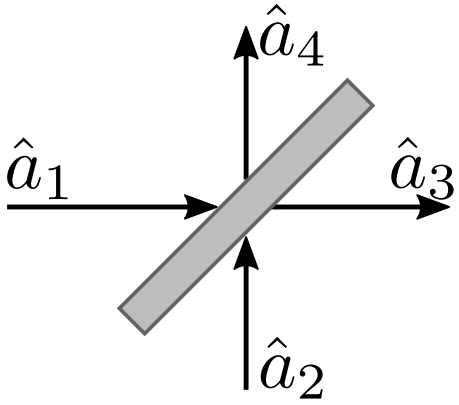


Figure 1.10: The beamsplitter transforms $\hat{a}_1, \hat{a}_2$ into $\hat{a}_3$, $\hat{a}_4$ via the matrix equation 1.55.

The beamsplitter transformation which we will make use of in this Thesis is

$$\begin{pmatrix} \hat{a}_3 \\ \hat{a}_4 \end{pmatrix} = \begin{pmatrix} \tau & -\rho \\ \rho & \tau \end{pmatrix} \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix}, \tag{1.55}$$

which transforms two input modes into two output modes as

$$\hat{a}_3 = \tau\hat{a}_1 - \rho\hat{a}_2 \quad \text{and} \quad \hat{a}_4 = \rho\hat{a}_1 + \tau\hat{a}_2. \tag{1.56}$$

To conserve energy we require $|\tau|^2 + |\rho|^2 = 1$. Finally, we will make extensive use of the following relation, which describes the output state when two input Fock states interfere on the beamsplitter. As in Ref. [1] we take τ and ρ to be real[6], such that $\tau = \sqrt{T}$ and $\rho = \sqrt{1-T}$, with $0 \leqslant T \leqslant 1$. The two-mode output state is:

$$|n_1, n_2\rangle' = \frac{1}{\sqrt{n_1! n_2!}} \sum_{k_1,k_2=0}^{n_1,n_2} \binom{n_1}{k_1} \binom{n_2}{k_2} \left(\sqrt{T}\right)^{k_1} \left(\sqrt{1-T}\right)^{n_1-k_1} \left(-\sqrt{1-T}\right)^{k_2} \left(\sqrt{T}\right)^{n_2-k_2} \sqrt{(k_1+k_2)!\,(n_1+n_2-k_1-k_2)!} \times |k_1+k_2, n_1+n_2-k_1-k_2\rangle\,. \tag{1.57}$$

We later identify T with channel transmission.

1.3.3 *Master equation*

We now introduce some formalisms which will account for dynamics of a quantum system described by density matrix ρ. In a closed system, in which ρ is a (potentially large) density matrix describing all degrees of freedom, the evolution is entirely governed by the von Neumann equation[7]

6 Reflectivity coefficient ρ has no relation to density operator $\hat{\rho}$.
7 Displayed with $\hbar = 1$ for convenience.

$$\frac{d}{dt}\rho = -i\left[\hat{H}, \rho\right], \tag{1.58}$$

with $\hat{H}$ the Hamiltonian which controls the time-evolution of ρ. Although exact, the von Neumann equation is often difficult to solve, especially in the case of very large ρ.

There are many instances, however, where we do not care about modelling precise evolution of all degrees of freedom of ρ. One may think, perhaps, of a few quantum modes of interest which are weakly coupled to many more modes. We denote the interesting modes as "system" and the uninteresting ones as "reservoir", and write $\rho_S = \mathrm{tr}_R[\rho]$. In this case, instead of solving the von Neumann equation we can model the evolution of ρ_S using the Lindblad master equation:

$$\frac{d}{dt}\rho_S = -i\left[\hat{H}_S, \rho_S\right] + \gamma\mathcal{L}\left[\hat{A}\right]\rho_S, \tag{1.59}$$

where $\hat{H}_S$ describes evolution of the system state only, γ is the decay rate of ρ_S into the reservoir, and

$$\mathcal{L}\left[\hat{A}\right]\rho_S = \hat{A}\rho_S\hat{A}^\dagger - \frac{1}{2}\hat{A}^\dagger\hat{A}\rho_S - \frac{1}{2}\rho_S\hat{A}^\dagger\hat{A} \tag{1.60}$$

describes decay of ρ_S into the reservoir. The term $\mathcal{L}\left[\hat{A}\right]$ is known as the Lindbladian, and $\hat{A}$ is the collapse operator which describes decay into the reservoir. The first term in Eq. 1.59 describes unitary (reversible) evolution of ρ_S, while the second term describes dissipative (irreversible) evolution.

We will make use of the Lindblad master equation with several different collapse operators in Chapter 6. For derivation of the master equation, including a detailed accounting of the requisite assumptions, we refer the reader to Refs. [6, 15].

1.4 QUANTUM MEASUREMENT

We define a set of measurement operators $\{\hat{M}_j\}$ which act on a quantum state $|\psi\rangle$, each measurement operator corresponding to a different possible measurement outcome j. The probability that j is observed after measurement on $|\psi\rangle$ is given by the overlap

$$P(j) = \langle\psi|\hat{M}_j^\dagger\hat{M}_j|\psi\rangle, \tag{1.61}$$

while the state immediately after measuring j is

$$|\psi'\rangle = \frac{\hat{M}_j|\psi\rangle}{\sqrt{P(j)}}. \tag{1.62}$$

The set $\{\hat{M}_j\}$ should allow for any possible outcome j, and so we require

$$\sum_j \hat{M}_j^\dagger\hat{M}_j = \mathbb{1}, \tag{1.63}$$

which encodes the normalization requirement for the probability distribution

$$\sum_j P(j) = 1. \tag{1.64}$$

Let us identify $\hat{M}_j^\dagger \hat{M}_j$ with an operator $\hat{E}_j$, which we shall refer to as a "POVM" element. The set $\{\hat{E}_j\}$ is known as a "POVM"[8] [16]. The POVM measurement formalism allows for a convenient description of quantum measurement statistics, as

$$P(j) = \langle\psi|\hat{E}_j|\psi\rangle \tag{1.65}$$

with no reference to the post-measurement state.

To illustrate the advantage of the POVM formalism, let us briefly consider an example, which we will revisit in later chapters. Suppose that Alice sends Bob one of two quantum states, either $|\psi_1\rangle = |0\rangle$ or $|\psi_2\rangle = (\alpha|0\rangle + \beta|1\rangle)$, with $\alpha^2 + \beta^2 = 1$. We assume that $\alpha, \beta \in \mathbb{R}$ for simplicity. Bob wishes to perform some measurement on his received state to determine whether he received $|\psi_1\rangle$ or $|\psi_2\rangle$. To do so, let Bob construct the following POVM:

$$\begin{aligned}
\hat{E}_1 &:= \frac{\sqrt{2}}{\alpha+\sqrt{2}}|1\rangle\langle 1| \\
\hat{E}_2 &:= \frac{\sqrt{2}\alpha^2}{\left(\sqrt{2}+\alpha\right)(\alpha^2+\beta^2)}\left(-\frac{\beta}{\alpha}|0\rangle + |1\rangle\right)\left(-\frac{\beta}{\alpha}\langle 0| + \langle 1|\right) \\
\hat{E}_3 &:= \mathbb{1} - \hat{E}_1 - \hat{E}_2.
\end{aligned}$$

One can readily check that if Bob performs $\{\hat{E}_1, \hat{E}_2, \hat{E}_3\}$ on state $|\psi_1\rangle$, there is zero chance he will record outcome E_1. Therefore, if Bob receives outcome E_1 he knows with certainty that Alice sent him $|\psi_2\rangle$. Likewise, if Bob receives outcome E_2 then he knows with certainty that Alice sent $|\psi_1\rangle$. However, should Bob receive E_3 then he gains no information about the state which Alice sent.

The POVM $\{\hat{E}_1, \hat{E}_2, \hat{E}_3\}$ thus performs an *unambiguous discrimination* [16] between the non-orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$, and Bob will never misidentify the state which Alice sent. This comes at a cost: sometimes Bob gains no information at all. Designing POVMs and measurement schemes to optimally distinguish between a known set of states is a difficult problem which has received considerable attention over the years. We will revisit this question in Chapters 3 and 4 in the context of quantum cryptography, where bounding a malicious party's ability to distinguish between quantum states is of critical importance.

8 Which stands for *positive operator valued measure*, for historical reasons.

1.4.1 *Homodyne measurement*

Homodyne measurement is a frequently used technique for measuring the quadrature components of the quantum state. A homodyne detection scheme consists in measurement of quadrature operator $\hat{q}_\theta = \cos\theta\hat{q} + \sin\theta\hat{p}$, which gives outcome probabilities

$$P(q_\theta) = \langle q_\theta|\rho|q_\theta\rangle \tag{1.66}$$

where $|q_\theta\rangle$ is the eigenstate of $\hat{q}_\theta$ (c.f. Eq. 1.34). The set of operators $|q_\theta\rangle\langle q_\theta|$ form the homodyne POVM.

In practice the homodyne POVM is realised by mixing ρ with a strong coherent state $|\alpha\rangle$, $|\alpha| \gg 1$ (the so-called "local oscillator"), on a balanced (50/50) beamsplitter, and subtracting the measured photocurrents at the output arms from each other. We depict this process in Fig. 1.11. We assume in the ideal case that the photocurrents I_1 and I_2 are such that

$$I_1 \propto \hat{n}_1 \quad \text{and} \quad I_2 \propto \hat{n}_2 \quad \text{with} \quad \hat{n}_i = \hat{a}_i^\dagger \hat{a}_i, \tag{1.67}$$

and that the local oscillator may be treated classically, so

$$\hat{a}_1 = \frac{1}{\sqrt{2}}(\hat{a} - \alpha_{LO}) \quad \text{and} \quad \hat{a}_2 = \frac{1}{\sqrt{2}}(\hat{a} + \alpha_{LO}). \tag{1.68}$$

Then the difference in photocurrents $I_2 - I_1$ is

$$I_2 - I_1 \sim \hat{n}_2 - \hat{n}_1 = \alpha_{LO}^* \hat{a} + \alpha_{LO}\hat{a}, \tag{1.69}$$

and so

$$I_2 - I_1 \sim \sqrt{2}|\alpha_{LO}|\,\hat{q}_\theta, \tag{1.70}$$

where θ is the phase of the local oscillator $|\alpha\rangle$. Varying the phase θ thus allows any general quadrature $\hat{q}_\theta$ of ρ to be measured. The prefactor $\sqrt{2}|\alpha_{LO}|$ does not affect our measurement, and may be taken into account by an appropriate rescaling of measurement outcomes. A more realistic treatment of homodyne detection, including discussion of the range of validity of the above expressions, may be found in Refs. [14, 17].

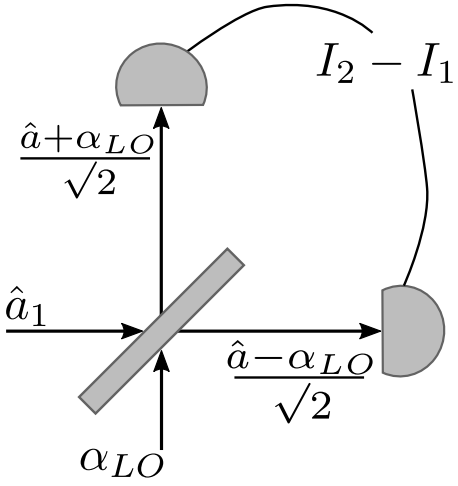


Figure 1.11: The homodyne detector mixes the mode to be measured, $\hat{a}_1$, with a strong local oscillator. The photocurrents are measured and subtracted $I_2 - I_1$, which gives measurement information about $\hat{q}_\theta$. The quadrature angle θ is controlled via the relative phase of the local oscillator.

1.4.2 *Heterodyne measurement*

A heterodyne measurement scheme corresponds to the POVM

$$\hat{\mathbb{1}} = \frac{1}{\pi} \int_{\alpha \in \mathbb{C}} d^2\alpha \; |\alpha\rangle\langle\alpha| \,. \tag{1.71}$$

The measurement gives outcome α with probability $(1/2\pi)\,\langle\alpha|\rho|\alpha\rangle$. This scheme may be realised as a "double-homodyne" protocol, in which an input state ρ is split on a balanced beamsplitter, and conjugate quadratures $\hat{q}_1$, $\hat{p}_2$ are measured on different output arms. Since they operate on different modes, the operators $\hat{q}_1$, $\hat{p}_2$ must commute. Simultaneous measurement of conjugate quadratures on the *same* mode cannot be performed with arbitrary accuracy, and so the heterodyne measurement outcomes must pay the penalty of increased variance in $P(q)$, $P(p)$. Physically this arises from mixing with ρ with vacuum on the first beamsplitter.

The heterodyne detector allows us to consistently define a joint probability distribution of the measurement outcomes q_1, p_2. This function is known as the Hussimi Q function and is a well-defined probability distribution on the phase space[9]. The Hussimi function corresponding to ρ is thus

$$Q(q,p) = \frac{1}{\pi}\,\langle\alpha|\rho|\alpha\rangle \quad \text{with} \quad \alpha = \frac{q+ip}{\sqrt{2}}. \tag{1.72}$$

In the main body of the Thesis we will speak of the heterodyne measurement as effectively giving two outcomes, q_{out}, p_{out}, one from

9 Unlike others such as Wigner function or P function, which we refer to only as *quasi*-probability distributions

each homodyned arm. The α required for Eq. 1.71 are then given by $\alpha = (q_{out} + ip_{out})/\sqrt{2}$.

1.5 ENTROPY AND PROBABILITY

We will introduce and discuss some quantum entropies which are used in the first part of this Thesis. Quantum entropies are a marvellous and interesting area of quantum information theory, and there are many interesting similarities with and departures from classical information theory. Below we summarise some of the key results which we will make use of in this Thesis, and the reader is referred to Refs. [16, 18–20] for further information.

1.5.1 *Conditional probabilities*

Let X and Y denote random variables, with their associated probability distributions $P(X), P(Y)$. The conditional probability of X given Y, $P(X \mid Y)$ measures the probability of event X, given prior knowledge of event Y. The probabilities $P(X)$, $P(Y)$ are known as the marginal probabilities, and are related to the conditional probability by summing over values of the prior Y:

$$P(X) = \sum_{Y=y} P(X \mid Y = y) P(Y = y). \tag{1.73}$$

Bayes' theorem may be used to relate conditional probabilities to each other:

$$P(X \mid Y) = P(Y \mid X) \frac{P(X)}{P(Y)}, \tag{1.74}$$

and we make extensive use of this formula in the first part of this Thesis.

1.5.2 *Hoeffding's inequalities*

Let $\mathcal{X} = X_1, X_2, \ldots, X_n$ be n independent binary random variables. Let $\bar{\mathcal{X}}$ be their empirical mean and let $\mathbb{E}(\bar{\mathcal{X}})$ be its expected value. Then $\forall \epsilon \geqslant 0$ we may bound the probability that the empirical mean $\bar{\mathcal{X}}$ differs from its expectation $\mathbb{E}(\bar{\mathcal{X}})$ by the following inequalities:

$$P\left(\bar{\mathcal{X}} - \mathbb{E}(\bar{\mathcal{X}}) \geqslant \epsilon\right) \leqslant \exp\left(-2\epsilon^2 n\right), \tag{1.75}$$

$$P\left(\mathbb{E}(\bar{\mathcal{X}}) - \bar{\mathcal{X}} \geqslant \epsilon\right) \leqslant \exp\left(-2\epsilon^2 n\right). \tag{1.76}$$

These inequalities are known as Hoeffding's inequalities [21] and will provide a necessary tool for analysis of our Quantum Digital Signatures protocol.

1.5.3 *Shannon entropy*

Let X be a random variable, which takes values $X_1, X_2, \ldots X_N$ with probability $P(X_1), P(X_2), \ldots, P(X_N)$. The Shannon entropy associated with this variable is defined as

$$H(X) = -\sum_{j=1}^{N} P(X_j) \log P(X_j) . \tag{1.77}$$

The Shannon entropy represents the degree of uncertainty which one possesses about the variable X. If the value of X is known (minimum uncertainty) then[10] $H(X) = 0$. Conversely, if all possible values of X are equally likely (maximum uncertainty) then $H(X) = \log N$.

1.5.4 *Binary entropy*

Let X be a binary random variable, which takes value 0 with probability p and value 1 with probability $1 - p$. Then the binary entropy of X is defined as

$$h(X) = -x \log x - (1 - x) \log (1 - x) . \tag{1.78}$$

The binary entropy is a special case of the Shannon entropy for a binary random variable. We display the binary entropy $h(X)$ in Fig. 1.12.

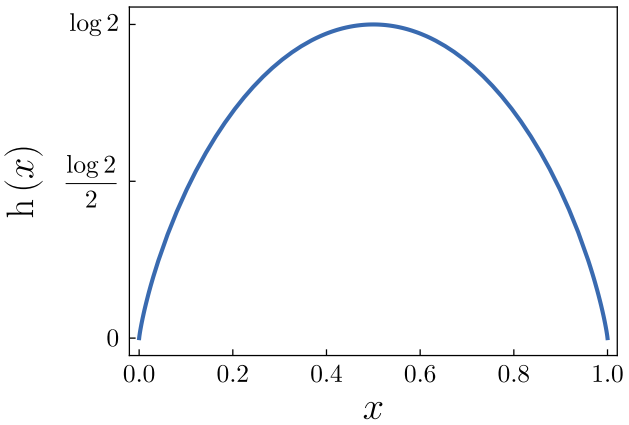


Figure 1.12: The binary entropy $h(x)$ is bounded by $\log 2$.

1.5.5 *Mutual information*

We define the joint entropy $H(X, Y)$ of two random variables X and Y as the Shannon entropy of the joint probability distribution $P(X, Y)$.

The conditional entropy of X, conditioned on Y, is

$$H(X \mid Y) = H(X, Y) - H(Y) , \tag{1.79}$$

10 By convention we take $0 \log 0 = 0$.

which measures the average uncertainty we have about variable X given that we know Y.

One may expand the conditional entropy as [19]

$$H(X \mid Y) = \sum_{Y=y} P(Y=y)\, H(X \mid Y=y), \tag{1.80}$$

where the expansion is over particular outcomes of the prior variable. Equation 1.80 admits a natural extension to the case when the prior variable is continuous rather than discrete, with $\sum_y$ replaced by $\int dy$.

The mutual information between X and Y may be defined as

$$I(X:Y) = H(X) - H(X \mid Y), \tag{1.81}$$

which is a measure of how much knowledge of one variable reduces uncertainty about the other variable. The mutual information is symmetric in its arguments.

1.5.6 *Von Neumann entropy*

The von Neumann entropy of a quantum state ρ is

$$S(\rho) = -\operatorname{tr}[\rho \log \rho], \tag{1.82}$$

which may be equivalently calculated as

$$S(\rho) = -\sum_j \lambda_j \log \lambda_j, \tag{1.83}$$

where λ_j are the eigenvalues of ρ. The von Neumann entropy is always non-negative, and is zero when ρ is pure.

By analogy with the Shannon entropy we will additionally define the joint entropy of a composite system $\rho_{A,B}$ in the obvious way

$$S(\rho_{A,B}) = -\operatorname{tr}[\rho_{A,B} \log \rho_{A,B}]. \tag{1.84}$$

The conditional von Neumann entropy between quantum systems A and B may then be defined:

$$S(A \mid B) = S(A,B) - S(B), \tag{1.85}$$

where the von Neumann entropy of a quantum system A or B should be understood as the entropy of the corresponding reduced state ρ_A, ρ_B.

1.5.7 *Holevo information*

The Holevo information χ is an upper bound on the mutual information I, and plays a crucial role in many areas of quantum information processing.

We introduce two players, Alice and Bob. Let Alice prepare a state ρ_j, $j = 1, 2, \ldots, N$, with probability $p_1, p_2, \ldots, p_N$. Bob wishes to distinguish which of the ρ_j Alice has prepared.

Bob may perform any measurement described by POVM elements $\{E_K\}$, and he receives a measurement outcome K. Then the mutual information $I(j : K)$ describes the knowledge of which ρ_j was prepared, given Bob's measurement outcome K. The mutual information is upper bounded by the Holevo information

$$I(j : K) \leqslant \chi(j : K), \tag{1.86}$$

with the Holevo information χ defined as

$$\chi(j : K) = S(\rho) - \sum_j p_j S(\rho_j), \tag{1.87}$$

with

$$\rho = \sum_j p_j \rho_j. \tag{1.88}$$

For a pleasing proof that I is bounded by χ we refer the reader to Ref. [16].

Throughout this Thesis we will refer to the first term in Eq. 1.87 as the *a priori* entropy (with its corresponding *a priori* state ρ), while we refer to the second term as the *a posteriori* entropy (with its corresponding *a posteriori* state ρ_j). The bound in Eq. 1.86 will be used extensively in the cryptographic security proofs in the first part of this Thesis.

1.5.8 *Conditioning cannot increase entropy*

A useful property of both Shannon and von Neumann entropies is that "conditioning cannot increase entropy." This directly encodes the intuition that gaining more information about a system cannot lead to increased uncertainty - at worst it will leave the uncertainty in our knowledge unchanged. Quantitatively, we have for a quantum state $\rho_{A,B}$

$$S(A) \geqslant S(A \mid B), \tag{1.89}$$

where the entropy of system A should be understood as the entropy of $\rho_A = \mathrm{tr}_B[\rho_{A,B}]$. Similarly, for classical random variables X, Y:

$$H(X) \geqslant H(X \mid Y). \tag{1.90}$$

1.5.9 *Chain rule for conditional Shannon entropy*

Let $X_1, \ldots, X_n$ and Y be random variables. Then [16, 19]

$$H(X_1, \ldots, X_n \mid Y) = \sum_{i=1}^{n} H(X_i \mid Y, X_1, \ldots, X_{i-1}). \tag{1.91}$$

This property is known as the conditional Shannon entropy *chain rule* and is readily proven by induction (see e.g. Ref. [16]) using Eq. 1.79.

1.6 SUMMARY

In this chapter we have provided a brief overview of several key concepts and tools which underpin this Thesis. Additional material which is required will be introduced as it is used. We have introduced the density matrix formalism and discussed how it relates to other methods for describing quantum states of light, such as the Wigner function and the covariance matrix. Although in this Thesis we work primarily in terms of the density matrix, the Wigner function has provided us with a useful visualization tool in this Chapter. Furthermore, the Wigner function simplifies calculations in Appendix A which are in principle possible, but difficult in general, using density matrices. The covariance matrix is another useful tool which warrants extensive study in its own right. We use the covariance matrix only in Chapter 6 to measure the Gaussian entanglement properties of a state. The Wigner function representation for a multimode quantum state is intertwined with the covariance matrix description, and we refer the reader to Ref. [14] for an excellent discussion of how to move between the two pictures.

In the first half of this Thesis, Chapters 3-5, we will use the density matrix description, along with the beamsplitter relation for input fock states, in order to model the passage of a quantum state through a channel. In the cryptographic protocols discussed there, a malevolent party is assumed to replace the channel with an ideal beamsplitter. They have control over the second input port, and receive the reflected output state. We model this interaction and then use the entropies introduced above to bound the ability of a dishonest player to break the protocol.

In the second half of this Thesis we will examine in depth the dynamics of a coherent state in several different scenarios. Our key tool here will be the Lindblad equation which describes the evolution of our density matrix. When possible we draw conclusions analytically, but our main techniques will be the numerical methods discussed at length in Appendix E. These allow us to gain an understanding of the state evolution, sometimes even if computational constraints prevent us from accessing the full density matrix.

Part I

AGILE CRYPTOGRAPHY: SIGNATURES AND SECRETS

2 INTRODUCTION TO QUANTUM CRYPTOGRAPHY

2.1 CONVENTIONAL (CLASSICAL) CRYPTOGRAPHY

Cryptography is a field probably as old as civilization itself. For as long as communication has existed, so too has the desire to keep information hidden. Both the Greeks and the Romans are known to have used ciphers to encrypt messages [22]. A cipher, after being applied to a message, allows the encrypted message to be freely transmitted and intercepted without an adverse party interpreting its meaning. The intended recipients, however, can undo the effects of the cipher and read the original message.

One famous example is the Caesar cipher. In the Caesar cipher, each element of the alphabet which makes up the message ("plain") is assigned a new symbol ("cipher"). Typically this is done by shifting the alphabet by a known quantity, Fig. 2.1. The plaintext message is encoded with the cipher, replacing letters from the plain with letters from the cipher. This encoded message is known as "ciphertext" and now may be freely distributed. At face value, the ciphertext is unreadable to anyone without access to the cipher.

Plain: `ABCDEFGHIJKLMNOPQRSTUVWXYZ`
Cipher: `FGHIJKLMNOPQRSTUVWXYZABCDE`
Plaintext: I like physics
Ciphertext: N qnpj umdxnhx

Figure 2.1: The cipher alphabet is formed of the plain alphabet shifted 5 elements to the left. Knowledge of the cipher allows the plaintext message to be recovered.

Cryptanalysis – the art and science of breaking cryptographic systems – has existed for as long as cryptography, and history of cryptographic development can be viewed as an arms-race between cryptographers and cryptanalysts. The cryptographers, which we canonically call Alice and Bob, continually invent new schemes to perform their secure communication task. The cryptanalyst, which we canonically call Eve, continually tries to break these schemes in order to interfere in Alice and Bob's communication and obtain their messages. For example, the Caesar cipher can be broken by trying all possible shifts

of the alphabet and checking which give a sensible message at the output. Against a more general cipher, Eve can perform a statistical analysis on the ciphertext, provided that she knows the language of the message. In English, for example, Eve knows that "e" is the most frequently occurring letter, and so the most common letter in the ciphertext is likely to decode to "e".

Many advances on the Ceasar cipher have been developed, in which a key (a shared secret piece of information) is used to encrypt and then decrypt a message. While many schemes are secure against decryption, they meet significant practical issues to actually distribute the key. Indeed, the key distribution problem was one of the longstanding and difficult problems which cryptographers have faced over the millenia. Should the shared keys fall into enemy hands, secret messages may be freely decrypted and their sensitive information made public.

One potential method to distribute keys requires Alice and Bob to meet face-to-face in advance of their communication, in order to share the keys which they will use for the next round of communication. While secure, this is impractical. A third party courier could instead be used as a go-between, but this places an assumption about the trustworthiness of the messenger, and requires an unweildly overhead for large-scale communications. In the second half of the 20^{th} Century, the following critical question became the focus of intense study of a small group of cryptographers: "How can Alice and Bob share a secret key, without ever meeting each other?"

To solve this problem, Diffie and Hellman [23] required a fundamental paradigm shift to the structure of conventional encryption. Normally, as with the Caesar cipher, Fig. 2.1, the same key is used to encrypt and to decrypt the message, Fig. 2.2 (a), a structure known as "private-key (symmetric) cryptography". It is the sharing of this key which is the weak link in the encryption protocol. Diffie and Hellman realised that it is possible to share the key without Alice and Bob ever meeting[1] face-to-face. The central idea behind the new "public-key (asymmetric) cryptography" was the existence of so-called *one way* functions, which are easy to perform but difficult to invert.

Diffie and Hellman's proposal runs as follows. At the start of communication, Alice and Bob publicly agree on a function, Y^x modulo P, with $Y < P$. The Y and P are assumed to be public knowledge. For example, they may choose the function $f(x) = 13^x$ modulo 19. Now, Alice and Bob each choose a number, labelled A, B, and keep it secret, e.g. $A = 2$ and $B = 4$. Each number is fed into f: $\alpha := f(A) = 17$ and $\beta := f(B) = 4$. The outputs α, β are shared between Alice and Bob. Crucially, although calculating α, β was simple, it is tricky to find A and B from this public information. Finally, Alice calculates β^A modulo $19 = 16$ and Bob calculates α^B modulo $19 = 16$: Alice

1 Of course, at the beginning of the protocol Alice and Bob must be sure that they are actually talking to each other [24].

and Bob reach the same number, 16, which can then be used as the encryption key. This discovery allows Alice and Bob to establish a key entirely over public and insecure communication channels.

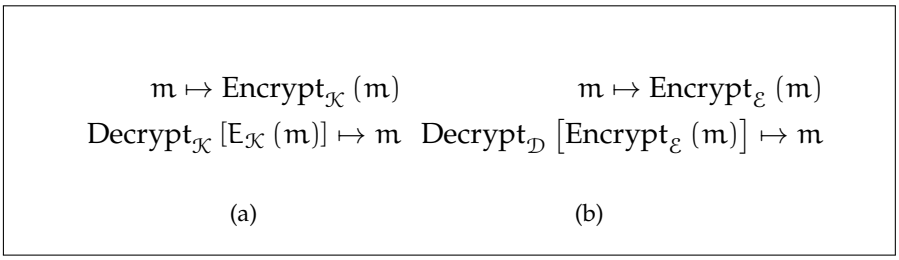


Figure 2.2: (a) Private-key encryption. The same key $\mathcal{K}$ allows Alice to encrypt and Bob to decrypt message m. (b) Public-key encryption. Alice and Bob use different keys, $\mathcal{E}$ and $\mathcal{D}$ to encrypt and decrypt m. The key $\mathcal{E}$ can be public knowledge without affecting the security of the key $\mathcal{D}$.

Security of this key exchange system relies on the fact that A and B are kept secret, and it is the distinctions and relationships between public and private information which underpin public key cryptography. The function f is sometimes referred to as a "trapdoor" or "one-way" function, and is typically based on a mathematical problem which is deemed to be computationally hard: that is, even the most powerful computers cannot hope to solve it in a feasible amount of time. Typically the time taken to solve scales exponentially in the size of the key. Perhaps the most well-known hard problem is that of factoring a large integer into primes, which underlies the commonly used RSA protocol [24, 25].

This type of security, relying on assumptions about computing power, is known as *computational* security. In principle these cryptosystems could be broken with a sufficiently powerful computer, or with algorithmic advances. It has been shown, however, that while these problems are hard for a classical computer, there exist algorithms for a future quantum computer which can break them. The most well known of these is Shor's algorithm [26], which provides an exponential speedup in the ability to split an integer into its prime factors. The existence of such algorithms which successfully solve the hard problems poses a threat to many commonly used cryptosystems [16, 24–27]. One must therefore carefully consider how to respond to this threat posed by quantum computers.

One solution will be to switch the underlying hard problem to a different class of problems, which even a quantum computer cannot solve. This is the approach adopted by the Post-Quantum Cryptography (PQC) community, whose aim is to design protocols based on problems for which no good quantum algorithm is yet known [28–33]. However, it is still an open question which problems a quantum computer can hope to solve, and so a premature implementation of a

secure system based on a PQC hard-problem may still be threatened by a quantum computer as new algorithms are developed.

The second solution to the threat posed by quantum computers is to begin to adopt cryptosystems which are provably secure against a quantum computer. There exist classical protocols for which this is possible [34, 35], and we will discuss some of them in Sec. 2.3. However for many applications classical cryptography does not allow for such provably secure systems without an initial face-to-face interaction[2], and so one must move to the quantum realm.

Quantum cryptography bases its security not on the assumption of a mathematical problem's difficulty, but on physical laws. Instead of aiming for computational security (albeit security against a quantum computer), quantum cryptography aims to build the stronger *unconditionally secure* (or *information-theoretically secure*) protocols, which cannot be broken even in principle. By basing security on physical laws, quantum cryptography requires the sharing of physical systems between players, and we shall see in the remainder of this Thesis that quantum light is a natural object with which to perform such cryptographic tasks.

One may think of the advantage provided by quantum cryptography in terms of the one-way functions discussed earlier, Fig. 2.3. While the classical one-way functions are only computationally hard, the quantum analogue of the one-way function is provably impossible to invert. For example, if the unknown quantum states are chosen to be non-orthogonal then it is impossible to perfectly determine the classical information which they encode [16, 36]. Any malevolent party attempting to gain information will not do so perfectly, and will thus leave evidence of their intrusion.

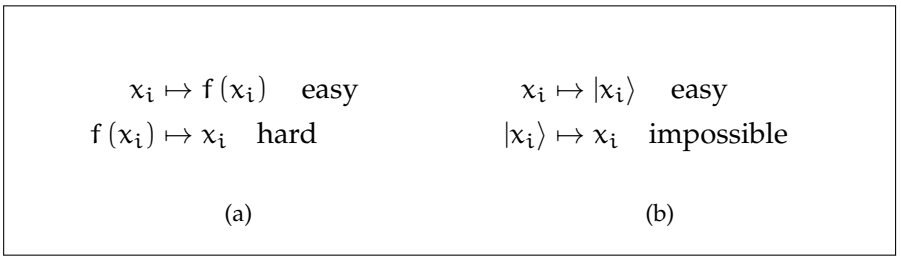


Figure 2.3: (a) A classical one-way function f is easy to perform but computationally difficult to invert. f is typically based on a hard problem. (b) A quantum one-way function. If the quantum states $|x_i\rangle$ are chosen to be non-orthogonal then it is impossible to perfectly determine the classical information x, given a quantum state $|x\rangle$. This forms the basis for quantum cryptosystems, whose security is guaranteed by the no-cloning theorem [16, 36]

2 To facilitate, for example, the sharing of large, random, secure keys.

2.2 QUANTUM DIGITAL SIGNATURES

2.2.1 *Classical digital signatures*

Although encryption is perhaps the most well known cryptographic protocol, it is by no means the only important task which is accomplished daily by modern cryptography. Digital signatures, for example, are ubiquitous in our everyday information infrastructure, and they are crucial to digital communication such as software distribution or financial transactions. In many countries, a digital signature is even legally meaningful. The aim of a digital signature scheme is to provide a way to securely sign a classical message, such that it can neither be forged nor tampered with. Additionally, every player should be able to agree about the validity of the message.

One method which may be used to perform this task requires a symmetric (private-key) cryptosystem, Fig. 2.2a, and a trusted arbiter. Assume that Alice wishes to securely sign a message to Bob. We will denote the arbiter as David. David should share one secure key κ_A with Alice, and another κ_B with Bob. Alice encrypts her message m with κ_A and sends it to David, who decrypts it. David adds to m a statement that m definitely originated with Alice, and encrypts the entire thing with κ_B and send it to Bob. Bob can decrypt and read m, and is confident that it definitely originated with Alice, because of David's stamp of approval.

Such a scheme will accomplish all of the requirements of a digital signature, including transferability, but the requirement that all communication be mediated by arbiter David is a strong one, and David will become a bottleneck in this system.

A more practical scheme uses asymmetric (public-key) cryptography[3], Fig. 2.2b. Assume that Alice has a private key, known only to her, while Bob possesses her public key, which is freely available to any interested party. Alice may sign her message by encrypting m and send it to Bob. Bob decrypts using the public key, and he can freely read m and be confident that it originated with Alice. Moreover, since Alice's public key is freely available her message m is transferable. This system has the advantage of not requiring any trusted arbiter[4] or bottleneck. The scheme described here was first invented by Diffie and Hellman in 1976 [23].

This idea was expanded upon by Lamport in 1979 [38], whose proposed signatures scheme uses one-way functions. Alice wishes to send a one-bit message m to Bob. For each m she will create a random string θ_0, θ_1 and input them to her one-way function f. Alice then freely distributes $\{f(\theta_0), f(\theta_1)\}$. Since f is one-way, a potential

3 A fascinating overview of the development of digital signatures may be found in Ref. [37] which describes historic details which motivated signatures, and which motivated the additional requirement of encryption-free signatures.

4 Though in practice one will use a certificate authority to distribute the public keys.

forger cannot discover Alice's θ_0, θ_1. When Alice wishes to send her message, she will declare $\{m, \theta_m\}$. Bob applies the function f to θ_m, and if the output agrees with Alice's earlier declaration he will accept m as genuine.

Lamport's scheme has the advantage that m is visible to all, and the scheme does not require encryption of the message. A drawback is that once the θ_m have been used they cannot be reused and must be discarded. We note also that this scheme is inherently very similar to hash-based signature schemes in which Alice first applies a hash function h [24] to m, and then signs $h(m)$ (e.g. via the Diffie-Hellman protocol described above) and distributes m and her signed $h(m)$.

2.2.2 *Quantum one-way function*

Gottesman and Chuang generalized Lamport's scheme in 2001 to build the first Quantum Digital Signatures protocol [39]. The key contribution of their scheme is to replace the one-way function in Ref. [38] with a so-called *quantum one-way function*, thereby securing the signatures protocol against a quantum adversary.

A direct analogue of public-key cryptography, their protocol relies on the difficult task, described above in Fig. 2.3, of accurately distinguishing between non-orthogonal quantum states. Security relies on the fact that performing measurement on a state of n qubits can yield at most n bits of information, and so the protocol in Ref. [39] is designed such that this is insufficient to distinguish between states.

The key tool in the protocol is a quantum SWAP test which probabilistically determines whether two states are identical. To perform this test, players prepare $|f_x\rangle, |f_{x'}\rangle$ and an additional ancilla $(|0\rangle + |1\rangle)/\sqrt{2}$. Players perform a Fredkin gate using the ancilla as a control, and then perform a Hadamard on the ancilla [16, 36]. In other words, the SWAP test performs

$$|f_x\rangle |f_{x'}\rangle \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \mapsto \frac{(|f_x\rangle |f_{x'}\rangle \pm |f_{x'}\rangle |f_x\rangle) |y_\pm\rangle}{2} \tag{2.1}$$

with $y_+ = 0$ and $y_- = 1$. Finally, the ancilla qubit is measured in the $0, 1$ basis, and since $|0\rangle, |1\rangle$ are orthogonal they can be distinguished. Therefore if $x = x'$ the coefficient of $|1\rangle$ is identically zero, and so the SWAP test always outputs $|0\rangle$. If $x \neq x'$ outputs either $|1\rangle$ or $|0\rangle$.

The probabilistic nature of this test will cause participants in the protocol to sometimes mistake distinct states for identical ones, but the probability that this occurs may be estimated. Crucially, the protocol may be proven secure when this probability of honest failure is smaller than the probability to correctly distinguish between states.

Although laying the groundwork for practical QDS protocols, this original proposal cannot be feasibly implemented. The most pressing problem is the requirement for long-term quantum memory. State-of-the-art technology can store a photonic state for $\mathcal{O}(1)$ μs [40], and so

long-term storage of many copies of quantum states with many qubits will be challenging. Furthermore, the need for every party to be able to create and distribute the states and the multiple required *SWAP* tests render this protocol impractical for implementation.

However, the structure of this protocol is very closely aligned to classical signatures protocols since the public keys are truly public (all of them can be handed to Eve). Furthermore, every recipient is given identical quantum public keys and so the number of recipients does not need to be fixed before the start of the protocol. These requirements are subtly changed in later – more practical – QDS protocols.

2.2.3 *QDS implementation*

A step forward to practical implementation of QDS occurs in Ref. [41], in which Andersson *et. al.* replace the tricky to perform *SWAP* test from Ref. [39] with a practical state comparison method. The previously required entangled qubits are also replaced by coherent states. The requirements for QDS have thus been reduced to the generation, distribution and storage of coherent states, with only beamsplitters and photon detectors required at the recipient.

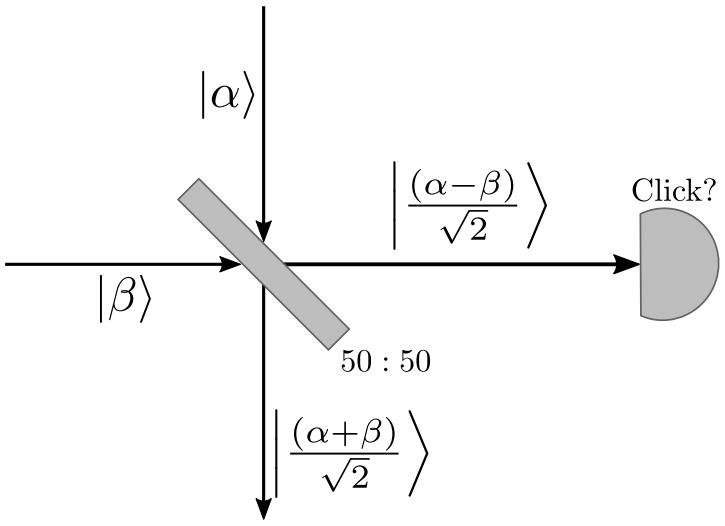


Figure 2.4: Non-destructive comparison method from Ref. [41]. The coherent states interfere on a balanced beamsplitter. Assuming an ideal detector, the absence of a detector click implies that $\alpha = \beta$. Otherwise, a click implies $\alpha \neq \beta$. A second balanced beamsplitter may be used to transform $|(\alpha+\beta)/\sqrt{2}\rangle \otimes |0\rangle \rightarrow |\alpha\rangle\,|\beta\rangle$, and hence this state comparison is non-destructive.

The key step, comparison of coherent states, is displayed pictorially in Fig. 2.4. If the photodetector clicks it is a strong indication[5] that $\alpha \neq \beta$. Furthermore this comparison is non-destructive, and simply by placing another beamsplitter in the path of the lower beam, with

5 It is a certain indication, in the ideal limit.

vacuum input to the second input port, one recovers $|\alpha\rangle|\beta\rangle$. Otherwise, for $\alpha \neq \beta$ the output states of the second beamsplitter are symmetrized and now identical to each other. This practical state comparison forms the building-block for their QDS protocol.

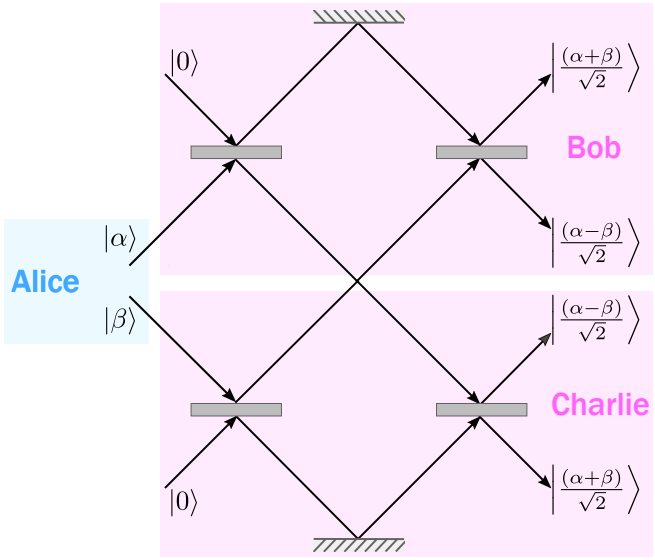


Figure 2.5: Multiport used in Ref. [41] which guards against a cheating Alice. The multiport symmetrizes Bob and Charlie's states so they always receive identical $|(\alpha+\beta)/\sqrt{2}\rangle$ at their signal outputs. By placing a photodetector at the null-ports Bob and Charlie can test whether $|(\alpha-\beta)/\sqrt{2}\rangle = |0\rangle$. In the ideal scenario, a detector click implies that $\alpha \neq \beta$, while its absence implies that $\alpha = \beta$.

Alice sends coherent states from her alphabet of possible coherent states, both to Bob and to Charlie, and keeps a record of which states she sent. To allow both parties to check whether they have received identical states, an optical multiport Fig. 2.5 is used. The multiport symmetrizes Bob and Charlie's received states, thus preventing a repudiating Alice. Each recipient has two outputs of the multiport: a "null-port" and a "signal-port". At the null-port is placed a photodetector which should be monitored for clicks, which in the ideal case will indicate either that Alice is trying to repudiate, or a malicious party is interacting with the state distribution. The signal-port yields the symmetrized quantum coherent states which Bob and Charlie then store in quantum memory.

Later, Alice sends the classical message, plus classical information describing which states she had previously sent. Bob and Charlie create the corresponding coherent states, and compare them via the method in Fig. 2.4 with the states retrieved from quantum memory. If no clicks are recorded during this comparison, it is an indication that the message is genuine and the protocol passes.

This protocol was implemented by Clarke *et. al.* in Ref. [42], where an alphabet with 8 phase-encoded coherent states was used. The total

number of coherent states required to sign a message, the *signature length*, was $L \sim 5 \times 10^6$. The signature length is the main figure of merit for QDS protocol[6]. To get around the requirement for quantum memory, the Messing and Distribution stages occurred at the same time so the coherent state corresponding to the chosen private key may be interfered with the distributed quantum signatures. This prevents their scheme from being used in a realistic setting where the Distribution and Messaging stages can typically occur with a delay of days, weeks or even years.

2.2.4 *Removing quantum memory*

The requirement that recipients possess long-term and efficient quantum memory makes the above protocols impractical for realistic implementation. The removal of this requirement by Dunjko *et. al.* [43] was one of the major milestones towards a practical QDS which can be implemented.

The key insight of Ref. [43] was to effectively replace the quantum public key by a classical one, albeit one mediated by the distribution and measurement of non-orthogonal quantum states. This physical requirement is practical, relying simply on beamsplitters and photodetectors capable of distinguishing just between zero and nonzero photon numbers, such as avalanche photodiodes (APDs). The storage of classical public keys is clearly no restriction.

The main difference then between Dunjko's [43] and Gottesman's [41] protocols is that in Dunjko *et. al.* the state recipients perform measurement immediately upon receipt of the quantum states. Remarkably, despite this fundamental change to the nature of the protocol's one-way function, secure QDS is still possible.

In the Distribution stage of the protocol, Alice generates classical strings $\left\{k_j^m\right\}_{j=0}^{L}$, length L, corresponding to each future one-bit message m. The k_j^m are chosen uniformly at random from an alphabet of coherent state phases $\{-\alpha, \alpha\}$. Alice then forms sequences of coherent states $\rho = \otimes_{j=0}^{L} |k_j^m\rangle$ which she then distributes to Bob and to Charlie.

Bob and Charlie pass their received coherent states through a shared optical multiport, which serves to symmetrize their individual quantum states. That is, after the multiport Bob and Charlie's reduced density matrices are identical, which guards against Alice's repudiation attack. Bob and Charlie monitor their null-ports, which guards against repudiation attack or malicious activity during the state distribution. Bob and Charlie perform unambiguous state discrimination (USD) on the outputs of their signal ports, which will accurately distinguish between non-orthogonal states $|\alpha\rangle, |-\alpha\rangle$ at the expense that it will sometimes fail to give an answer.

6 Analogously to the key rate in QKD.

During Messaging, Alice will declare $\left\{m, k_j^m\right\}$ which recipients will compare to their USD outcomes. Provided that there are enough matches between Alice's phase declarations k_j^m and Bob/Charlie's USD outcomes, message m is accepted and the protocol has succeeded.

This first protocol avoiding the requirement for quantum memory shows that QDS may be both practical and secure. Furthermore the limited physical requirements – tensor-products of coherent states, beamsplitters and non-photon-number-resolving detectors – are feasible to work with, unlike the large number of superposition qubits required for Ref. [39] or the quantum memories required for Ref. [41].

An implementation of a variation of Dunjko's scheme is described in Ref. [44]. Collins *et. al.* modify Dunjko's scheme in two key ways. Firstly, a QPSK alphabet is used. This is in order to make the second modification: instead of using unambiguous state discrimination (USD) measurement, they perform unambiguous state *elimination* (USE) measurement. If the measurement succeeds, rather than being able to say definitively which state was received, a recipient can say with certainty which state was *not* received. The main advantage of the USE measurement scheme is that the probability that the measurement fails is significantly smaller than for USD, and so the resulting QDS scheme gains a boost in efficiency. Indeed, if the USE eliminates $N-1$ of N possible states, then one knows with certainty which state was sent. USD may be thus viewed as a special case of the more general USE measurement, and the shift from state discrimination to state elimination allows for much greater efficiency in QDS schemes.

Collins *et. al.* estimate a signature length $L = 5.1 \times 10^{13}$ in order to sign a message. Notice the subtle shift between Refs. [39] and [41–44]. While in Gottesman's protocol the number of recipients did not need to be determined until the Messaging stage, in later protocols it must be determined before Distribution. After the coherent states have passed through the multiport the number of recipients cannot be changed. Because of the physical requirements for the optical multiport, it will also be challenging to generalize to more recipients. Realistic implementation of the multiport also introduces noise and losses due to misalignment and instability, further reducing the efficiency of the protocol, and requires Bob and Charlie to be physically connected. In Ref. [42, 44], for example, Bob and Charlie are separated by 5 m of optical fibre.

2.2.5 *Removing multiport*

The fact that the QDS schemes discussed above require dedicated multiport hardware at the receivers makes implementation in real-world situations difficult. The multiport introduces losses and noise, and requires tricky synchronisation between Bob and Charlie in order

to correctly interfere the states. The experiment in Ref. [44] therefore has Bob and Charlie only separated by 5 m optical fibre.

To combat this, Wallden *et. al.* [45] propose two QDS schemes specifically designed to run over the same hardware platform as QKD. In particular, they get rid of the multiport which was previously used to symmetrize Bob and Charlie's reduced output states. Their key insight is that rather than symmetrizing their states, it is sufficient to symmetrize their measurement outcomes. Therefore, a step is added to the distribution stage in which Bob and Charlie randomly swap half of their measurement outcomes over a secure classical channel. If Alice can gain no information about which outcomes were swapped then she cannot repudiate.

This protocol was implemented by Donaldson *et. al.* in Ref. [46] in which a message is securely signed over distances 500 m, 1000 m, and 2000 m, with no requirement on the physical separation between Bob and Charlie. The secure classical link may be realised via QKD, and so Refs. [45, 46] begin to explore the close connections between these two different quantum communication protocols. We explore this further in Chapter 5. Donaldson *et. al.* achieve signature length $L = 1.93 \times 10^9$ using QPSK coherent states and USE measurement, which is a vast improvement over the $L = 5 \times 10^{13}$ required in Ref. [44] and means that secure quantum signatures may actually be both useful and practical.

The most difficult assumption which Refs. [41–44] make, however, is that there should be no eavesdroppers on the quantum channels. This is a strong and impractical assumption, and one which subsequent works have endeavoured to remove.

2.2.6 *Allowing Eve*

All signature schemes considered so far have made the assumption that the quantum distribution channels are secure and they may not be attacked or monitored by an eavesdropper, Eve. This is clearly an unrealistic and unphysical assumption, but was a sensible one while the pressing impracticalities of early QDS schemes (quantum memory, multiport, tricky state comparison tests) were overcome. The emphasis in earlier papers was on dishonesty internal to the protocol, i.e. which attacks can Bob or Charlie mount when they already hold perfect copies of the quantum public keys. However, in a realistic scenario it is clear that an eavesdropper *could* attack the quantum channels as states are being distributed, and so it is important to consider whether this has any effect on QDS security.

Amiri *et. al.* [47] provide a QDS scheme which allows for an Eve to eavesdrop on the quantum channels. In the worst-case scenario it is assumed that Eve will conspire with a dishonest internal player (Bob or Charlie in the case of a forging attack), and knowledge which

Bob/Charlie hold about their own quantum public key measurements is supplemented by knowledge learned through Eve's attack.

The key modification which Ref. [47] makes is to have Alice use *different* private keys (and so different sequences of quantum coherent states for her public keys) for each recipient. This means that the dishonest recipient is forced to eavesdrop on the honest recipient's quantum channel if he is to gain any information. This is in contrast to earlier protocols in which the dishonest recipient held a perfect copy of the quantum public key, which was identical to that of the honest recipient.

The protocol relies on sending weak attenuated coherent states with three different randomly chosen intensities, identically to decoy-state BB84 [48]. The coherent states are randomly polarized in one of two non-orthogonal polarization bases, and photon-number resolving detection in one (randomly chosen) polarization basis is performed at the receiver. The three different intensities are required in order to circumvent a photon-number splitting attack [49, 50]. Players gain classical binary strings, which are later compared during the Messaging stage. The protocol is secure provided that Bob's (Charlie's) string is closer[7] to Alice's string than any possible string which a dishonest eavesdropper can hold.

Because the security of discrete-variable QKD is advanced, the QDS protocol proposed in Ref. [47] is secured against coherent eavesdropping attacks[8] via an estimation of the smooth-min entropy [18, 51]. This is the commonly bounded quantity for analysis of quantum cryptographic protocols [52, 53]. Amiri *et. al.* note specifically that the quantum stages of their protocol are identical to the equivalent QKD protocols, with difference only in the classical postprocessing of measurement results. This becomes a common factor of many QDS protocols as they move towards realistic and practical implementation, even in commercial systems and installed fibers, and is a thread which we shall pick up again in Ch. 5.

Because the dishonest player is forced to eavesdrop, he in fact receives a worse copy of the honest player's public key than in the previously discussed protocols, and so somewhat counter-intuitively Ref. [47] requires only an estimated $L = 6 \times 10^8$ over 50 km fiber. Remarkably, this is *shorter* than previous protocols, despite relaxing a security assumption.

An experimental implementation of a protocol which is similar to Ref. [47] is described in Ref. [54], based on the protocol Ref. [55]. This protocol relies on distribution of decoy-state BB84 (attenuated coherent states of several different polarizations, as with Ref. [47]). The crucial difference betweens Refs. [47] and [54, 55] are that the

7 in Hamming distance.

8 We will discuss the hierarchy of eavesdropping attacks in Sec. 3.6.

latter use a larger set of non-orthogonal polarization bases, while Alice sends to Bob and Charlie identical public keys.

Yin *et. al.* [54] sign a 32 bit message over a distance of 102 km, making their experiment the longest implemented message to-date.

Finally, we note the recent work by An *et. al.* [56] which boasts an experiment with GHz clock rate based on Ref. [47], allowing for coherent forging attacks by Eve and requiring single-photon detectors at the receiver.

2.2.7 *Side-channel attacks*

It should be noted that "security" of a protocol is a theoretical statement, and not a physical one. A protocol is secure only with respect to a model of how it operates in the real world, and whether a so-called unconditionally secure protocol can be broken in practice depends on how realistic or practical its underling modelling assumptions are. For example, although in many QKD protocols Eve is allowed to attack the quantum channels and eavesdrop on all communication, she is assumed unable to attack the physical devices which implement the protocol.

For example, the QDS scheme presented in Ref. [47] relies on distribution and detection of attenuated coherent states in different polarization bases. A realistic Eve could attack the sending device in order to gain information about the polarization of the prepared state and so gain enough information to forge without detection even though the protocol is unconditionally secure against conventional types of eavesdropping attack.

An example of such a "side-channel" attack is the Trojan Horse attack presented in Ref. [57]. Here, Eve shines a bright laser pulse into Alice's device and measures the few back-reflected photons. These photons have picked up the same polarization which Alice imparted to her prepared state, and so Eve is able to infer the chosen polarization basis choice, giving her an undetected advantage.

To guard against side-channel attacks, honest parties have several options. One direction is to close known side-channels by additional protocol steps or additional hardware. Leakage of intensity-modulation information may be removed by using a passive decoy-state scheme, as in Ref. [58], which uses a parametric down conversion (PDC) source to generate photon pairs. The idler is used to estimate channel parameters, much like decoy intensity modulations were earlier, and the signal is projected into different non-orthognal polarization states. Although Zhang *et. al.* reach channel distances of 200 km, they require single-photon detectors cryogenically cooled to 2 K, and so it is difficult to see how this protocol could be implemented in a real-world scenario.

Against the Trojan Horse attack Alice and Bob could add additional filters to their devices to block out light at Eve's required wavelength. It was shown however that Eve can bypass this by breaking Alice's filters in a way that is undetectable to honest players [59]. Closing side-channels in this way may open up the protocols to additional attack methods, which must then be understood, modelled and reacted-to. This moves quantum cryptography into the same "cat-and-mouse" development cycles as conventional cryptography.

To break this cycle, and to provide genuinely unconditional security which is guaranteed against all conceivable side-channel attacks, there has been a recent push towards device-independent cryptography. The security of device-independent (DI) protocols makes no trust assumptions about the devices used and it may even be assumed that the devices are held by the malevolent party. DI cryptography is then based entirely on laws of quantum mechanics, specifically on the violation of a Bell inequality [60–62].

Full DI cryptography, while secure, is difficult to perform and may offer figures of merit which are too pessimistic for the desired application. One may compromise, then, and instead implement measurement device independent (MDI) cryptographic protocols, in which no trust assumptions are placed on the measurement devices (and they can even be owned by Eve), while the state-preparation and sending devices are held by honest parties and are trusted [63].

The first MDI QDS scheme is presented by Puthoor *et. al.* in Ref. [64], which requires only a characterization of the states which are distributed through the quantum channel. Crucially, no assumptions are placed on the detectors. An experiment by Roberts *et. al.* implements either MDI-QDS, MDI-QKD or regular QKD with a switchable setup [65]. By handing the untrusted measurement device to Charlie, and allowing Bob and Charlie to additionally share a QKD link, they securely sign a message between Alice and Bob situated 50 km apart. They also only require two quantum links, between Alice-Charlie and Bob-Charlie (with Charlie playing the role of Eve), which reduces the resource cost of distributing signatures across a network. Roberts *et. al.* sign a single-bit message in just 74 ms.

2.2.8 *Installed fibers*

There have been several experiments seeking to move secure QDS from the laboratory setting to a practical network of deployed fibers. The first demonstration of QDS over installed fibers [66] allowed for a single-bit to be signed in approximately one second over 90 km fiber, relying on a differential phase shift (DPS) quantum state distribution [67].

In this DPS-QDS protocol, sequences of coherent state pulses are distributed with complex phase either α or $-\alpha$, and information is

encoded in the phase difference between subsequent pulses [68]. Key to the long distances reached in this protocol is the move to telecom wavelengths 1550 nm, allowing the use of very low loss fibers.

H.-L. Yin *et. al.*, in a second implementation of MDI-QDS [69], securely sign a message over a deployed fiber network in approximately 40 hours using the protocol from Ref. [64], although they note that a full parameter optimization was not performed. Regardless, there has been quick and marked progress from early QDS experiments, assuming quantum memories and tricky detection methods which were unique to QDS, to the recent advanced experiments demonstrating, for example, unconditionally secure MDI-QDS over installed metropolitan fiber communication systems.

Both of these schemes, although running over deployed fiber networks, require difficult detection methods. Collins *et. al.* [66] rely on single-photon detectors, while Yin *et. al.* [69] is required to perform Bell measurements. Both of these require dedicated hardware not normally present in a standard deployed telecommunications network.

2.2.9 *Continuous-variables*

Despite the many recent advances in single-photon detection, and its progress towards practical implementation, the protocols presented above still require a dedicated hardware platform. Deploying such a platform will be difficult and costly, especially if it requires entirely new network infrastructure. An alternative approach is to build quantum cryptographic protocols specifically designed for integration with the classical telecommunications network.

The protocols discussed above, relying on single-photon detectors which give a discrete outcome (click or no click), fall within the discrete-variables category. These protocols boast a high level of theoretical development and mature security proofs, owing in part to the small Hilbert spaces in which their systems live. It should be no surprise, therefore, that while many protocols for quantum information processing are designed first for DV systems, they are often implemented first on a continuous variable (CV) platform [70].

CV quantum cryptography, relying on distribution of phase-encoded coherent states and heterodyne detection typically requires complex security proofs. An important issue is the infinite-dimensional Hilbert spaces in which the quantum states live. There are several properties of quantum states which hold for any finite dimension but which break in the infinite dimensional case [71]. Additionally, numerical methods which work efficiently at low dimension [72] cannot be implemented in the infinite-dimensional case without simplifying assumptions.

Despite this, the CV platform has preferable implementation. Optical homodyne and heterodyne detection are mature technologies routinely used throughout currently deployed telecommunications

networks, and they can run at GHz (or larger) clock-rates. Furthermore, these detection methods are highly efficient and run at room temperature. One is therefore motivated to pursue CV cryptography by the allure of its technological maturity and compatibility with already deployed architecture.

The first CV QDS protocol was proposed in Ref. [73] by Croal *et. al.* This protocol relied on distribution of QPSK coherent states, Fig. 1.3, and heterodyne detection of their phase. The structure of the protocol is similar to those discussed previously. Alice, for each future one-bit message she might send, first creates strings of classical information corresponding to a phase from the QPSK alphabet. She then creates sequences of the corresponding phase-modulated coherent states, and sends them through the quantum channel to recipients Bob and Charlie.

Bob and Charlie perform heterodyne measurement and receive a phase measurement outcome. Unlike the schemes discussed earlier implementing an unambiguous state discrimination [43] or unambiguous state elimination [46], the measurement used here may be interpreted as an "ambiguous state elimination" (ASE), which is a natural next step in the progression USD $\rightarrow$ USE $\rightarrow$ ASE. The heterodyne measurement outcome is used to eliminate one of the possible QPSK states, similar to Ref. [46]. The USE will always give the correct outcome (i.e. it will never eliminate the state which Alice has sent) at the expense of sometimes failing to give any outcome. In contrast the ASE will never fail to give an outcome, at the expense of sometimes eliminating the state which Alice did indeed send. So, while in Donaldson's protocol [46] the ideal minimum number of errors between honest parties is zero, for Croal [73] there will always be a minimum threshold of errors between honest parties, even in the ideal case.

Croal *et. al.* implement their scheme over a 1.6 km free-space channel, which makes Ref. [73] both the first demonstration of CV QDS and the first demonstration of free-space QDS. Surprisingly, the experiment reaches signature lengths $L = 7 \times 10^4$ to sign a one-bit message, shorter than previous protocols. This is partly due to the employed measurement scheme, and partly due to the technological maturity of the CV experiment and hardware. Because of the short signature length and the experimental clock-rate of 2.2MHz, Ref. [73] additionally boasts the shortest required time to sign a single-bit message, a fact which is noted in the recent QDS reviews Refs. [66, 74].

Despite these advances in CV QDS, Ref. [73] still makes the assumption that there can be no eavesdropper on the quantum channel. One of the main results of this Thesis is to relax this assumption, as performed in our recent work Ref. [75]. We will discuss this further in Ch. 3.

To summarise, in contrast to DV implementation, the CV quantum cryptographic platform typically boasts fast sending rates and ready

implementation with deployed network architecture, at the expense of being sensitive to channel loss and noise. The distances over which CV quantum cryptography is secure are limited, and so the conventional wisdom is that a future quantum cryptography network should use the fast CV protocols over short distances (metropolitan distances within cities would be a perfect application of this), while long-distance quantum communication should be performed using a DV protocol [76].

2.2.10 *Other directions*

Before we move on, it is worth spending a moment to acknowledge some directions of QDS research which are orthogonal to the impractical → practical narrative presented above.

Unconditionally secure classical digital signatures

It is important to note that unconditionally secure *classical* digital signatures schemes do exist [45, 77, 78]. For example, the protocol P2 proposed by Wallden *et. al.* [45] offers unconditional security requiring preshared classical keys. Similarly, the protocol [77] uses hash functions to securely sign a message. Both of these are unconditionally secure against even a quantum adversary.

Therefore, one may rightly ask why a future quantum-secure cryptographic network should not use one of these classical protocols. Indeed, there may be applications where one of these protocols is preferable to any quantum protocol. However, it is worth considering the full practical requirements of these protocols. For example, protocols [45, 77] each require secret preshared keys between all players.

Unconditional security for these schemes therefore realistically assumes QKD between participants in order to securely share the secret keys before the classical signatures protocol may be run. We may therefore denote these "classical" unconditionally secure schemes as "*indirect* quantum digital signatures," since in practice they will require first the distillation of secret keys (via QKD) and then classical postprocessing. It is not clear *a priori* whether this will be more or less resource intensive than the "direct" QDS schemes above, which perform the signatures task without first distilling secret keys. A promising indication that direct QDS may be often advantageous was given in Ref. [47], who noted that since QDS does not require the same costly reconciliation steps as QKD, there will be channels which cannot sustain QKD but for which direct QDS is still possible.

Longer channels

We have seen that the CV protocols are expected to be useful over the short intra-city distances, while DV cryptography will be most

practical over long distances. New protocols in each of these paradigms are regularly designed and implemented, boasting faster key rates over longer distances, and so one is drawn to the following question: for a given distance, is there a fundamental physical limit to the distillable key rate? Or, how does the maximum distillable key rate *for any protocol* scale with distance? This question was quantitatively answered by Pirandola *et. al.* [79] who revealed that the best achievable key rate R for a given channel transmittance η is

$$R \leqslant -\log_2(1-\eta). \tag{2.2}$$

This "PLOB"-bound[9] is an upper bound on the maximum key rate attainable for a given channel loss in a QKD setup. Crucially, the PLOB bound applies to a point-to-point QKD setup, without any quantum repeater to effectively amplify the quantum signal. For small η, we have an approximately linear scaling $R \approx \mathcal{O}(\eta)$.

Can this linear scaling be beaten? A recent proposal [80] effectively doubles the distance at which a given key rate can be distilled, by replacing a point-to-point QKD network, in which Alice and Bob share a direct quantum channel, with a three-node network. Alice and Bob each share a quantum channel of length L with Charlie, but share no quantum channel with each other[10]. Alice and Bob can be situated $2L$ apart from each other, but the maximum distance any quantum state has to travel is L. This new Twin-Field QKD leads to a super-PLOB scaling $R \approx \mathcal{O}\left(\sqrt{\eta}\right)$ of the key rate.

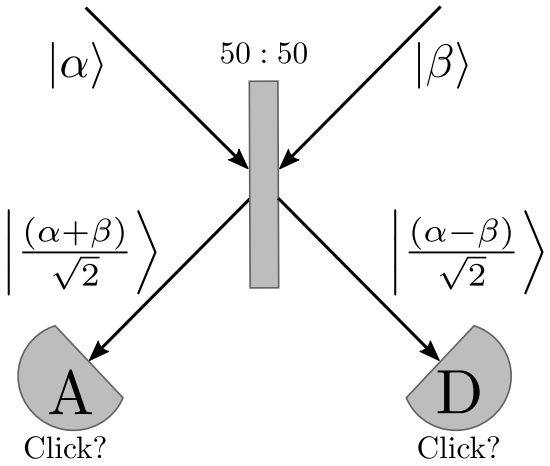


Figure 2.6: Eve's central node in the simplest TF-QKD setup [81]. Since the two incoming pulses are interfered Alice and Bob can know whether their initial state choices agree (A) or disagree (D), thus enabling them to generate a raw key. Perfect secrecy is then established by the usual error correction and privacy amplification routines.

9 So named after the authors of Ref. [79]: S. Pirandola, R. Laurenza, C. Ottaviani and L. Banchi.

10 Notice the strong similarities with MDI cryptography

In its simplest construction [81], in TF-QKD Alice and Bob each prepare coherent pulses $|\alpha\rangle, |\beta\rangle$, Fig. 2.6, chosen from some predetermined alphabet, and send then to Charlie. The central Charlie can even be a dishonest eavesdropper, so we will refer to them now as Eve. For illustration let us assume that Alice and Bob choose from QPSK, although more general alphabets are normally required [82, 83]. Eve interferes the incoming pulses on her beamsplitter, and performs single-photon detection on the two output ports. She then announces which detector, A or D clicked. Alice and Bob each publicly announce whether they prepared a state with real $(|\alpha\rangle, |-\alpha\rangle)$ or imaginary $(|i\alpha\rangle, |-i\alpha\rangle)$ displacement, and keep only the trials for which they both displaced in the same basis. In the ideal case, if for example the real basis was chosen then if detector A clicks it means $\alpha = \beta$, whereas if detector D clicks it means that $\alpha = -\beta$. using this information, combined with their own knowledge about what they sent, Alice and Bob can generate a key with each other. The TF-QKD is thereby able to double the possible distance between Alice and Bob for a given key rate, and since the central node is assumed to be under Eve's control it is inherently MDI.

Theoretical and experimental development of TF-QKD is ongoing, owing both to its promise of long composite channel lengths without the requirement of a quantum repeater, and its inherent measurement device independence without requiring a tricky bell-state measurement. The key practical challenge of such a system is path length matching between the Alice↔Eve and Bob↔Eve channels, to ensure that the pulses correctly interfere on the central beamsplitter. This is likely to require active stabilisation and monitoring of incoming pulses [80], the full security implications of which are yet to be determined.

General advances and open questions

Each of the QDS protocols which we described have assumed that there are only three players: one sender (Alice) and two recipients (Bob and Charlie). This simplifies the security analysis and allows a focus on the key aspects of security for each scheme. However in realistic contexts it may be desirable to allow for more than two recipients. In this case new attack strategies are possible and so careful attention must be paid to whether a particular QDS scheme remains secure against conspiracies of multiple dishonest players. Arrazola *et. al.* [84] consider QDS with many recipients.

Similarly, a simplifying assumption which each protocol has made was to assume that Alice wished only to sign a single-bit message $m \in \{0, 1\}$. It is clear that by iterating each protocol longer messages may be signed, but a naive and identical repetition of the distribution and messaging steps opens up new attack strategies. The works [85, 86] propose iteration methods for successful signing of longer messages which are applicable to any of the above QDS protocols, which require

still linear scaling of L with $|m|$. It is not yet clear what the optimal procedure for signing long messages is, or whether the scaling $L \propto 2^{|m|}$, from a naive iteration, can be beaten.

Finally, we note that while some recent advances in QKD, such as measurement device independence or passive decoy-states, have been translated into the QDS context, there are many recent developments which have not yet been leveraged by QDS. For example, there as yet no QDS equivalent of device-independent scenarios such as fully DI [60], detector-DI [87] or one-sided DI [88]. There are only preliminary theoretical developments of a twin-field [80, 82] QDS protocol [89] which promises to increase the possible channel lengths over which the scheme remains secure. More exotic developments such as counterfactual communication [90–93] also have yet to be translated to the QDS task.

Even developments in CV QKD, such as the recent proof of unconditional security against coherent attacks for Gaussian-modulated coherent states [94] have yet to find an analogue in QDS. Indeed, any fully-Gaussian QDS is missing, and future work should seek to rectify this. A clear motivation for doing so is that description of fully-Gaussian QKD relies only on finite-dimensional covariance matrices size 8×8 [95] and so the problems with modelling and numerics on the infinite-dimensional Hilbert space can be avoided. Indeed, an assumption about the Gaussianity of the QPSK alphabet (which is increasingly valid as the states' amplitude tends towards zero) was even a necessity for the recent developments in numerical semi-definite programming (SDP) methods for QPSK-based QKD [96]. Unfortunately, it is not immediately obvious whether any of these results for fully-Gaussian QKD can be utilised in the existing CV QDS protocol, since the ASE measurements used in Ref. [73] break Gaussianity. Fully-Gaussian QDS therefore remains an exciting, but still open, question.

2.2.11 *Summary*

Quantum Digital Signatures protocols perform a fundamentally different task to the more familiar QKD protocols. The goals of QDS, message authentication and transferability, are important tasks which are routinely performed by computationally secure classical algorithms in our day-to-day information infrastructure. In recent years the security of QDS has been catching up with QKD, and security proofs against an eavesdropping attack [47, 55] or for QDS in the MDI setting [64] have been proposed, and their respective protocols have been implemented.

Despite this, and despite their immediate practical advantages for implementation, continuous variables (CV) QDS protocols have been an under-researched platform for secure digital signatures. A recent

work [73] has proposed, proved security, and implemented a CV QDS protocol involving discretely-modulated coherent states and heterodyne detection. The protocol assumed secure quantum channels, and until Ref. [75], which constitutes part of this Thesis, there has been no security proof which allowed for an eavesdropping attack on the channels.

2.3 HOW TO SHARE A SECRET

A secret sharing scheme allows for secure splitting and distribution of classical information among multiple recipients, an unknown subset of whom may be dishonest. The canonical example of such a scheme is that of a bank. The head of the bank, Alice, wishes to distribute keys to the vault between several potentially untrusted deputies. If the deputies work together and use their keys simultaneously they are able to access the vault, but any nefarious deputies working alone should not be able to gain access.

2.3.1 *Classical secret sharing*

Although many existing classical secret-sharing schemes are already information-theoretically secure [34, 35], they may encounter problems when distributing shares of the secret across insecure channels. This is analogous to the classical unconditionally secure signature schemes [45, 77] discussed in Sec. 2.2, which implicitly required an underlying QKD encryption. Thus we may ask whether it is more or less resource-efficient to first run pairwise QKD between players, or to run a "direct"-QSS scheme without first distilling pairwise secret keys. We should expect interesting parallels between QSS and QKD, since intuitively they are very similar, both effectively performing encryption of classical messages.

Let us consider some examples. Alice wishes to share a secret, m, between n players, such that any $k \leqslant n$ of them can access m. The general framework for this is called an (n, k)-threshold scheme, where of the n players any subset of k players can reconstruct the secret. An information-theoretically secure threshold sharing scheme was designed by Shamir in Ref. [34]. Shamir's scheme relies on polynomial equations over finite fields, and is provably secure even against an adversary with infinite computing power.

For example, Alice wishes to distribute a secret m between four players, such that any three of them can access m. Alice generates a prime number p, and the polynomial

$$\left(ax^2 + bx + m\right) \quad \text{modulo} \quad p. \tag{2.3}$$

Prime p should be chosen larger than any of the coefficients a, b or m. Alice then evaluates this polynomial at four different points x, and

sends the outcomes to each player. These points will be referred to as "shares".

The polynomial has three unknown coefficients, a, b and m, and so any three players can combine their shares to create three equations, which may be solved for each unknown. Any fewer shares will yield an underdefined system which cannot be solved. An attempt to guess the final share will show that any message m can be the secret, and so such a guessing attempt is useless.

Another threshold secret sharing scheme was built on similar principles by Blakley [35]. In this scheme, the message m is defined as a point in a large k dimensional space. Each share is then a hyperplane in a $k-1$ dimensional space, which includes the point m. It therefore requires the intersection of all k hyperplanes to reveal m. For example, if Alice again wishes to share a secret between four players, such that three of them are able to access m, then each share is a two-dimensional plane. The intersection of any two planes is a one-dimensional line containing m, and the third plane is required to reduce this line to the point m.

While both of these schemes are information-theoretically secure once the shares have been distributed (assuming that each share is securely stored and cannot be stolen), the main issue arises when considering how the shares can be distributed in the first place. If a malevolent party can access the shares during distribution then they can reconstruct the secret. In implementation, Shamir's and Blakley's schemes are therefore only as secure as the underlying encryption which is used to share the shares.

2.3.2 *Quantum secret sharing*

We therefore wish to investigate whether the task of secret sharing can be made secure using quantum resources. It is important to notice that the translation from classical secret sharing to quantum secret sharing is not straightforward, and there are at least three directions which one can pursue:

- quantum-assisted classical secret sharing (qCSS): encrypt a classical secret sharing protocol [34, 35] using quantum resources. For example, perform pairwise QKD between Alice and each recipient, then encrypt the shares of the classical secret sharing protocol. This is analogous to the classical unconditionally secure schemes discussed earlier.

- quantum secret sharing (QSS): use quantum states to securely distribute shares of a classical secret.

- quantum state sharing (QStS): securely distribute shares of a quantum state.

Quantum state sharing is an important and exciting research direction in its own right and helps to establish the close links between quantum secret sharing, QKD and quantum teleportation [70, 97, 98]. Despite the fact that both QSS and QStS are natural extensions of classical secret sharing to the quantum realm, and despite the fact that early work [97] proposes related protocols for each task, it should be understood that they are distinct quantum tasks with different goals and hardware requirements. For the rest of this Thesis we will restrict ourselves to QSS. In what follows we will only refer to the first two options as "quantum secret sharing", while the third option we shall refer to as "quantum state sharing".

2.3.3 *Entanglement-based QSS*

All three directions, qCSS, QSS and QStS, are discussed at length in the pioneering work by Hillery *et. al.* [97]. They propose the use of a GHZ resource state

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) \tag{2.4}$$

shared between three players, which can be used to distribute shares of a classical secret. Collaborating recipients can recover the secret while a dishonest subset of players cannot. Alternatively, the GHZ resource state may be used to distribute shares of a quantum state (for QStS), such that collaborating players may reconstruct the original quantum state while a dishonest subset of players can gain no information.

For QSS, each player chooses independently and at random to measure their state in either x or y basis:

$$|\pm x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right),$$
$$|\pm y\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \pm i|1\rangle\right).$$

If, for example, all three players measure in the x basis, then Charlie can infer from his measurement outcome whether Alice and Bob's measurements are correlated or anticorrelated. By collaborating, then, Bob and Charlie can accurately infer Alice's bit. In fact, whenever Alice and Bob measure in the same basis, Charlie must measure in x in order to gain information. Conversely, if Alice and Bob measure in opposite bases then Charlie must measure in y, otherwise he gains no information. We see, then, that since each player randomly chooses which basis to measure, 50% of the resource GHZ states will yield no information, and are effectively discarded.

Despite its high resource requirement, and despite the fact that 50% of the resource states are wasted, Hillery's protocol has influenced the direction of all subsequent QSS protocols, and the paper was instrumental in demonstrating that multipartite entanglement is

an important resource for quantum communication protocols. Multipartite entanglement is difficult to create and manipulate, and will degrade quickly as it is distributed over a quantum channel exposed to realistic loss or noise. However, just as QKD has an equivalence between entanglement-based and prepare-and-measure versions [95, 99], it should be expected that the requirement of large multipartite state in Ref. [97] can likewise be reduced [100–103].

To accomplish this, Karlsson *et. al.* [100] propose an entanglement-based QSS scheme which, rather than relying on creation and distribution of the GHZ state, relies on distribution of *pairs* of entangled qubits in a Bell state. This configuration allows for correlations between players to be established identically to Hillery's scheme, but with more readily accessible resources. Recipients Bob and Charlie can determine with certainty which Bell state Alice sent, which allows Alice to establish a key with Bob/Charlie, and which may subsequently be used to encrypt a message.

This protocol drastically reduces the resource requirements for experimental QSS, but the resulting protocol is still tricky to implement. The protocol requires Bell states and superpositions of Bell states, which will degrade over a realistic channel. The protocol also introduces a fundamental asymmetry into QSS at the quantum level. While in Hillery's protocol protocol any of the three players can be chosen as dealer even after the GHZ state has been distributed, for Ref. [100] it is established at the time of quantum state distribution that Alice is dealer.

Both the protocols from Hillery [97] and Karlsson [100] assume perfect state creation and noiseless and lossless quantum channels. This is an unrealistic assumption and one which must be relaxed before entanglement-based QSS can be implemented securely.

Chen *et. al.* [104] modify the Hillery's protocol [97] to allow for an imperfect distribution of entangled state. By proposing a method for entanglement distillation on a multipartite state, which can be used before a cryptographic protocol, Chen effectively reduces the extreme resource requirement of protocols like Ref. [97]. The resource state used does not even need to violate a Bell inequality.

An important generalization of Hillery's scheme allows for analysis of the optimal entangled states required to share a secret between more than three players. While one option would be to simply replace the resource state with the N-partite GHZ state

$$|N-GHZ\rangle = \frac{1}{\sqrt{2}}\left(|000\ldots0\rangle + |111\ldots1\rangle\right) \tag{2.5}$$

another option is to generalize to graph states [98, 105–107], under which the tasks qCSS, QSS, QStS and entanglement-based QKD may be united and described within the same framework. One advantage of using such a state is that it can allow for QSS to be completed without collaboration from all recipients, which may help practical

QSS to be robust and prevent against denial-of-service attacks from a dishonest internal player[11].

There have been several attempts to prove security of entanglement-based QSS. As we have seen, security proofs based on highly-entangled GHZ states or graph states become insecure once realistic channel parameters are considered, even though they offer unconditional security in the ideal limit. One way to tackle this is to borrow tools from entanglement-based QKD. Kogias *et. al.* [108] use similar analysis to so-called one-sided device-independent (1sDI) QKD [88, 109] in order to prove QSS security while modelling channel effects on their CV resource state.

Key to Kogias' protocol is the assumption that neither the measurement device of Bob, nor of Charlie, should be trusted. Rather, each player is assumed to possess a black-box which can output one of two measurement outcomes, corresponding in the honest case to homodyne measurement in either x or p quadrature. Protocol security is based on monogamy of entanglement and employs an entropic uncertainty relation which makes no assumption about the action of a dishonest player. To our knowledge Ref. [108] marked the first full security proof of QSS, against all forms of dishonesty and all types of attack over realistic channels. It was later shown that the resource required for entanglement-based QSS is two-way steering of the shared state [110], where the optimal Gaussian resource states for a given energy were also considered.

The links between QSS and 1sDI QKD considered in Ref. [108] hint at an interesting direction for exploration: what is the relationship between QSS and other quantum communication protocols? It was already shown in Ref. [98] that qCSS, QSS and QStS may be united under the same framework using graph states, while even in Hillery's original work [97] the links between qCSS and QSS were acknowledged. Additionally it can be shown [97] that a QStS protocol may be readily constructed from a teleportation protocol plus QSS (or qCSS or QKD) scheme if Alice teleports a quantum state to Bob, but sends the classical information required for state reconstruction to Charlie.

There are strong links between QSS and quantum conferencing [107, 111] which is a natural multipartite generalization of QKD in which N players receive identical keys. Indeed, as shown in Refs. [107, 111] the same resource states and network configurations may be readily used for both QSS and quantum conferencing. It is an open question however whether these additional tasks have the same optimal requirements [108, 110] on the resource state as QSS.

11 Though we note that even QKD is susceptible to denial-of-service attack where Eve simply destroys the quantum (or classical) channels between Alice and Bob.

2.3.4 *Sequential QSS*

The above protocols which implement QSS using entangled resource states offer an advanced level of security and neatly demonstrate the important role of entanglement in quantum communication. However, it is hard to see how they will be preferable to qCSS which can offer equivalent levels of security for the same task, but without the problems associated with generation and distribution of large entangled states. An entanglement-based scheme may even be fine if the number of players is small – for example the scheme [100] relies only on Bell-pairs, but they cannot be easily scaled to many parties. We note that qCSS scales much more favourably as the number of required quantum channels is linear in the total number of players.

It should still be explored whether there are any QSS protocols which outperform qCSS. One promising direction is that of sequential[12] QSS in which the QSS task is fulfilled by sharing of a single quantum system between multiple players.

In the first sequential QSS protocol [112], Zhang *et. al.* propose a system in which Bob prepares a single photon state with his choice of polarization and sends it to Charlie. Charlie performs a unitary operation, either the identity, a Hadamard gate or a bit-flip, on the photon and sends it to Alice who stores the photon in a quantum memory. This process is repeated many times. Later, Alice will sample some of her stored photons for errors by asking Bob and Charlie to declare which state was sent and which operation was performed. She then performs the claimed operation, and measures the claimed basis, in order to check for errors.

On the remaining photons Alice performs her unitaries (either the identity or a bit-flip) to encode her secret. She then sends the photons back to Charlie. If Bob and Charlie collaborate they can deduce the correct basis in which to measure Alice's photon, and so recover her information.

Sequential protocols have the obvious advantage that large entangled states are not required. Even though Ref. [112] proposes to use a quantum memory it is ultimately not necessary for the protocol, and the work by Schmid *et. al.* demonstrates this in a sequential QSS experiment [113]. Their experiment, in which players perform operations on heralded single photons, allows for a secret to be shared among six players in a setup which is much more readily scalable to more players than the earlier QSS schemes requiring entanglement.

Schmid's scheme relies on sequential interactions with a qubit state encoded into the polarization of a heralded single photon. Each player imposes a randomly chosen phase onto the state

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \rightarrow \frac{|0\rangle + e^{i\phi_k}|1\rangle}{\sqrt{2}} \tag{2.6}$$

12 Sometimes referred to as entanglement-free QSS.

and so at the end of the distribution the state is

$$\frac{|0\rangle + \exp\left(i\sum_k^N \phi_k\right)|1\rangle}{\sqrt{2}}. \tag{2.7}$$

The final player measures in the $|0\rangle \pm |1\rangle$ basis. Collaboration of the first $N-1$ players allows them to infer, with certainty, the N^{th} player's outcome.

This sequential scheme, while secure against an Eve external to the protocol, is difficult to secure against dishonesty from one of the internal players [114–116]. For example, Ref. [116] points out that the order in which recipients declare their information is of utmost importance, and this is adopted into the sequential protocol in Ref. [117]. Unfortunately, the protocol remains insecure against a so-called Trojan Horse attack [114], in which an internal player to the protocol adds one mode of an entangled state to the single photon as it is being distributed. This entangled mode will undergo the same subsequent gates as the signal photon, granting the dishonest player additional information.

The Trojan Horse attack is guarded against in the recent work from Grice *et. al.* [118]. In their protocol for sequential QSS, each player creates a coherent state which is chosen from a Gaussian modulation. These states are added to the initial coherent state as it travels, and the final state is heterodyned by the dealer, Alice. With combined knowledge of their injected states, the players are able to estimate Alice's measurement outcome. This protocol has the advantage of high tolerable losses, especially when compared to entanglement-based QSS. Crucially, the scheme is immune to Trojan Horse attacks since once a coherent state has been added to the total state, it only interacts with Alice's measurement apparatus and does not pass through the equipment of any other player. Additionally a dishonest player cannot access other players' devices.

Owing to its simplicity of implementation QSS has been performed in many experiments [113, 119] including those explicitly using telecom fiber networks [120]. This latter work, Ref. [120], demonstrates QSS in two experiments between three players and four players using phase encoding of single qubits. Their implementation uses a Sagnac interferometer, with light travelling in two directions around a loop. The light is at standard telecom wavelengths 1550 nm and channel lengths are between 50 and 70 km, rendering secure QSS eminently practical.

2.3.5 *Summary*

Quantum Secret Sharing has been an intense field of active research for the quantum communications community for the last two decades. Entanglement-based QSS boasts a high level of provable security

against both internal and external dishonesty. While there have been some proof-of-principle demonstrations of these QSS schemes [101, 121–123] the style of protocol is still far off routine and practical implementation.

In contrast, sequential QSS involving sharing of a single quantum system is much more practical for implementation, and has been demonstrated in realistic settings with many players [113, 119, 120]. However, these protocols face difficulty against a dishonest player internal to the protocol, which is precisely the context which secret sharing should guard against. Moreover, even though these schemes do not require generation or distribution of entangled states, they still require a dedicated hardware setup in order to distribute the quantum state and perform sequential measurements. To our knowledge, the most plausible protocol in terms of both its security and practicality, that of Grice *et. al.* [118], is yet to be implemented.

It is therefore yet unclear whether these quantum secret sharing protocols will give an advantage over the quantum-mediated qCSS protocols which we have discussed in Sec. 2.3.1. The underlying quantum encryption algorithm, QKD, boasts advanced security proofs and intensely researched hardware, and any proposed QSS scheme must be benchmarked against a QKD-based classical protocol which performs the same task.

3

QUANTUM DIGITAL SIGNATURES

In this chapter we introduce and investigate a continuous-variable Quantum Digital Signatures (QDS) protocol, which allows for secure authentication of classical messages even against a quantum adversary. We describe the protocol and its similarities and differences to recent QDS protocols from the literature in Sec. 3.1, and then prove its security against several different attack strategies in Secs. 3.2-3.6. It is only recently that QDS protocols in the discrete-variable regime have been proven secure against an eavesdropping attack on the quantum channels [47, 55], and the work in this chapter marks the first time that continuous-variable QDS is proven secure against an eavesdropper. Finally, in Secs. 3.7-3.9 we analyse the performance of our protocol, including a postselection technique to improve performance, and demonstrate that a remarkably small number of quantum states are required to securely sign a message. Our protocol is implemented in Chapter 5.

3.1 OUR QDS PROTOCOL

In the simplest instance we may consider a signature scheme involving only three parties: a sender, Alice (A), and recipients Bob (B) and Charlie (C). Alice wishes to send a classical message m to B and C, such that B and C can correctly determine whether m was indeed sent by A. Furthermore the recipients should be able to check whether m has been altered. The three-party setting is the smallest setting to fully distinguish a digital signatures protocol from related protocols such as MACs[1]. Because more than two (potentially dishonest) players are present, this allows for new attack strategies which distinguish QDS from other quantum tasks such as QKD.

3.1.1 *QDS setup*

Our signature scheme is displayed pictorially in Fig. 3.1. Alice (A) wishes to send a message m to Bob (B) and Charlie (C) such that both Bob and Charlie accept it as genuine. To accomplish this she appends to m a signature σ_m which should be unique to the message and uniquely generated by Alice. In this way our digital signatures scheme is a quantum generalization of Lamport's protocol [24, 38]. As we shall see later, any player in our protocol may be dishonest.

1 Message Authentication Codes. See Ref. [24].

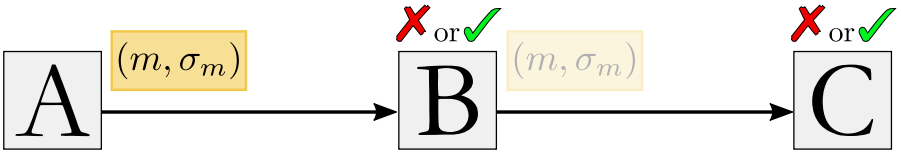


Figure 3.1: Setup of a 3-party digital signatures scheme. Alice (A) wishes to securely sign her message m such that Bob (B) and Charlie (C) both accept it as genuine.

3.1.2 *Goals of a signature scheme*

A digital signature scheme must fulfill the requirements outlined in List. 3.1. If requirement 1 (security against forgery) holds then no dishonest player will be able to impersonate Alice, which fulfills requirement 2 (genuine sender). In order to do so they will be required to generate σ_m which at the start of the protocol is known only to her. The dishonest player's only hope for successful impersonation is to take Alice's place at the start of the protocol and perform a so-called "man-in-the-middle" attack. We do not investigate this possibility further, though we note that without previous authenticated interaction between players even QKD is insecure for this attack [124].

For our scheme involving three parties, requirements 3 and 4 are equivalent. A QDS protocol involving N recipients may distinguish between non-repudiation and transferability by defining a message $m^{(k)}$ as k-transferable if it may be successfully forwarded up to k times. An honest participant should be able to determine the transferability level of m [84], while non-repudiation then refers to Alice's ability to cause a message to be non-transferable. In what follows we treat these requirements as equivalent.

A digital signature scheme which rejects all messages trivially fulfills requirements $1-4$, and so in order to get a useful digital signature scheme we must also impose requirement 5.

1. *Security against forgery*, Fig. 3.2a. Neither a dishonest recipient (B or C), nor an external fourth party (Eve, E), should be able to alter m and have it accepted as genuine by an honest recipient. The signature scheme should ensure that m is the message which Alice sent.

2. *Genuine sender*, Fig. 3.2a. Neither a dishonest recipient (B or C), nor an external fourth party (Eve, E), should be able to impersonate A. Any message which falsely claims to have originated with Alice should be rejected.

3. *Security against repudiation*, Fig. 3.2b. A dishonest sender A should not be able to cause disagreement between B, C about the previous two requirements. After genuinely sending m she should not later be able to deny it, and if Bob accepts the message as genuine then so too should Charlie.

4. *Message transferability*, Fig. 3.2b. If B accepts a message as genuine, then he should be sure that C will also accept.

5. *Robustness*, Fig. 3.2c. The message m should be accepted if all players behave honestly and there is no tampering by an eavesdropper.

List 3.1: A secure QDS scheme should fulfill each of the above requirements. Requirement 1 implies requirement 2. In our 3-party setting, requirements 3 and 4 are equivalent. We depict each type of attack which a QDS scheme must prevent in Fig. 3.2.

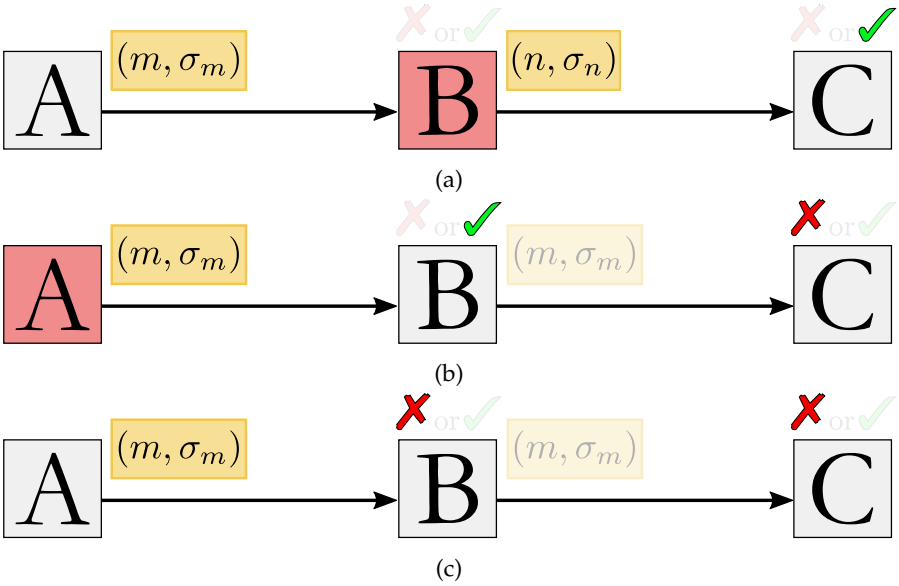


Figure 3.2: The multipartite setting permits many different methods for attack on the protocol depicted in Fig. 3.1. Gray boxes depict honest players while red boxes depict dishonest players. (a) Forging attack with dishonest Bob. Bob will change the message $m \to n$ with fake signature σ_n. The attack succeeds if Charlie accepts. Alternatively, either Charlie or a fourth player, Eve, may attempt a forging attack against an honest player. (b) Repudiation attack with dishonest Alice. Alice tries to convince Bob to accept the message and Charlie to reject it. (c) Honest failure: all players behave honestly but the protocol fails and both Bob and Charlie reject m. A protocol which does not fail due to honest failure is called robust.

3.1.3 *QDS protocol description*

We here present a continuous-variable (CV) QDS protocol based on the quadrature phase-shift keying (QPSK) alphabet of coherent states, Fig. 1.3. For the first time in a continuous-variables QDS protocol, our protocol takes into account insecure quantum distribution channels and permits the presence of an eavesdropper. Surprisingly, the same step of the protocol which ensures security against eavesdropping also makes the protocol efficient in its use of quantum resources. We shall see later in Sec. 3.9 that we outperform recent comparable QDS protocols.

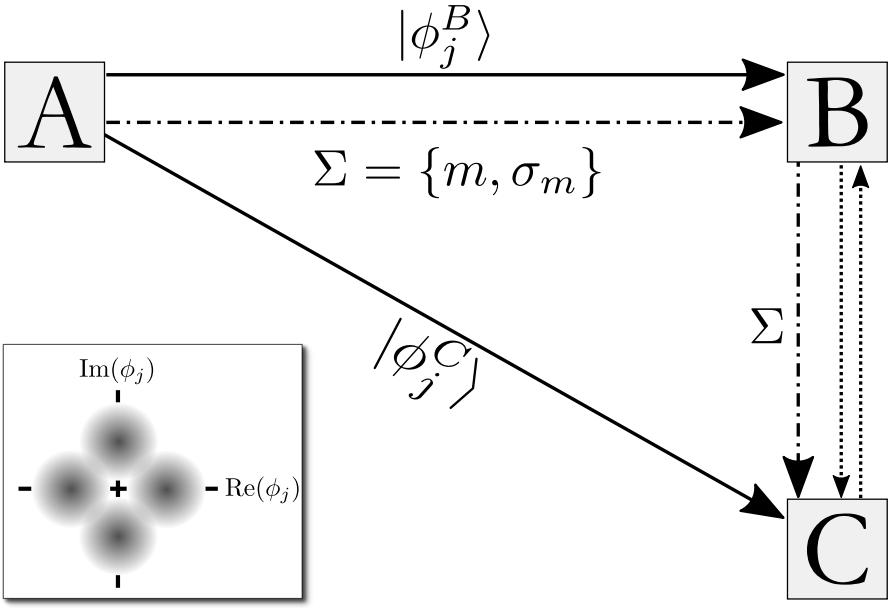


Figure 3.3: Setup of the QDS protocol considered in this chapter. Alice (A) wishes to securely sign a 1 bit message m. Alice distributes quantum coherent states $|\phi_j^{(B,C)}\rangle$ along insecure quantum distribution channels (solid lines) during the Distribution stage. Bob and Charlie swap eliminated signature elements via their securely encrypted classical channel (dotted lines). During the Messaging stage Alice sends Σ, containing her message m and her corresponding signature σ_m along a classical broadcast channel (dot-dashed line). Inset: QPSK alphabet.

Our QDS scheme is split into two stages, Distribution and Messaging, which, by analogy with classical digital signatures, may occur with significant time delay. Quantum states are sent and measured during Distribution. During Messaging Alice will send her message and classical signature, and recipients Bob and Charlie will try to determine its validity.[2] Our protocol setup is outlined in Figs. 3.1, 3.3.

2 Note the intrinsic separation between the Distribution (quantum) and Messaging (classical) stages of the protocol. We will take further advantage of this separation between quantum and classical steps in Chapter 5

We will now describe in detail the running of the protocol.

Distribution stage

STEP 1. Alice wishes to send a signed 1 bit message m to Bob and Charlie. For each possible future m, and for each recipient, Alice creates the following classical strings

$$\Phi_m^{(B,C)} = \left\{ \phi_{j,m}^{(B,C)} \right\}_{j=1}^{L} \tag{3.1}$$

which are of length L. The ϕ_j are complex phases chosen uniformly at random from the QPSK alphabet. The strings $\Phi_m^{(B,C)}$ may be interpreted as Alice's *private key*. The signature length $L \in \mathbb{N}$ is chosen to ensure the desired level of security.

STEP 2. Corresponding to each private key, Alice forms the following quantum states

$$\rho\left[\Phi_m^{(B,C)}\right] := \otimes_{j=1}^{L} \rho\left[\phi_{j,m}^{(B,C)}\right] \tag{3.2}$$

with

$$\rho\left[\phi_{j,m}^{(B,C)}\right] := |\phi_{j,m}^{(B,C)}\rangle \langle \phi_{j,m}^{(B,C)}|$$

understood to be the coherent state from QPSK with phase corresponding to the relevant element of Alice's private key.

The states Eq. 3.2 may be interpreted simply as sequences of coherent states, and correspond to Alice's *public key*. An important difference between quantum and classical digital signatures is that here the public key may no longer be freely distributed, copied and stored. We also note that Alice no longer has a single public key for each message (unlike Lamport's scheme [38]), and her quantum public key differs both for each possible m and for each recipient (unlike the recent scheme Ref. [73]). This is a requirement for security against an eavesdropping forger, Sec. 3.4.

STEP 3. Each recipient B, C performs heterodyne detection on their received coherent states, and receives outcomes (q_{out}, p_{out}) which we will write as $z = q_{out} + ip_{out} \in \mathbb{C}$. Crucially, since measurement is performed immediately on receipt of the states no quantum memory is required. The remainder of the protocol is entirely classical.

At the end of the quantum stage of the protocol, recipients Bob and Charlie now possess classical strings, length L, containing their phase measurements on Alice's distributed states. They now form *eliminated signatures*, Fig. 3.4. For each $z \in \mathbb{C}$, recipients record the phases $\phi_{j,m}^{(B,C)}$ which Alice was *least likely* to have sent. At position j this may be understood as computing the four conditional probabilities

$$p\left(\phi_j \mid x_j\right) \quad \text{for each phase} \quad \phi_j \in \text{QPSK}, \tag{3.3}$$

Element	QPSK elements	Heterodyne outcome
e_1	$\|-\alpha\rangle, \|-i\alpha\rangle$	$q_{out} > 0, p_{out} > 0$
e_2	$\|-i\alpha\rangle, \|\ \alpha\rangle$	$q_{out} < 0, p_{out} > 0$
e_3	$\|\ \alpha\rangle, \|\ i\alpha\rangle$	$q_{out} < 0, p_{out} < 0$
e_4	$\|\ i\alpha\rangle, \|-\alpha\rangle$	$q_{out} > 0, p_{out} < 0$

Table 3.1: We denote possible eliminated signature elements as e_1, e_2, e_3, e_4, and display their corresponding states from QPSK and their requisite heterodyne measurement outcomes.

and recording the two ϕ_j which yield the smallest of these. This record of ϕ_j forms the j^{th} element of their eliminated signatures. We note that the ϕ_j comprising the eliminated signature element will always be adjacent in phase space, and an example of this elimination procedure is displayed in Fig. 3.4. We denote Bob and Charlie's total eliminated signatures at this stage as $X_m^{(B,C)}$. Each is of length L and they will later be compared to Alice's private key in order to test the validity of the message. We display the possible eliminated signature elements and their requisite heterodyne outcomes in Tab. 3.1.

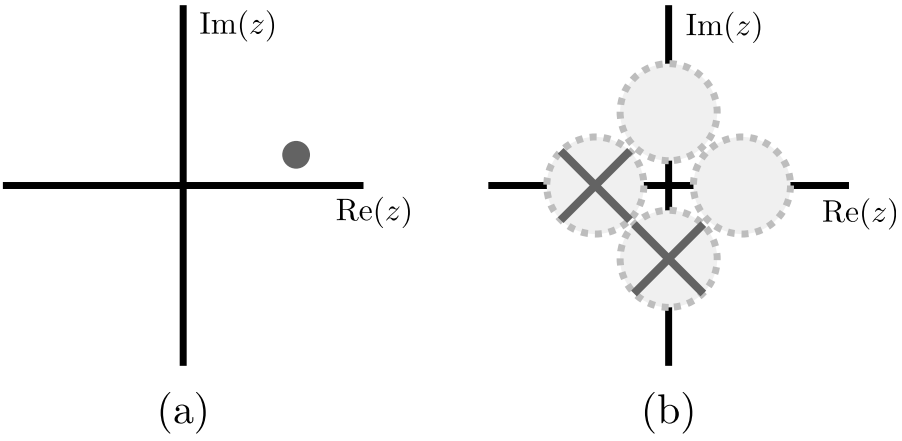


Figure 3.4: Bob and Charlie each perform heterodyne measurement on their received coherent states, and obtain (q_{out}, p_{out}). We define $z = q_{out} + ip_{out}$, which is the dark gray circle in (a). From their z, Bob and Charlie then record the two states from QPSK which are least likely to have been sent by Alice, (b). We display the possible eliminated signature elements and their requisite heterodyne outcomes in Tab. 3.1.

STEP 4 *symmetrization:* Bob and Charlie now swap a random $L/2$ elements of their $X_m^{(B,C)}$ over their encrypted classical channel. Signature elements which have been forwarded by a player will no longer be used by him in the protocol. We denote these resulting strings as $Y_m^{(B,C)}$. By using an encrypted classical channel the positions and values of swapped elements are kept secret from Alice, which will ensure that the information which Bob and Charlie each hold is symmetric from Alice's point of view [43, 45].

In other words, at the end of Step 3, having sent the state $|\phi_{j,m}^B\rangle\langle\phi_{j,m}^B|$ to Bob, Alice knows that Bob holds the corresponding eliminated signature element $X_{j,m}^B$, even though she doesn't know its value. Since Alice knows which state she sent to Bob, she may gain an advantage in trying to guess $X_{j,m}$. At the end of Step 4 however, Alice does not know whether it is Bob or Charlie who holds $X_{j,m}^B$. This uncertainty will prove crucial for preventing successful repudiation.

Bob (Charlie) now possesses an eliminated signature $\tilde{X}_m^{(B)}$ in two halves: one half $Y_m^{(B)}$ ($Y_m^{(C)}$) containing those elements received directly from Alice, and one half $Z_m^{(B)}$ ($Z_m^{(C)}$) containing elements received during this Symmetrization step from Charlie (Bob).

The key parameters for the Distribution stage are the signature length L, which directly measures the quantum resources required for the protocol, and the alphabet parameter α, related to the average photon number of the distributed coherent states. Channel parameters such as loss and thermal noise will be discussed later[3].

Messaging stage

Messaging may occur at any time after Distribution.

STEP 5. To sign m, Alice sends to Bob the classical information $\Sigma = (m, \sigma_m)$, consisting of the message m which she would like to convey, and her private key $\sigma_m = \left(\Phi_m^B, \Phi_m^C\right)$ consisting of declared phases, which acts as m's signature.

STEP 6. Bob rearranges $\sigma_m \to \tilde{\sigma}_m^B := \left(\tilde{\Phi}_{Y,m}^B, \tilde{\Phi}_{Z,m}^B\right)$ by selecting elements from Alice's declaration which correspond to the two halves of his eliminated signature $\tilde{X}_m^{(B)}$. The original σ_m has length $2L$, while $\tilde{\sigma}_m^B$ has length L.

Bob compares relevant elements of $\tilde{\sigma}_m^B$ to his $\tilde{X}_m^B$, choosing which half of $\tilde{X}_m^B$ to compare to based on whether he kept or swapped the eliminated signature element. Bob makes a decision about whether to accept m as genuine based on the number of *mismatches* between Alice's signature and his own eliminated signatures. A mismatch is defined below in Sec. 3.1.4 and in Fig. 3.5.

3 In Appendix C we discuss an extension to the protocol which allows it to run with an NPSK alphabet of coherent states, where N is an even integer.

If Bob measures fewer than $s_B L/2$ mismatches on both of his eliminated signature halves then he accepts Alice's message as genuine, otherwise the protocol aborts. Bob's threshold mismatch rate s_B determines how many mismatches he can observe before a signature fails his check. In general, s_B is a free parameter of the protocol and will be discussed further in Secs. 3.1.4, 3.2, 3.7.

STEP 7. If Bob has accepted m, then he forwards Σ to Charlie, who similarly checks for mismatches between Alice's signature and his eliminated signature. Charlie accepts the message if there are fewer than $s_C L/2$ mismatches between $\tilde{\sigma}^C_m$ and $\tilde{X}^{(C)}_m$. If Charlie also accepts m then the protocol has succeeded, otherwise it aborts. Charlie's threshold mismatch rate is s_C and will be discussed further in Secs. 3.1.4, 3.2, 3.7.

The key parameters for the Messaging stage are s_B, s_C which may be freely chosen by Bob and Charlie in order to optimize security. We observe in Sec. 3.2 that the choice $s_B \leqslant s_C$ will ensure security against Alice's repudiation attack.

3.1.4 *Counting mismatches*

The key test of validity which our protocol employs is a check on the number of mismatches between Bob or Charlie's eliminated signatures $\tilde{X}^{(B,C)}_m$ and Alice's declaration σ_m. A mismatch occurs if the state which Alice claims to have sent has been eliminated, Fig. 3.5.

To be concrete, a mismatch occurs at position j if

$$\phi^{B(C)}_{j,m} \in Y^{B(C)}_{j,m} \quad \text{or} \quad \phi^{C(B)}_{j,m} \in Z^{B(C)}_{j,m}, \tag{3.4}$$

and we let

$$\mathcal{M}(F, G) \tag{3.5}$$

denote the probability of mismatch between an arbitrary eliminated signature G, and an arbitrary list of phases F. Both F and G should be of the same length.

3.2 SECURITY AGAINST REPUDIATION

We now turn to consider the security of the QDS protocol desribed in Sec. 3.1. In what follows we will prove that our protocol is:

1. Sec. 3.2: secure against a repudiation attack (List 3.1 requirement 3, Fig. 3.2b),
2. Sec. 3.3: robust (List 3.1 requirement 5, Fig. 3.2c),
3. Sec. 3.4 secure against a forgery attack (List 3.1 requirement 1, Fig. 3.2a)

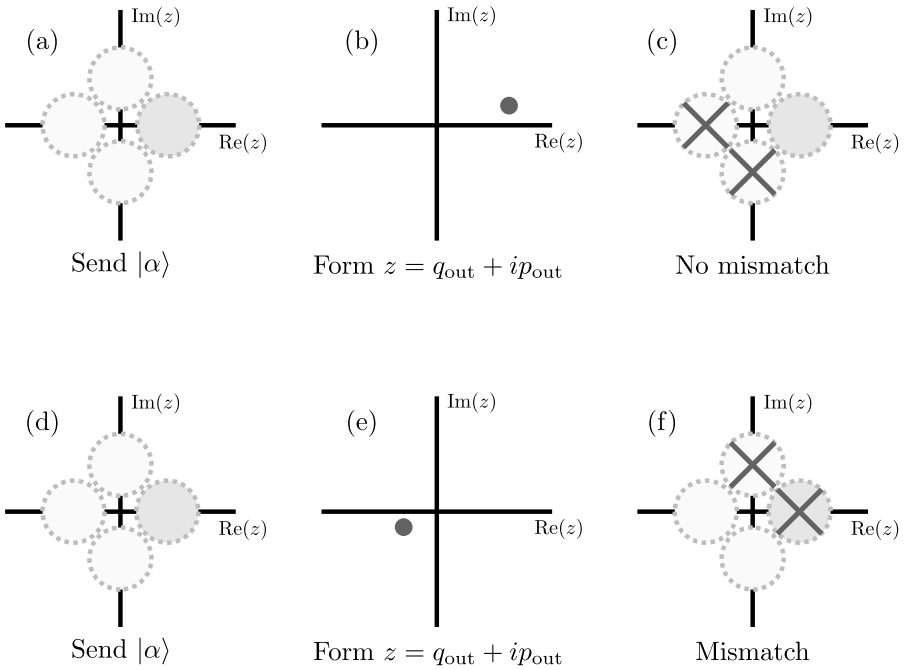


Figure 3.5: A mismatch occurs when an honest party eliminates the state which Alice claims to have sent. (a, d) Alice sends coherent state $|\alpha\rangle$. (b, e) Bob (Charlie) heterodynes and receives $(q_{\text{out}}, p_{\text{out}})$. We define $z = q_{\text{out}} + ip_{\text{out}}$. Even when all players are honest there is some probability of measuring $q_{\text{out}} < 0$, Sec. 3.3.1. (c) The eliminated signature element consists of $|-\alpha\rangle, |-i\alpha\rangle$ so there is no mismatch. (f) The eliminated signature element consists of $|\alpha\rangle, |i\alpha\rangle$ and so there is a mismatch.

Our proof will proceed by demonstrating that an attempted repudiation or forgery will induce a large mismatch rate, while a small mismatch rate is obtained when no attack is attempted. Thus, by appropriate choice of security parameters s_B, s_C and signature length L, the probability of a *successful* attack of any type may be made arbitrarily small.

We assume that in our 3 party setting at most one of the players A, B, C may behave dishonestly. For simplicity of notation we give a dishonest player the power to eavesdrop on the distribution of quantum states, and so the label "Eve" is not required. An internal eavesdropper is at least as powerful as an external Eve. If two or more players are dishonest then we assume that they will collaborate, which allows them to trivially break the protocol, and so this scenario is not discussed. We note that a collaboration of multiple dishonest players must be considered for an $n > 3$ party QDS protocol, as discussed in Ref. [84].

To succeed in a repudiation attack, a dishonest Alice aims to convince Bob that message m is genuine, while Charlie that m is fake, Fig. 3.2b. Security against repudiation is guaranteed by the symmetrization procedure (Step 4 of the protocol) which ensures that Alice does not know which recipient holds the eliminated signature element corresponding to a particular distributed state. Proof of security against repudiation follows along similar lines to Refs. [43, 45, 46, 73, 75].

At the end of Step 3, having sent the state $|\phi^B_{j,m}\rangle\langle\phi^B_{j,m}|$ to Bob, Alice knows that Bob holds the corresponding eliminated signature element $X^B_{j,m}$, and she may be able to guess it with high probability. In any case, knowing which recipient holds the $X^{(B,C)}_{j,m}$ gives Alice additional power to repudiate, even if she does not know what the individiual eliminated signature elements are[4].

At the end of Step 4, however, Alice does not know whether it is Bob or Charlie who holds an element $X^B_{j,m}$. This uncertainty will prove crucial for preventing her from successfully repudiating. Recall that Bob (Charlie) possesses an eliminated signature $\tilde{X}^{(B)}_m$ in two halves: one half ($Y^{(B)}_m$) containing those elements received directly from Alice, and one half ($Z^{(B)}_m$) containing elements received during this symmetrization step from Charlie (Bob).

We assume that Alice is completely free to manipulate her declared $\sigma_m = (\Phi^B_m, \Phi^C_m)$. We also assume that she may freely manipulate the number of mismatches between her declared signature and the eliminated signatures $X^{(B,C)}_m$ which Bob or Charlie held before sym-

4 Alice could, for example, perform an optimal strategy in order to guess the $X^{(B,C)}_{j,m}$. Then she may declare σ_m using guesses on Bob's elements to reduce her mismatch rate with respect to Bob, while declaring the opposite of her guesses on Charlie's elements to increase her mismatch rate with respect to Charlie.

metrization. We denote these observed mismatch rates as p_B and p_C, respectively:

$$\begin{aligned} p_B &= \mathcal{M}\left(\Phi_m^B, X_m^B\right), \\ p_C &= \mathcal{M}\left(\Phi_m^C, X_m^C\right). \end{aligned} \tag{3.6}$$

Alice may even choose them to be zero

Alice succeeds in her repudiation attack if Bob accepts both of his halves as genuine, while Charlie rejects at least one of his halves as fake. Let E_A, E_B denote the events that Bob accepts on the first or second half of his eliminated signature, respectively, and let E_C, E_D denote the events that Charlie rejects on the first or second half of his eliminated signature, respectively. Then a successful repudiation attack occurs when

$$(E_A \quad \text{and} \quad E_B) \quad \text{and} \quad (E_C \quad \text{or} \quad E_D)$$

where the events are defined as

$$\begin{aligned} E_A \quad &\text{when} \quad \mathcal{M}\left(\tilde{\Phi}_{Y,m}^B, Y_m^B\right) < s_B L/2, \\ E_B \quad &\text{when} \quad \mathcal{M}\left(\tilde{\Phi}_{Z,m}^B, Z_m^B\right) < s_B L/2, \\ E_C \quad &\text{when} \quad \mathcal{M}\left(\tilde{\Phi}_{Y,m}^C, Y_m^C\right) \geqslant s_C L/2, \\ E_D \quad &\text{when} \quad \mathcal{M}\left(\tilde{\Phi}_{Z,m}^C, Z_m^C\right) \geqslant s_C L/2. \end{aligned} \tag{3.7}$$

The $\tilde{\Phi}$ denotes the rearranged form of Alice's declared phases Φ in order to compare corresponding elements, symbol Y denotes that an element was received directly from Alice and symbol Z denotes that it was received during symmetrization. Function $\mathcal{M}$ measures the mismatch probability between two strings, and is defined above in Sec. 3.1.4.

Thus, the probability $\varepsilon_{\text{repudiation}}$ of a successful repudiation attack is given by

$$\varepsilon_{\text{repudiation}} = P\left[(E_A \cap E_B) \cap (E_C \cup E_D)\right]. \tag{3.8}$$

To proceed, we require the following two probability inequalities for arbitrary events x, y:

$$P(x \cap y) \leqslant \min\{P(x), P(y)\}, \tag{3.9}$$

$$P(x \cup y) \leqslant P(x) + P(y). \tag{3.10}$$

We may now use the probability inequality Eq. 3.9 and observe that

$$\varepsilon_{\text{repudation}} \leqslant \min\{P(E_A \cap E_B), P(E_C \cup E_D)\}.$$

Again using Eqs. 3.9, 3.10, we arrive at

$$\varepsilon_{\text{repudiation}} \leqslant \min\{\min\{P(E_A), P(E_B)\}, P(E_C) + P(E_D)\}, \tag{3.11}$$

which provides an upper bound for the probability of successful repudiation attack in terms of the individual probabilities for distinct events. We now wish to demonstrate that the probability for each event may be made arbitrarily small by suitable choice of L, and thus $\varepsilon_{\text{repudiation}}$ may also be made arbitrarily small.

We rely on Hoeffding's inequalities Eqs. 1.75, 1.76 which we use to bound each probability appearing in Eq. 3.11. Let $\mathcal{F}$ be a string of declared phases, and $\mathcal{G}$ be an eliminated signature. Strings $\mathcal{F}$ and $\mathcal{G}$ each have length n. We define a string $\mathcal{E}$ such that

$$\mathcal{E}_j = \begin{cases} 1 & \text{if a mismatch occurs between } \mathcal{F}_j \text{ and } \mathcal{G}_j \\ 0 & \text{otherwise} \end{cases}$$

which measures whether a mismatch has occurred between the j^{th} elements of $\mathcal{F}$ and $\mathcal{G}$, Fig. 3.5, Sec. 3.1.4.

The mismatch rate $\mathcal{M}(\mathcal{F}, \mathcal{G})$ is equivalent to the observed (empirical) mean $\bar{\mathcal{E}}$, while its expectation $\mathbb{E}(\bar{\mathcal{E}})$ is equal to the arithmetic mean

$$\mathbb{E}(\bar{\mathcal{E}}) = \frac{1}{n}\sum_{j=1}^{n} \mathcal{E}_j.$$

We wish to bound the probability that there are fewer than s observed mismatches,

$$P(\mathcal{M}(\mathcal{F}, \mathcal{G}) \leqslant s) = P\left(\mathbb{E}(\bar{\mathcal{E}}) - \bar{\mathcal{E}} \geqslant \mathbb{E}(\bar{\mathcal{E}}) - s\right). \tag{3.12}$$

By applying Hoeffding inequality Eq. 1.75,

$$P(\mathcal{M}(\mathcal{F}, \mathcal{G}) \leqslant s) \leqslant \exp\left(-2\left[\mathbb{E}(\bar{\mathcal{E}}) - s\right]^2 n\right) \tag{3.13}$$

provided that $\mathbb{E}(\bar{\mathcal{E}}) - s \geqslant 0$. This Eq. 3.13 gives an upper bound for the probability that there are fewer than s mismatches observed when the average probability for mismatch is $\mathbb{E}(\bar{\mathcal{E}})$.

Similarly, we derive

$$P\left(s \leqslant \bar{\mathcal{E}}\right) \leqslant \exp\left(-2\left[s - \mathbb{E}(\bar{\mathcal{E}})\right]^2 n\right) \tag{3.14}$$

by applying Eq. 1.76, provided that $s - \mathbb{E}(\bar{\mathcal{E}}) \geqslant 0$. This Eq. 3.14 gives an upper bound for the probability that there are more than s mismatches observed when the average probability for mismatch is $\mathbb{E}(\bar{\mathcal{E}})$.

Using Eqs. 3.13, 3.14 we may now bound the probabilities for events of Eq. 3.7:

$$\begin{aligned}
P(E_A) &\leqslant \exp\left(-[p_B - s_B]^2 L\right) \quad \text{provided that} \quad p_B > s_B, \\
P(E_B) &\leqslant \exp\left(-[p_C - s_B]^2 L\right) \quad \text{provided that} \quad p_C > s_B, \\
P(E_C) &\leqslant \exp\left(-[s_C - p_C]^2 L\right) \quad \text{provided that} \quad p_C < s_C, \\
P(E_D) &\leqslant \exp\left(-[s_C - p_B]^2 L\right) \quad \text{provided that} \quad p_B < s_C, \qquad (3.15)
\end{aligned}$$

where in the first two inequalities we have applied Eq. 3.13 and in the second two inequalities we have applied Eq. 3.14.

Alice has the power to choose any $0 \leqslant p_B, p_C \leqslant 1$. Let us consider some cases.

CASE 1: Assume that $p_B \geqslant s_B$. Then, by the first inequality of Eq. 3.15, the probability Eq. 3.11 must decay exponentially and so we are secure against repudiation. An analogous argument holds for the choice $p_C \geqslant s_B$ using the second inequality of Eq. 3.15.

CASE 2: Assume that $p_B < s_B$ and $p_C < s_B$. It follows that if we choose $s_B \leqslant s_C$, then we force $p_B < s_C$ and $p_C < s_C$, and so Eq. 3.11 decays exponentially via the third and fourth inequalities of Eq. 3.15. Intuitively, we have demonstrated that even though Alice has full control over p_B, p_C she cannot engineer a situation in which Bob measures fewer than s_B mismatches while Charlie measures more than s_C. This relies on the choice $s_B \leqslant s_C$ to ensure that $\varepsilon_{\text{repudiation}}$ decays exponentially in L.

Let us substitute Eq. 3.15 into Eq. 3.11 and simplify. Clearly, increasing p_B or p_C will cause both of the exponentials in the first term to decrease. Because of the inner minimum, we will only care about $\max\{p_B, p_C\}$, and so we define $p := \max\{p_B, p_C\}$ and write

$$\min\left\{\exp\left(-[p_B - s_B]^2 L\right), \exp\left(-[p_C - s_B]^2 L\right)\right\} = \exp\left(-[p - s_B]^2 L\right).$$

In the case $p_B, p_C \leqslant s_C$ we may increase the second term of Eq. 3.11:

$$\exp\left(-[s_C - p_C]^2 L\right) + \exp\left(-[s_C - p_B]^2 L\right) \leqslant 2\exp\left(-[s_C - p]^2 L\right). \qquad (3.16)$$

This leads to

$$\varepsilon_{\text{repudiation}} \leqslant \min\left\{2\exp\left(-[p - s_B]^2 L\right), 2\exp\left(-[s_C - p]^2 L\right)\right\}. \qquad (3.17)$$

Since the minimum over two distinct Gaussians is maximized when the Gaussians have equal arguments, the probability $\varepsilon_{\text{repudiation}}$ is maximized when

$$p = \frac{s_B + s_C}{2}. \qquad (3.18)$$

Finally, we reach

$$\varepsilon_{\text{repudiation}} \leqslant 2\exp\left(-\frac{[s_C - s_B]^2}{4}L\right) \tag{3.19}$$

as our useful bound for the probability that Alice succeeds in her repudiation attack. Since Eq. 3.19 is exponentially decaying, the probability that she succeeds may be made arbitrarily small by choice of L. Our protocol can therefore be secured against a repudiation attack by a sufficiently large choice of L, provided that we choose $s_B \leqslant s_C$.

3.3 ROBUSTNESS

The QDS protocol must be robust (List 3.1 requirement 5, Fig. 3.2c) and allow the message m to be accepted provided that all parties behave honestly and there is no attack present. This is a requirement for useful QDS, since a protocol which aborts for every message will certainly abort in the presence of an attack and thus is trivially secure. In this Section we will find an upper bound to the probability that the protocol fails even when everyone behaves honestly.

The protocol fails in the absence of attack if either Bob or Charlie rejects a message which Alice did in fact send, i.e. if Bob or Charlie detect too many mismatches on Alice's declaration σ_m. Since in Sec. 3.2 we derived that $s_B \leqslant s_C$, it will always be more likely that Bob rejects than Charlie. We will seek to bound the probability that Bob measures more than $s_B L/2$ mismatches on either of his signature halves. This will also provide an upper bound for the probability that Charlie rejects with no attack.

We define an *honest mismatch* to have occured if there is a mismatch between Alice's declaration and either of Bob's (or Charlie's) eliminated signature halves in an honest scenario. Let p_{err} be the probability of honest mismatch. Because of the non-orthogonality of coherent states even in an ideal setting we have $p_{\text{err}} > 0$. This is in contrast to protocols such as Refs. [44, 46] which could attain an ideal $p_{\text{err}} = 0$. We model p_{err} in the next Section 3.3.1, and there demonstrate that it is nonzero.

Using probability inequality Eq. 3.10, the probability that Bob rejects either of his halves is given by

$$\varepsilon_{\text{Bob rejects}} \leqslant 2P(E_A) \tag{3.20}$$

where E_A is the event that Bob measures more than $s_B L/2$ mismatches on either of his halves. We have implicitly assumed that p_{err} is identical for states originally sent to Bob and those originally sent to Charlie, but this is easy to relax if desired.

Using Hoeffding inequality Eq. 3.14 in an identical manner to the derivation of Eq. 3.15, Sec. 3.2, we see that

$$\varepsilon_{\text{honest abort}} = \varepsilon_{\text{Bob rejects}} \leqslant 2\exp\left(-\left[s_B - p_{\text{err}}\right]^2 L\right) \tag{3.21}$$

provided that $s_B - p_{\text{err}} \geqslant 0$. Equation 3.21 is our useful bound for the probability that the protocol fails the robustness requirement. Since it is exponentially decaying, the probability that this happens can be made arbitrarily small, and so our protocol is robust.

3.3.1 *Modelling* p_{err}

The probability p_{err} corresponds to the probability that a heterodyne measurement outcome $(q_{\text{out}}, p_{\text{out}})$ has $q_{\text{out}} < 0$ when Alice distributed the coherent state $|\alpha\rangle$, Fig. 3.6. In the absence of thermal noise the channel simply acts as a beamsplitter with vacuum at the unused input port, and so

$$|\alpha\rangle_A \to |\sqrt{T}\alpha\rangle_{(B,C)} \tag{3.22}$$

when the channel has transmission T (see Appendices A, B). A heterodyne measurement on the output state yields $(q_{\text{out}}, p_{\text{out}})$ which we write as $z = q_{\text{out}} + ip_{\text{out}}$. We receive z with probability

$$P(z) = \frac{1}{\pi}\exp\left(-\left|z - \sqrt{T}\alpha\right|^2\right) \tag{3.23}$$

where ket vector $|z\rangle$ denotes the coherent state centred on z (c.f. Appendix A). Then,

$$\begin{aligned} p_{\text{err}} = P(\text{Re}(z) < 0) &= \int_{\text{Re}(z)<0} d^2z\, P(z) \\ &= \frac{1}{\pi}\int_{-\infty}^{\infty} dy \exp(-y^2) \int_{-\infty}^{0} dx \exp\left(-\left[x - \sqrt{\frac{T}{2}}\alpha_x\right]^2\right), \end{aligned} \tag{3.24}$$

where $x = \text{Re}(z) = q_{\text{out}}, y = \text{Im}(z) = p_{\text{out}}$ and $\alpha_x = \text{Re}(\alpha)$.

Integrating, we arrive at

$$p_{\text{err}} = \frac{1}{2}\text{erfc}\left(\sqrt{\frac{T}{2}}\alpha\right) \tag{3.25}$$

which models the probability of honest mismatch over a lossy channel with transmission T. Probability p_{err} is motivated in Fig. 3.6 which elucidates the above discussion, and explains why $p_{\text{err}} \neq 0$. An equivalent analysis when the channel contains thermal noise is discussed in Appendix A.

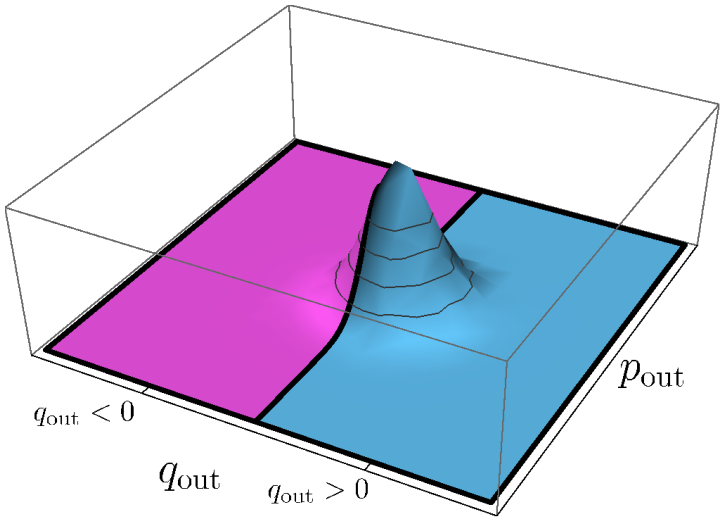


Figure 3.6: Histogram of possible heterodyne outcomes. A coherent state $|\alpha\rangle$ with $\alpha > 0$ has nonzero probability to give the measurement outcome $q_{\text{out}} < 0$. In other words, $p_{\text{err}} > 0$ always, and $p_{\text{err}} \to 0$ only as $\alpha \to \infty$. The blue region corresponds to measurement outcomes which will not give a mismatch, while the pink region corresponds to measurement outcomes which will yield a mismatch. This histogram is equivalent to the Hussimi Q function [1] of the received coherent state, and is thus also Gaussian.

3.4 SECURITY AGAINST FORGERY

We now turn to consider security against forgery, List. 3.1 requirement 1, Fig. 3.2a. In a forging attack, a dishonest player (or a fourth party, Eve) will declare some fake message m' with the aim that it should be accepted by honest players as being genuine and having originated with Alice. We will not consider the possibility that a dishonest player is impersonating Alice from the beginning of the protocol (see Sec. 3.1.2 for brief discussion). The fake message m' will have an appended signature $\tau_{m'}$ consisting of declared coherent state phases. Message m' will be accepted if $\tau_{m'}$ has sufficiently few mismatches with respect to an honest player's eliminated signature.

Since Bob and Charlie already know $L/2$ of each other's eliminated signature elements – those which were forwarded during the symmetrization step of the protocol – a dishonest player who is internal to the signature scheme will always have an advantage over an external Eve. Additionally, since $s_B < s_C$, Charlie is more likely than Bob to accept a forged message m' and fake signature $\tau_{m'}$, and so the most dangerous forger will be a dishonest Bob. We thus proceed with the mantra "Bob is Eve," and take Bob as our dishonest forging party. Since this is a worst-case scenario, our following analysis will implicitly also guard against the possiblity that Charlie or Eve are the forger.

Security against a forging attack arises because the sequence of states which Alice sends to Bob is different from the sequence which she sends to Charlie. This is in stark contrast to the recent work Ref. [73] and earlier works Refs. [39, 43, 44, 46]. Since Bob already knows the $L/2$ elements Z^C_m which Charlie received from Bob during Symmetrization, Step 4, Bob is able to cause arbitrarily few mismatches on that half of Charlie's signature. Bob's goal then is to declare a string $\tilde{\Phi}^C_{Y,m'}$, length $L/2$ such that

$$\mathcal{M}\left(\tilde{\Phi}^C_{Y,m'}, Y^C_{m'}\right) \leqslant s_C \frac{L}{2}, \tag{3.26}$$

which will be accepted by Charlie.

Bob's only strategy to gain information about the $Y^C_{m'}$ is to eavesdrop on the distribution of states from Alice to Charlie during Steps 2 and 3 of the protocol, and Bob's eavesdropping strategies will be fully considered in Sec. 3.6 below.

Defining p_e as the probability that Bob will induce a mismatch on an individual given signature element, the probability $\varepsilon_{\text{forgery}}$ that Bob succeeds in his forging attack is

$$\varepsilon_{\text{forgery}} \leqslant 2\exp\left(-\left[p_e - s_C\right]^2 L\right), \tag{3.27}$$

provided that $p_e - s_C \geqslant 0$. Equation 3.27 is derived using Eq. 3.13 similarly to Eqs. 3.19, 3.21 in Secs. 3.2, 3.3 by calculating the probability that Charlie accepts a message with more than p_e mismatches.

Charlie's threshold s_C may be freely chosen, and by combining it with conditions required for derivation of Eqs. 3.19, 3.21 we deduce the requirement

$$p_{\text{err}} \leqslant s_B \leqslant s_C \leqslant p_e, \tag{3.28}$$

where threshold parameters s_B, s_C may be freely chosen to optimize security.

Equation 3.28 encodes the intuitive condition that the QDS protocol is secure provided that $p_e > p_{\text{err}}$; or, in other words, that a dishonest forger will cause more mismatches than an honest player. The protocol security analysis thus relies on finding channel parameters, signature lengths and QPSK amplitudes for which a forger is guaranteed to make more errors than the honest error rate p_{err}, and thus for which a forging attack will be detectable. In Sec. 3.5 we demonstrate how p_e relates to the quantum system held by Bob at the end of the protocol's Distribution stage, while in Sec. 3.6 we analyse several types of eavesdropping attack which Bob may attempt, and we perform explicit calculations of p_e under different channel conditions.

3.5 BOUNDING p_E

To complete the security analysis of our protocol we must find a lower bound for p_e, the rate at which a forging Bob will induce a mismatch

with respect to Charlie's signature. Our protocol may be secured by choice of L provided that $p_e > p_{err}$ and an honest Charlie outperforms dishonest Bob. The key contribution of this section will be a lower bound for p_e which may be calculated once Bob's quantum system at the end of the Distribution stage of the protocol is known.

Bob will declare a string $\tilde{\Phi}^C_{Y,m'}$, length L/2, aimed to cause sufficiently few mismatches with respect to Charlie. For convenience we will abbreviate Bob's declared string as $\tilde{\Phi}_{Bob}$. Our analysis differs from QKD analysis in that Bob's mismatch probability is *not equivalent* to the probability that he misidentifies an element of Chalie's eliminated signature. Because Charlie eliminates two states from QPSK, Fig. 3.4, there are two remaining states from the QPSK alphabet which Bob can declare without introducing a mismatch. Each of the remining states is shared with another possible eliminated signature element, and so it is entirely possible for Bob to misidentify Charlie's eliminated signature and yet still not introduce a mismatch.

This forces us to work directly in terms of mismatch probability p_e, which we do via our error variable $\mathcal{E}$, Eq. 3.2, the j^{th} element of which is 1 if Bob induces a mismatch there, and 0 if there is no mismatch. We will continue to work in terms of the QPSK alphabet, though in Appendix C we demonstrate how the proof may be generalized to an NPSK alphabet.

To proceed, recall that $Y^C_{m'}$ is the half of Charlie's eliminated signature based on states he received directly from Alice. This is the half which Bob will attack. We define Y_j to be its j^{th} element, and write $Y_j = \left\{y^j_1, y^j_2\right\}$ for phases y^j_1, y^j_2 in the QPSK alphabet. The $y^j_{1,2}$ denote the states which Charlie has eliminated. Note that $y^j_{1,2}$ must be adjacent to each other in phase-space, that is, if $y^j_1 = \alpha$ then y^j_2 must be either $i\alpha$ or $-i\alpha$. The string $\tilde{\Phi}_{Bob} = \left\{\phi_j\right\}_{j=1}^{L/2}$ is Bob's declaration, which is the result of an unspecified but optimal POVM and classical strategy.

A mismatch occurs when $\phi_j = y^j_1$ or $\phi_j = y^j_2$. Bob's average mismatch rate p_e may be equivalently written in terms of $\mathcal{E}$

$$p_e = P\left(\mathcal{E}_j = 1\right).$$

Because $\mathcal{E}_j$ can take one of two values, the Shannon entropy $H\left(\mathcal{E}_j\right)$ is equivalent to the binary entropy $h\left(p_e\right)$, which is defined in Eq. 1.78.

Now, consider the conditional entropy

$$H\left(\mathcal{E}_j, y^j_1, y^j_2 \,\middle|\, \phi_j\right), \tag{3.29}$$

which is related to the uncertainty about whether a mismatch has occurred under Bob's declaration ϕ_j. Using the chain rule for conditional entropies, Eq. 1.91, we may write

$$H\left(\mathcal{E}_j, y^j_1, y^j_2 \,\middle|\, \phi_j\right) = H\left(\mathcal{E}_j \,\middle|\, y^j_1, y^j_2, \phi_j\right) + H\left(y^j_1, y^j_2 \,\middle|\, \phi_j\right). \tag{3.30}$$

Since an element $\mathcal{E}_j$ is uniquely determined once ϕ_j, y_1^j, y_2^j are known, we may immediately deduce

$$H\left(\mathcal{E}_j \,\middle|\, y_1^j, y_2^j, \phi_j\right) = 0.$$

Using chain rule Eq. 1.91 once again on the left hand side of Eq. 3.30, but this time expanding over variable y_1^j, y_2^j, we get:

$$\begin{aligned} H\left(\mathcal{E}_j, y_1^j, y_2^j \,\middle|\, \phi_j\right) &= H\left(y_1^j, y_2^j \,\middle|\, \mathcal{E}_j, \phi_j\right) + H\left(\mathcal{E}_j \mid \phi_j\right) \\ &\leqslant H\left(y_1^j, y_2^j \,\middle|\, \mathcal{E}_j, \phi_j\right) + H\left(\mathcal{E}_j\right) \\ &= H\left(y_1^j, y_2^j \,\middle|\, \mathcal{E}_j, \phi_j\right) + h\left(p_e\right), \end{aligned} \tag{3.31}$$

where the inequality follows because conditioning cannot increase entropy.

Combining Eqs. 3.30 and 3.31,

$$\begin{aligned} H\left(y_1^j, y_2^j \,\middle|\, \phi_j\right) &\leqslant H\left(y_1^j, y_2^j \,\middle|\, \mathcal{E}_j, \phi_j\right) + h\left(p_e\right) \\ &= P\left(\mathcal{E}_j = 0\right) H\left(y_1^j, y_2^j \,\middle|\, \mathcal{E}_j = 0, \phi_j\right) \\ &\quad + P\left(\mathcal{E}_j = 1\right) H\left(y_1^j, y_2^j \,\middle|\, \mathcal{E}_j = 1, \phi_j\right) + h\left(p_e\right), \end{aligned} \tag{3.32}$$

with

$$P\left(\mathcal{E}_j = 0\right) = 1 - p_e \quad \text{and} \quad P\left(\mathcal{E}_j = 1\right) = p_e. \tag{3.33}$$

Now, because there are two eliminated signature elements consistent with a given $\mathcal{E}_j = 0$ and ϕ_j, and since we are free to permute and relabel $y_1^j \leftrightarrow y_2^j$, we have four choices for the variable y_1^j, y_2^j once $\mathcal{E}_j$ and ϕ_j are chosen[5]. Thus,

$$H\left(y_1^j, y_2^j \,\middle|\, \mathcal{E}_j = 0, \phi_j\right) \leqslant \log_2 4 = 2. \tag{3.34}$$

Additionally, since Charlie eliminates precisely half of the alphabet to form his eliminated signature, we see that

$$H\left(y_1^j, y_2^j \,\middle|\, \mathcal{E}_j = 0, \phi_j\right) = H\left(y_1^j, y_2^j \,\middle|\, \mathcal{E}_j = 1, \phi_j\right), \tag{3.35}$$

and so Eq. 3.32 becomes

$$H\left(y_1^j, y_2^j \,\middle|\, \phi_j\right) \leqslant 2 + h\left(p_e\right). \tag{3.36}$$

Let us expand the left hand side of Eq. 3.36 using the definition of mutual information, Eq. 1.81:

$$H\left(y_1^j, y_2^j \,\middle|\, \phi_j\right) = H\left(y_1^j, y_2^j\right) - I\left(y_1^j, y_2^j : \phi_j\right). \tag{3.37}$$

5 And eight choices *a priori*.

There are four possible eliminated signature elements, therefore eight possible choices for y_1^j, y_2^j including relabeling $y_1^j \leftrightarrow y_2^j$, and so

$$\mathrm{H}\left(y_1^j, y_2^j\right) = \log_2 8 = 3. \tag{3.38}$$

We lower bound Eq. 3.37 by using the fact that the Holevo information maximizes the mutual information, Sec. 1.5.7, and so

$$\mathrm{H}\left(y_1^j, y_2^j \,\middle|\, \phi_j\right) = 3 - \chi\left(y_1^j, y_2^j : \phi_j\right). \tag{3.39}$$

Finally, combining Eqs. 3.36 and 3.39, we arrive at

$$\mathrm{h}\left(p_e\right) \geqslant 1 - \chi\left(y_1^j, y_2^j : \phi_j\right), \tag{3.40}$$

which is one of the key results for this chapter, and a key result of Ref. [75].

In order to use the bound Eq. 3.40 we must calculate forging Bob's Holevo information χ, Eq. 1.87. Since binary entropy $\mathrm{h}\left(p_e\right)$ is monotone for $p_e \leqslant 1/2$, Fig. 1.12, we conclude that a lower bound for $\mathrm{h}\left(p_e\right)$ also gives us a lower bound for p_e. Equation 3.40 therefore fully quantifies the best mismatch probability which Bob can attain from an optimal measurement on his quantum system, combined with an optimal classical strategy. We may solve this equation for a lower bound on p_e one Bob's Holevo information χ is quantified. We do this under several important classes of eavesdropping attack in the following Section, 3.6.

3.6 ATTACK ANALYSIS

We will consider several different models of dishonest Bob's eavesdropping attack. Different models will affect both the parameter regimes over which our protocol can be made secure, and the cost of resources required for that security. We will demonstrate how Bob's Holevo information may be calculated in each model, which may then be used to calculate p_e, Eq. 3.40.

As in the QKD literature [125], we define the following three types of quantum attack:

- individual: Fig. 3.7a;
- collective: Fig. 3.7b;
- coherent: Fig. 3.7c.

In an individual attack, Fig. 3.7a, Bob interacts separately with each signal state distributed from Alice to Charlie, and performs separate measurements on each state. For a collective attack, Fig. 3.7b, Bob again interacts with each signal state separately, but is permitted to perform a global measurement on his entire quantum system. This

may include either introducing or exploiting classical correlations between signal states. Finally, in a coherent attack, Fig. 3.7c, Bob interacts with all signal states globally and (assumed) simultaneously, and he is permitted to perform a global measurement on his entire system. This attack affords him the full power of quantum mechanics, and Bob can even introduce and exploit quantum correlations between signal states.

Before we proceed, it is pertinent to discuss the general strategy adopted in this Thesis to bound the power which an eavesdropper has to attack the protocol. Intuitively, Eve's power must be related to her ability to correctly distinguish between possible states which she possesses at the end of the Distribution stage. As we have seen, her overall mismatch probability is *not equivalent* to her state-discrimination probability, but the two are intimately related. Questions about optimal discrimination between non-orthogonal quantum states have a long history [126], and one should expect that advances in answering these questions will pay dividends in quantum security analysis.

In Section 1.4 we encountered one type of discrimination strategy, an *unambiguous measurement*, which can probabilistically, but accurately, differentiate between two non-orthogonal states. Such strategies never give an error, but will sometimes fail to give any information. The QDS scheme [43] is built on honest players performing such a measurement. Could Eve benefit from using an unambiguous measurement, generalised to the states which she receives after the Distribution stage? When the measurement yields a result, she will perfectly know her held state, and thus can introduce no mismatch on that signature element. However, on the elements which she gains no result she will still be forced to guess which state to declare, which will have high probability to introduce a mismatch. In principle, Eve could sabotage the state distribution whenever she gains no information from her unambiguous measurement, though this intuitively will raise the p_{err} mismatch rate as the honest players still heterodyne on the vacuum.

There are other concrete measurement strategies which Eve could try to perform. The most natural class to consider are so-called *minimum-error measurements* [127, 128], which are chosen precisely to reduce Eve's error probability[6]. For symmetric sets of states[7], the POVMs describing the required minimum-error measurements can be constructed and take a well-known form, that of a "square-root measurement" [127, 128, 130]. When considering sequences of quantum states, the best global measurement is not always a sequence of optimal individual measurements [129], and finding the optimal global POVMs

6 Their generalisation, the *minimum-cost measurements* [129] were considered in the QDS protocol in Ref. [73].

7 Let $\hat{U}$ be a unitary operator such that $\hat{U}^N = \mathbb{1}$, and define $|\psi_i\rangle = \hat{U}^i|\psi_0\rangle$ for a state $|\psi_0\rangle$. Then the set of N states $\{|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{N-1}\rangle\}$ generated from $|\psi_0\rangle$ by repeated actions of $\hat{U}$ is known as a *symmetric* set [129]. The NPSK alphabets considered in this Thesis are a common example of a symmetric set.

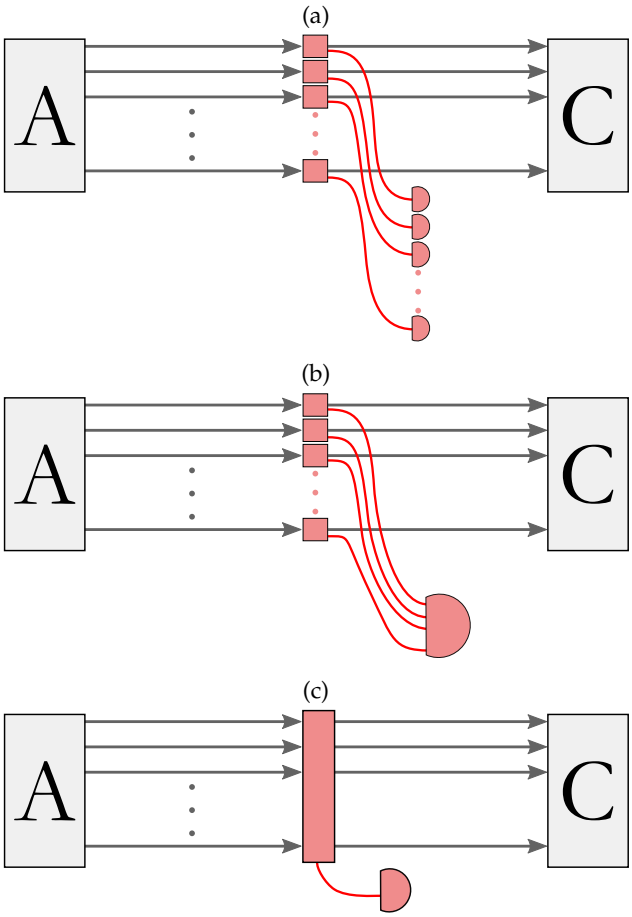


Figure 3.7: Taxonomy of different eavesdropping attack strategies [125]. Black arrows denote quantum signal states distributed from Alice to Charlie. Red items belong to Bob. (a) Individual attack. Bob inserts separate probes (red boxes) into state distribution and performs measurement on each system individually. (b) Collective attack. Bob inserts separate probes into state distribution and stores his states until the end of signal distribution. He may then perform a measurement on his entire system. (c) Coherent attack. Bob interacts with all signals at the same time and he can perform a measurement on a single, global, probe. Attack (a) cannot introduce correlations between signals. Attack (b) may introduce classical correlations, and attack (c) may introduce any correlations between signals.

is difficult. To proceed, one requires a more general approach. Most quantum cryptographic proofs focus instead on information-theoretic quantities bounding the information available to Eve, or bounding her error probability, without reference to a specific measurement strategy. This is the the method we have adopted in this Chapter, whereby the Holevo information implicitly assumes that it has been optimized over all POVMs which Eve could perform [16]. This allows us to apply the analysis to a greater class of states[8], and hints at future generalisations in terms of the smooth min-entropy [18].

Thus, in this section we will focus on individual and collective forging attacks, for which we calculate the eavesdropper's Holevo information. Full security against coherent quantum attacks in the CV QKD literature has only been proven for the simpler case of coherent states modulated with a Gaussian distribution [95, 131–135], and a full security proof remains elusive for a discrete modulation. There has been some recent success in applying convex optimization methods to the problem [96], but these proofs often rely on an assumption about the Gaussianity of the discretely modulated alphabet [136] which is only strictly valid in the limit $\alpha \to 0$. In keeping with recent trends in the QKD literature for discretely modulated coherent states without the assumption of Gaussianity [137], we will focus on bounding the attack strength of individual attacks, and then assume the i.i.d. criterion [94, 95] in order to reach security against collective attacks.

In particular, we will study both a beamsplitter attack and an entangling cloner attack for our protocol [99, 138]. In both of these attacks, Bob will replace the quantum distribution channel with a beamsplitter intended to mimic the effect of the channel on Charlie's measurement. Since Bob chooses his beamsplitter, he can do so without alerting Alice and Charlie to his presence, and so all channel loss must be attributed to Bob. Bob will either leave the second beamplitter input port empty, or he will mimic channel thermal noise by injecting there a thermal state Eq. 1.40, or one arm of his entangled two-mode squeezed vacuum state Eq. 1.51. This so-called "entangling cloner" attack allows Bob to gain additional information which is stored in the correlations between his two modes. This is known to be a dishonest player's optimal attack strategy in asymptotic QKD with Gaussian-modulated coherent states [95, 131], while the optimal attack strategy against discrete-modulated QKD remains an open question. However, we conjecture that entangling cloner should be optimal in the Gaussian limit $\alpha \to 0$, and close to optimal for the small amplitudes α considered in this thesis. Certainly, performing an entangling-cloner attack on each signal state as it passes will be physically demanding for Bob.

8 Although the QPSK alphabet is a symmetric set, the more realistic variations on QPSK considered in Chapter 5 are not.

3.6.1 *Beamsplitter attack*

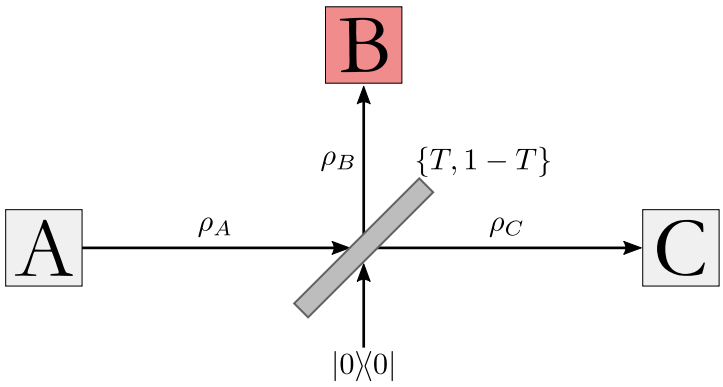


Figure 3.8: Attack BS0. Bob replaces the channel with a lossless channel, plus a beamsplitter. By inputting vacuum $|0\rangle\langle 0|$ into the beamsplitter, Bob mimics channel loss while imposing zero excess noise.

In its canonical form, the beamsplitter attack, Fig. 3.8, allows Bob to replace a lossy channel, transmission T, with a corresponding lossless channel and beamsplitter. Bob inputs vacuum $|0\rangle$ into the unused input port. Bob receives his quantum system ρ_B from the reflected output port, and from ρ_B he will attempt to gain information about Charlie's measurement outcomes. Crucially, to honest players Alice and Charlie this attack is indistinguishable from simply having a lossy transmission channel, and so in analysis all channel loss must be attributed to the action of the dishonest Bob. This attack cannot model any channel thermal noise, which should therefore be ignored in the analysis. A realistic channel will, however, impose noise onto Charlie's measurement outcomes, and later we describe some modificaions to the beamsplitter attack to include this.

BS0: $\xi = 0$

Attack BS0 is depicted in Fig. 3.8. This attack is the canonical beamsplitter attack, in which Bob will replace the channel with a lossless channel plus a beamsplitter. Crucially, the beamsplitter is chosen so that it mimics the channel exactly, and honest players should be unable to tell whether an attack has taken place. In a run of the protocol, therefore, all channel loss is attributed to dishonest Bob.

Consider a single input coherent state $|\alpha_k\rangle\langle\alpha_k|$, with the α_k chosen uniformly at random from the QPSK alphabet ($k = 0, 1, 2, 3$). Bob's attack effectively inputs the vacuum state $|0\rangle\langle 0|$ into the second input port of the beamsplitter. We will calculate the Holevo information χ, Eq. 1.87, of Bob's state conditioned on Charlie receiving a particular eliminated signature element after his heterodyne measurement.

Using beamsplitter relation Eq. 1.55 (c.f. Appendix B), we see that a beamsplitter with transmission T enacts the following transformation on the input state:

$$|\alpha_k\rangle\langle\alpha_k|_A \otimes |0\rangle\langle 0|_B \rightarrow \left|\sqrt{T}\alpha_k\right\rangle\left\langle\sqrt{T}\alpha_k\right|_C \otimes \left|\sqrt{1-T}\alpha_k\right\rangle\left\langle\sqrt{1-T}\alpha_k\right|_B . \tag{3.41}$$

So Charlie holds the state $|\sqrt{T}\alpha_k\rangle\langle\sqrt{T}\alpha_k|$, while Bob holds $|\sqrt{1-T}\alpha_k\rangle\langle\sqrt{1-T}\alpha_k|$. When the α_k is chosen uniformly at random, we must mix over the alphabet and so the mixed two-mode output state is

$$\left(\frac{1}{4}\sum_{\alpha_k}|\alpha_k\rangle\langle\alpha_k|_A\right)\otimes|0\rangle\langle 0|_B \rightarrow \frac{1}{4}\sum_{\alpha_k}\left(\left|\sqrt{T}\alpha_k\right\rangle\left\langle\sqrt{T}\alpha_k\right|_C \otimes \left|\sqrt{1-T}\alpha_k\right\rangle\left\langle\sqrt{1-T}\alpha_k\right|_B\right). \tag{3.42}$$

Charlie heterodynes on his mode and receives outcomes $(q_{out,C}, p_{out,C})$. We write $z_C = q_{out,C} + ip_{out,C}$, and so Bob now holds

$$\rho_{B\,|\,z_C} = \frac{1}{4}\frac{1}{P(z_C)}\sum_{\alpha_k} P(z_C \mid \alpha_k, T) \times \left|\sqrt{1-T}\alpha_k\right\rangle\left\langle\sqrt{1-T}\alpha_k\right|_B . \tag{3.43}$$

Here $P(z_C \mid \alpha_k, T) = \left|\langle z_C|\sqrt{T}\alpha_k\rangle\right|^2$ corresponds to the probability that Charlie measures z_C on his mode given that he received state $|\sqrt{T}\alpha_k\rangle\langle\sqrt{T}\alpha_k|$, while $P(z_C) = \sum_{\alpha_k} P(z_C|\alpha_k, T)$ corresponds to the total unconditional probability that he measures z_C.

Recall that the eliminated signature element held by Charlie is determined entirely by his heterodyne outcome z_C, Fig. 3.9. Since Holevo information χ is defined in terms of Charlie's eliminated signature element rather than heterodyne measurement outcome, and since many outcomes z_C will return the same eliminated signature element, we must now mix $\rho_{B\,|\,z_C}$ over entire quadrants in phase-space.

Let us use the notation for eliminated signature elements from Tab. 3.1, and consider the first eliminated signature element e_1. We mix $\rho_{B\,|\,z_C}$ over all outcomes z_C which are consistent with e_1, i.e. $q_{out} > 0$ and $p_{out} > 0$:

$$\rho_{B\,|\,e_1} = \frac{1}{\mathcal{N}(e_1)}\int_{q_{out}>0, p_{out}>0} d^2 z_C\, P(z_C)\ \rho_{B\,|\,z_C}, \tag{3.44}$$

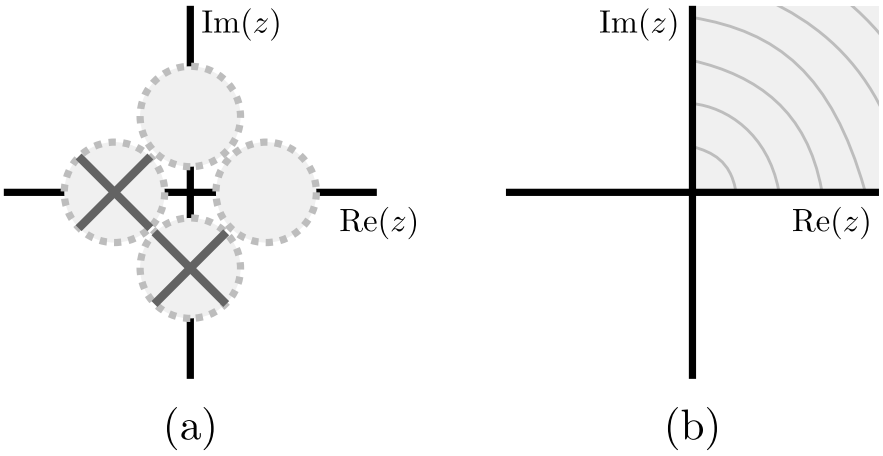


Figure 3.9: Multiple heterodyne outcomes give rise to the same eliminated signature element. (a) A particular eliminated signature element. (b) All possible heterodyne outcomes consistent with (a).

with the normalization factor[9] defined as

$$\mathcal{N}(e_1) = \int_{q_{out}>0, p_{out}>0} d^2 z_C \, P(z_C) \, . \tag{3.45}$$

The conditional state $\rho_{B \mid e_1}$ is the quantum state held by Bob when Charlie has received eliminated signature element e_1. Bob's states conditioned on eliminated signature elements e_2, e_3, e_4 are calculated likewise by varying the limits of integration.

Bob's *a posteriori* entropy, in terms of von Neumann entropy S, reads

$$S_{aposteriori} = \sum_{e_k} P(e_k) \, S\left(\rho_{B \mid e_k}\right) . \tag{3.46}$$

In this chapter we are working in the ideal case where each eliminated signature element is equally likely, and where the entropies of each of the $\rho_{B \mid e_k}$ are equal, and so we may simply write Bob's *a posteriori* entropy as

$$S_{aposteriori} = S\left(\rho_{B \mid e_1}\right) . \tag{3.47}$$

Bob's *a priori* state is given by

$$\rho_{apriori} = \sum_{e_k} P(e_k) \, \rho_{B \mid e_k} \tag{3.48}$$

and the corresponding *a priori* entropy is simply $S\left(\rho_{apriori}\right)$. Finally, using the definiition of Holevo information, Eq. 1.87,

$$\chi = S_{apriori} - S_{aposteriori} . \tag{3.49}$$

We calculate and plot χ under attack BS0 in Fig. 3.12.

9 Clearly the normalization factor $\mathcal{N}$ as defined in Eq. 3.45 is equal to 1/4 for each e_1, e_2, e_3, e_4. We explicitly show the general form for Eq. 3.45 here for completeness, though, as it will become important in Sec. 3.8 when we discuss postselection on measurement outcomes, and in Ch. 5 when assumptions about uniform sending probabilities are relaxed.

BS1: $\xi > 0$

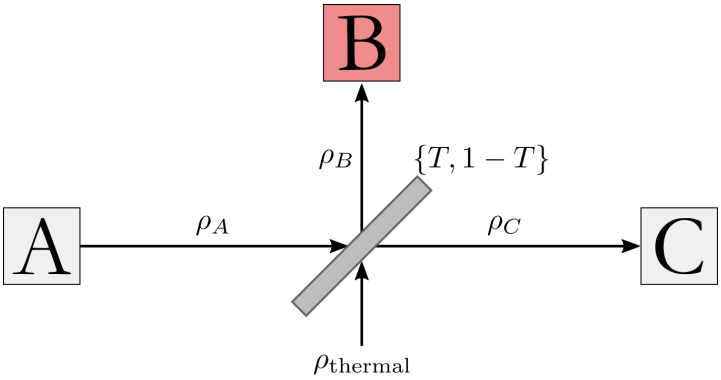


Figure 3.10: Attack BS1. The beamsplitter mimics channel loss, while mixing with thermal state ρ_{thermal} introduces excess noise into Charlie's outcome.

Next, let us consider a modification to attack BS0 which will allow us to model lossy channels which also induce excess noise in Charlie's measurement outcomes. In the first modification, denoted BS1 and displayed in Fig. 3.10, Bob inputs a thermal state ρ_{thermal}, Eq. 1.40, into the second input port of the beamsplitter. This will induce excess noise $\xi > 0$ in Charlie's measurement outcomes consistent with the thermal channel noise, where we define the excess noise in Charlie's q quadrature, when coherent state $|\alpha_k\rangle$ was sent, as

$$\xi_q = \text{Var}\left(q_{\text{out}} \mid \alpha_k\right) - \frac{1}{2}, \tag{3.50}$$

and similarly for p quadrature. In other words, the excess noise in the q quadrature is defined as the quadrature variance above the vacuum variance, and similarly for p. The total excess noise ξ is then taken to be

$$\xi = \max\{\xi_q, \xi_p\}, \tag{3.51}$$

and should be attributed to the action of dishonest Bob. We will calculate Bob's Holevo information under this attack.

We wish to mix a coherent state $\rho_{\alpha_k} = |\alpha_k\rangle\langle\alpha_k|$ and a thermal state ρ_{thermal} on a beamsplitter with transmission T. In the Fock basis our states take the following form:

$$\begin{aligned}
\rho_{\alpha_k} &= e^{-|\alpha_k|^2} \sum_{n,m=0}^{\infty} \frac{\alpha_k^n \alpha_k^{*m}}{\sqrt{n!m!}} |n\rangle\langle m| \\
\rho_{\text{thermal}} &= \left(1 - e^{-\tilde{\beta}}\right) \sum_{p=0}^{\infty} e^{-p\tilde{\beta}} |p\rangle\langle p| \quad \text{with} \quad \tilde{\beta} = \log_e\left(\frac{1}{\bar{n}} + 1\right)
\end{aligned} \tag{3.52}$$

where α_k^* denotes the complex conjugate of α_k. The input state into the beamsplitter is

$$\rho_{\text{input}} = \rho_{\alpha_k} \otimes \rho_{\text{thermal}}. \tag{3.53}$$

Enacting beamsplitter relation Eq. 1.57 on ρ_{input}, and heterodyning on Charlie's mode, we arrive at Bob's conditional output state $\rho_{B\,|\,z_C}$. The state is displayed in full in Eq. B.9, Appendix. B.3.

Now, to reach the *a posteriori* state under this attack we will integrate this $\rho_{B\,|\,z_C}$ over all $z_C \in \mathbb{C}$ consistent with a particular eliminated signature element. Mathematically, this corresponds to simply integrating scalar terms involving z_C in Eq. B.9, noting that the integration operation commutes with the rest of the state. Writing $z = z_C$ for convenience, the required integration is

$$I_{BS1} = \int_{q_{\text{out}}>0, p_{\text{out}}>0} d^2c\; z^k z^{*l} e^{-|z|^2} \tag{3.54}$$

where $k, l = 0, 1, 2, \ldots$.

The integration is best performed in polar coordinates since the radial and angular integrals separate. We find

$$I_{BS1} = \begin{cases} \frac{\pi}{4}\Gamma(k+1) & \text{if } k = l; \\ \frac{-i}{k-l}\left(-1 + e^{i\frac{\pi}{2}(k-l)}\right)\frac{1}{2}\Gamma\left(\frac{1}{2}(k+l+2)\right) & \text{if } k \neq l \end{cases} \tag{3.55}$$

with Γ the gamma function [139]. Indeed, the radial component of the integrand of Eq. 3.54 is a standard integral for Γ. The final *a posteriori* state is now accessible by substituting Eq. 3.55 into Eq. B.9.

The *a priori* state is calculated likewise, but the limits of integration should be extended to the entire complex plane. In this case,

$$\int_{\mathbb{C}} d^2c\; e^{-|z|^2} z^k z^{*l} = \pi\Gamma(k+1) = \pi k! \tag{3.56}$$

since the polar integral forces $k = l$. The Holevo information may now be calculated in the same way as Sec. 3.6.1 by the difference of *a priori* and *a posteriori* entropies, and we compare Holevo information under different attacks in Fig. 3.12.

3.6.2 *Entangling-cloner attack*

The entangling cloner attack [99, 138], depicted in Fig. 3.11, is ideally suited to consistently incorporate the presence of excess noise ξ, and we shall see that it is a much more powerful attack than any of the beamsplitter attacks considered above. The entangling cloner attack, which we shall denote EC, may be viewed as a natural extension of attack BS1.

Instead of inputting a thermal state into the beamsplitter's fourth port, Bob will input one arm of his entangled two-mode squeezed

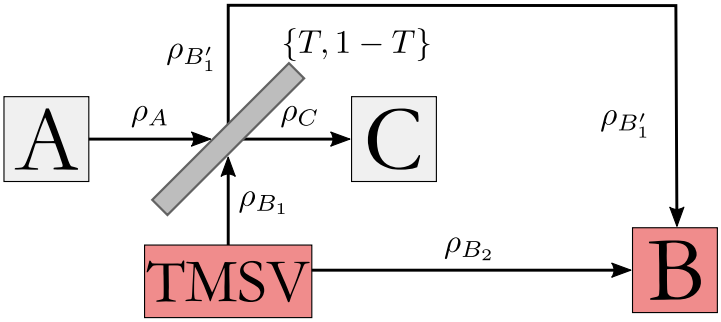


Figure 3.11: EC attack. Locally, one mode of the TMSV looks like ρ_{thermal} and so allows channel excess noise to be emulated. Bob can exploit correlations in noise between his two mode output state ρ_{B_1',B_2} to gain additional information.

vacuum (TMSV) state, Eq. 1.51. The mode which Bob inputs into the channel is locally indistinguishable from ρ_{thermal}, and so honest players are unable to distinguish between BS1, BS2 and EC.

Let us analyse the EC attack. Alice creates the coherent state $|\alpha_k\rangle\langle\alpha_k|$, while Bob generates

$$\rho_{\text{TMSV}} = \frac{1}{\cosh^2\zeta} \sum_{n,m=0}^{\infty} (\tanh\zeta)^{n+m} \, |n,n\rangle\langle m,m| \, . \tag{3.57}$$

Let us write the three-mode input state to the channel as

$$\begin{aligned} \rho_{\text{input}} = \frac{e^{-|\alpha_k|^2}}{\cosh^2\zeta} \sum_{n_1,m_1=0}^{\infty} \sum_{n_2,m_2=0}^{\infty} \frac{\alpha_k^{n_1}\overline{\alpha_k}^{m_1}}{\sqrt{n_1!m_1!}} (\tanh\zeta)^{n_2+m_2} \\ \times \Big[|n_1,n_2\rangle\langle m_1,m_2| \Big] \otimes |n_2\rangle\langle m_2| \, , \end{aligned} \tag{3.58}$$

where we have explicitly separated in square brackets the two modes which will interfere on the beamsplitter.

The beamsplitter mixes $|n_1,n_2\rangle\langle m_1,m_2|$ via Eq. 1.55, and gives an entangled three-mode state at the output. Charlie heterodynes on his mode and receives outcome z_C, and we arrive at Bob's conditional two-mode output state $\rho_{B\,|\,z_C}$, which we display fully in Eq. B.13, Appendix. B.4. Once again the state is readily integrated in z_C, either over the entire complex plane or a single quadrant, and we may simply substitute Eqs. 3.55, 3.56 into Eq. B.13 to reach the *a posteriori* and *a priori* states, respectively.

The *a priori* state is automatically normalized by virtue of the integration over $\mathbb{C}$, while the *a posteriori* state is normalized by multiplying by $\mathcal{N}(e_1 \mid \xi)$, defined as

$$\mathcal{N}(e_1 \mid \xi) = \int_{q_{\text{out}}>0, p_{\text{out}}>0} d^2c \, P(z_C \mid \xi) \, . \tag{3.59}$$

where we have included excess noise ξ in our probability, as in Appendix. A. The performance of this attack is analysed in Fig. 3.12.

3.6.3 *Comparison of attacks*

We compare attacks BS0, BS1 and EC in Fig. 3.12 as amplitude α and channel transmission T are varied. We observe that for all α, T and for all channel thermal photon numbers $\bar{n}$ the EC attack performs best, while attack BS1 performs worse than even attack BS0 where no excess noise is considered. Under EC, Bob is permitted to exploit correlations between his two modes, and the $\bar{n}$ restricts the level of entanglement between his modes. Larger $\bar{n}$ means greater entanglement, and so we should expect that as $\bar{n}$ increases Bob gains more information. However, under BS1 Bob is not permitted to use these correlations, and so his outcomes and Charlie's outcomes are both noisy. The added noise reduces Bob's information without providing him the advantage of EC.

The thermal photon number $\bar{n}$ is related to the inverse temperature of the input thermal state in BS1 as [1]

$$\beta = \log_e\left(\frac{1}{\bar{n}} + 1\right), \tag{3.60}$$

while $\bar{n}$ is related to the squeezing parameter ζ of the input TMSV state in EC as [1]

$$\zeta = \mathrm{Sinh}^{-1}\left(\sqrt{\bar{n}}\right). \tag{3.61}$$

Since under attack BS1 Bob performs worse than BS0, we are led to consider an attack which can be considered mid-way between the power of BS0 and EC. We modify the attack by imposing that the channel excess noise should *only* affect honest players. That is, the presence of ξ causes p_{err} to increase, but Holevo information and therefore p_e should both be unaffected. We call this attack BS2. While strictly this attack is physically inconsistent, and therefore impossible for Bob to perform, it is more pessimistic for honest players than either BS0 or BS1 and so the security bounds it gives are also safe bounds on both of those attacks. Indeed, since an analytic expression for Bob's states under attack BS0 is readily attainable without resort to the numerical methods required for BS1 (Appendix B), in some circumstances it may even be computationally preferable to assume attack BS2. The Holevo information is given by using Eqs. 3.44 and 3.48 in the usual way, while p_{err} is given in Appendix A.

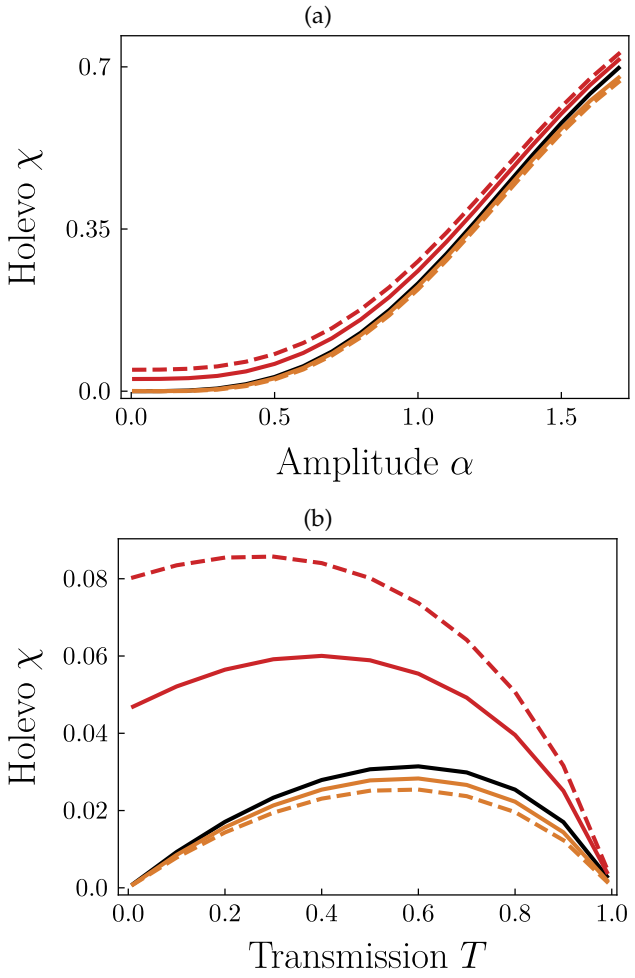


Figure 3.12: Comparison of Holevo information χ under attacks BS0 (black), BS1 (orange) and EC (red). BS0 has no excess noise in the channel which corresponds to channel thermal photon number $\bar{n} = 0$. BS1 and EC both include excess noise, with $\bar{n} = 0.01$ (solid red/orange lines) and $\bar{n} = 0.02$ (dashed red/orange lines). (a) Increasing amplitude α of the QPSK alphabet leads to larger Holevo information for dishonest Bob. Honest players should therefore choose small α. (b) At $T = 0$ and $T = 1$ Bob gains no information about Charlie's outcomes. In both (a) and (b), we see that EC attack gives Bob much more information than BS0, while BS1 performs worse.

3.7 SIGNATURE LENGTH L

We have proven protocol security against both repudiation (Sec. 3.2) and forgery (Sec. 3.4). and we have shown that our QDS protocol is robust (Sec. 3.3). Additionally, we have demonstrated how a forging Bob's probability p_e to introduce a mismatch into his signature is related to the Holevo information χ of his quantum system (Sec. 3.5) and have explicitly analysed several attacks which he may perform which mimic different channel conditions (Sec. 3.6). We are now in a position to calculate the total probability that our QDS protocol fails to meet the security requirements outlined in List. 3.1. We shall see that the total failure probability decays exponentially, and so our protocol is secure.

Let us define $\varepsilon_{\text{fail}}$ as the total probability that our protocol fails, either by allowing a repudiation or forging attack, or by aborting when all players behaved honestly. To gain a figure of merit we assume that the protocol is equally likely to fail in any of these ways, and so we set

$$\varepsilon_{\text{fail}} = \varepsilon_{\text{honest abort}} = \varepsilon_{\text{repudiation}} = \varepsilon_{\text{forgery}}, \tag{3.62}$$

though we note that alternative combinations may be easily considered. Let us eliminate the free parameters s_B, s_C by equating the arguments of Eqs. 3.19, 3.21, 3.27:

$$(p_e - s_C)^2 = \frac{1}{4}(s_C - s_B)^2 = (s_B - p_{\text{err}})^2, \tag{3.63}$$

from which we may derive

$$s_B = \frac{3}{4}p_{\text{err}} + \frac{1}{4}p_e \quad \text{and} \quad s_C = \frac{1}{4}p_{\text{err}} + \frac{3}{4}p_e, \tag{3.64}$$

as our choices of security thresholds. Notice that since $p_{\text{err}} \leqslant p_e$, Eq. 3.64 automatically fulfils the requirement that $s_B \leqslant s_C$. The overall probability of failure Eq. 3.62 therefore becomes

$$\varepsilon_{\text{fail}} \leqslant 2\exp\left(-\left[p_e - p_{\text{err}}\right]^2 \frac{L}{16}\right). \tag{3.65}$$

This probability $\varepsilon_{\text{fail}}$ decays exponentially in L, and so provided that p_{err} and p_e are known, and $p_e - p_{\text{err}} \geqslant 0$, any security level $\varepsilon_{\text{fail}} > 0$ may be reached by varying signature length L. In keeping with the recent works Refs. [44, 46, 47, 73] in this Thesis we will take $\varepsilon_{\text{fail}} = 0.01\%$. Equation 3.65 may then be solved for the signature length. We take L as the main figure of merit[10] for a QDS protocol, and analyse the performance of our protocol in Sec. 3.9.

10 Analogously to the key rate in QKD.

3.8 POSTSELECTION

In the context of QKD it has been known for some time that a postselection of measurement outcomes, in which measurement outcomes unfavourable to honest players are discarded, will improve the key rates in the presence of excess noise. Postselection is even a requirement to distill a key below $T \leqslant 1/2$ in the direct reconciliation regime [140]. We are thus motivated to apply postselection to our QDS protocol in order to allow a message to be securely signed over a larger range of channel parameters, and we shall see that it can reduce the necessary L. The results of this section will be especially useful in Ch. 5 where – as for direct reconciliation QKD – we shall see that postselection is a necessity for some QDS protocols.

For now, we will apply postselection to the protocol outlined in this chapter. To apply the postselection technique, recipients Bob and Charlie will simply disregard unfavourable measurement outcomes, i.e. outcomes for which a dishonest player is deemed to have too much knowledge, or for which the probability of honest mismatch is too high.

We define a region $\mathcal{R}_{PS} \in \mathbb{C}$, Fig. 3.13. Honest recipients will only accept measurement outcomes (q_{out}, p_{out}) with $c := q_{out} + ip_{out} \in \mathbb{C} \setminus \mathcal{R}_{PS}$. We may then vary $\mathcal{R}_{PS}$ in order to increase the range of channel parameters for which the QDS protocol is secure, and to minimize signature length L.

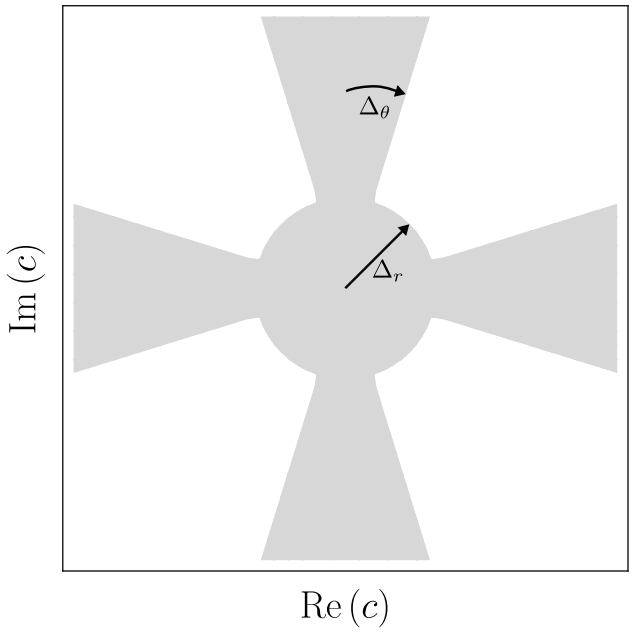


Figure 3.13: The postselection region $\mathcal{R}_{PS}$, gray, is parametrized by Δ_r, Δ_θ in polar coordinates. Participants will only accept measurement outcomes $c \in \mathbb{C} \setminus \mathcal{R}_{PS}$.

Our chosen $\mathcal{R}_{PS}$ is parametrized by two variables Δ_r, Δ_θ in polar coordinates, Fig. 3.13. This is the same postselection region which was considered in the recent work Ref. [141], but if desired more general regions may be readily considered. We make no claims as to the optimality of our choice of the shape $\mathcal{R}_{PS}$, though once the form of $\mathcal{R}_{PS}$ is set we may optimize over Δ_r and Δ_θ to improve protocol security.

The crucial quantity which controls the security of our QDS protocol is $g_{sec} := p_e - p_{err}$, which describes how much more likely a dishonest player is to induce a mismatch than an honest player. We saw in Sec. 3.7 that our QDS protocol is secure provided that $g_{sec} > 0$, and that the signature length L required to sign to a given level of security ε_{fail} is directly controlled by g_{sec}. We therefore must consider how postselection affects g_{sec}.

Let us begin with the effect of postselection on $p_{err} = p_{err}(\Delta_r, \Delta_\theta)$. Recall that when Alice sends state $|\alpha\rangle$ through a lossy but noiseless channel, transmission T, Charlie receives $c \in \mathbb{C}$ with probability

$$P(c \mid \alpha, T) = \frac{1}{\pi} \exp\left(-\left|c - \sqrt{T}\alpha\right|^2\right). \tag{3.66}$$

Thus the probability of eliminating the state $|\alpha\rangle$ when no postselection is used is, in polar coordinates,

$$\begin{aligned} p_{err} &= \int_{r=0}^{\infty} dr\, r \int_{\theta=\pi/2}^{3\pi/2} d\theta\, P\left(re^{i\theta} \mid \alpha, T\right) \\ &= \frac{1}{2}\operatorname{erfc}\left(\sqrt{\frac{T}{2}}|\alpha|\right). \end{aligned} \tag{3.67}$$

When the postselection technique is used we must change the limits of integration, so the mismatch probability becomes

$$\begin{aligned} p_{err}(\Delta_r, \Delta_\theta) = \frac{1}{\mathcal{N}} \int_{\Delta_r}^{\infty} dr\, r \Bigg[&\int_{\pi/2+\Delta_\theta}^{\pi-\Delta_\theta} d\theta\, P\left(re^{i\theta} \mid \alpha, T\right) \\ &+ \int_{3\pi/2-\Delta_\theta}^{\pi+\Delta_\theta} d\theta\, P\left(re^{i\theta} \mid \alpha, T\right) \Bigg], \end{aligned} \tag{3.68}$$

where we effectively have the same integrals as Eq. 3.67 restricted by $\mathcal{R}_{PS}$. The normalization probability $\mathcal{N}$ is the probability that Charlie will accept his measurement outcome, which is calculated by extending the integration in Eq. 3.68 to the entire $\mathbb{C} \setminus \mathcal{R}_{PS}$

$$\mathcal{N} = \int_{\mathbb{C}\setminus\mathcal{R}_{PS}} d^2c\, P(c \mid \alpha, T, \xi). \tag{3.69}$$

The calculation of $p_{\text{err}}(\Delta_r, \Delta_\theta)$ follows identically to Eq. 3.68 when excess noise ξ is included, simply using the requisite formula (Appendix A) and performing the integrations as Eq. 3.68.

Since a dishonest player's declaration will depend on an honest player's heterodyne outcome, the probability p_e must also vary with $\mathcal{R}_{\text{PS}}$. We will calculate the effect of $\mathcal{R}_{\text{PS}}$ on Holevo information χ, from which the probability p_e is calculated via Eq. 3.40 as normal.

Assume that Bob has performed any one of the attacks examined in Sec. 3.6, and let Bob's state after Charlie's heterodyne measurement be denoted $\rho^j_{B\,|\,c}$. Again, since Charlie's eliminated signature element is entirely determined by the quadrant in which c lies, the state $\rho^j_{B\,|\,e_k}$ is calculated by mixing $\rho^j_{B\,|\,c}$ over an entire quadrant of phase-space, as in Eqs. 3.44, 3.55, Tab. 3.1. We must therefore update these integrals to include the effect of $\mathcal{R}_{\text{PS}}$. For example,

$$\rho^j_{B\,|\,e_1} = \frac{1}{\mathcal{N}} \int d^2c\, \rho^j_{B\,|\,c} = \frac{1}{\mathcal{N}} \int_{\Delta_r}^{\infty} dr\, r \int_{\Delta_\theta}^{\pi/2-\Delta_\theta} d\theta\, \rho_{B\,|\,re^{i\theta}}, \tag{3.70}$$

and similarly for e_2, e_3, e_4. The $\mathcal{N}$ is identical to that required for Eq. 3.68, and Bob's *a priori* state is found by mixing Eq. 3.70 over all quadrants. Probability $p_e(\Delta_r, \Delta_\theta)$ may now be calculated via Eq. 3.40.

To actually perform the integration, we separate out terms involving c in Bob's state and so the integration becomes

$$\frac{1}{\mathcal{N}} \int_{\Delta_r}^{\infty} dr\, r \int_{\Delta_\theta}^{\pi/2-\Delta_\theta} d\theta\, r^k r^l e^{-r^2} e^{i\theta(k-l)}. \tag{3.71}$$

where we have used $c = re^{i\theta}$. To perform the integration, it is helpful to perform the angular integral first, which readily integrates to a sum of exponentials when $k \neq l$, or to $\pi/2 - 2\Delta_\theta$ when $k = l$. The remaining radial term is

$$\int_{\Delta_r}^{\infty} dr\, r^{k+l+1} e^{-r^2} \tag{3.72}$$

which is the definition of an upper incomplete Gamma function [142], which we denote as $\Gamma_\uparrow$. The radial integration Eq. 3.72 is thus identically

$$\Gamma_\uparrow\left(\frac{1}{2}[2+k+l], \Delta_r^2\right), \forall k, l \geqslant 0 \tag{3.73}$$

which may be easily calculated.

We have now included the effects of $\mathcal{R}_{\text{PS}}$ on g_{sec}, and so the performance of the protocol under postselection may be analysed. In Fig. 3.14 we plot g_{sec} varying $\mathcal{R}_{\text{PS}}$ for attacks BS0, BS1, and EC, and

for different coherent state amplitude α's at $T = 0.5$. We observe that when considering g_{sec}, it is advantageous to choose a large postselection region as this always allows g_{sec} to increase. However we also observe that the effectiveness of postselection depends on our coherent state amplitude. For example, at $\alpha = 0.2$ we see smaller increase in g_{sec} as $\mathcal{R}_{PS}$ is increased, and there is almost no effect of postselection as Δ_θ is varied under EC attack.

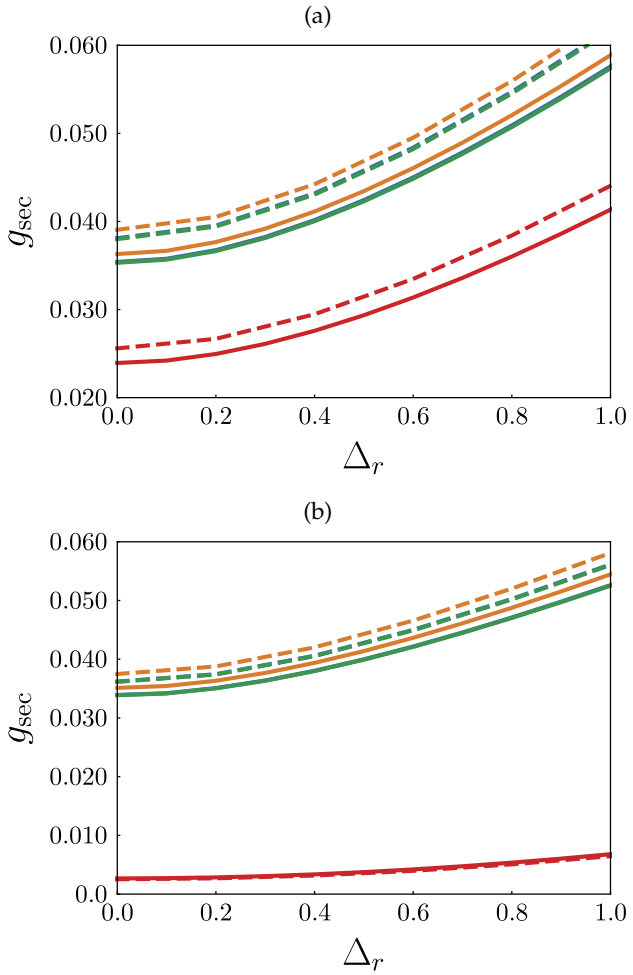


Figure 3.14: The efficacy of postselection depends strongly both on attack type and parameters α, T. Solid: $\Delta_\theta = 0$. Dashed: $\Delta_\theta = 0.3$. Green: BS0. Orange: BS1. Red: EC. (a) $\alpha = 0.5, T = 0.5$ and (b) $\alpha = 0.2, T = 0.5$. In both graphs attacks BS1 and EC have excess noise $\xi = 0.1\%$.

Let us turn now to examine our main figure of merit, the number of quantum states L used in the protocol. Directly incorporating $g_{sec}(\Delta_r, \Delta_\theta)$ into Eq. 3.65 will give an erroneous level of security, for the following reason. Our calculations in this section, culminating in $g_{sec}(\Delta_r, \Delta_\theta)$, correctly bound the number of states required to sign a message to security level ε_{fail}. However, this is not equivalent to the number of states which Alice has actually sent.

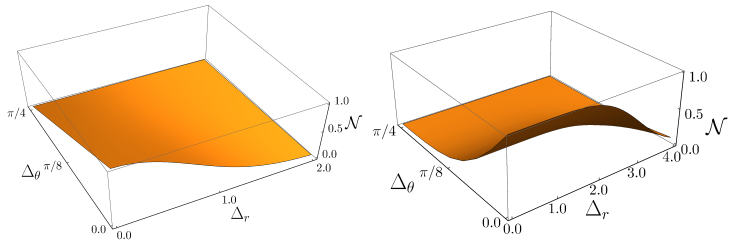
For example under attack EC with $\alpha = 0.5, T = 0.5, \xi = 0.1\%$, choosing $\Delta_r = 4.0$ and $\Delta_\theta = 0.4$ gives $g_{sec} = 0.1225$. Substituting this into Eq. 3.65 and solving for L gives $L = 10560$. But in order to have that many states accepted at Charlie, Alice will actually need to have sent 7×10^{10} coherent states in total, since Charlie will reject his measurement outcomes with probability $1 - (1.5 \times 10^{-7})$, Eq. 3.69. It follows that L, as implicitly defined by Eq. 3.65, is actually a poor figure of merit to measure the resource-use of our protocol when postselection is used.

Instead, we will work in terms of $\tilde{L}$, which we define as the total number of states sent by Alice. This may be written as a rescaling of L given by

$$L \mapsto \tilde{L} := \frac{L}{\mathcal{N}}, \tag{3.74}$$

with the normalization factor $\mathcal{N}$ interpreted sthe average probability that Charlie accepts a given state sent by Alice, Eq. 3.69.

We plot $\mathcal{N}$ in Fig. 3.15, and figure of merit $\tilde{L}$ in Fig. 3.16. We observe that even though large Δ_θ causes g_{sec} to increase, Fig. 3.14, it also causes an increase in $\tilde{L}$, owing to the quick decay of $\mathcal{N}$ with Δ_θ, Fig. 3.15. We also may deduce from the graphs Fig. 3.16 that there is an optimum Δ_r which minimizes $\tilde{L}$ and gives the best performance of our protocol.



(a) (b)

Figure 3.15: Normalization factor $\mathcal{N}$ Eq. 3.69 varies dramatically with postselection region $\mathcal{R}_{PS}$. (a) $\alpha = 0.5, T = 0.5$. (b) $\alpha = 3.0, T = 1.0$

Since the figures of merit $\tilde{L}$ (with postselection) and L (without postselection) measure the same thing – how many states must Alice send in order to sign a 1 bit message – they may be directly compared. For the remainder of this Thesis, then, we will not distinguish between $\tilde{L}$ and L. It should be understood that when postselection is used we are using the rescaled $\tilde{L}$, while when postselection is not use we are using L. Furthermore, since $\Delta_\theta > 0$ causes $\tilde{L}$ to increase we will take the optimal $\Delta_\theta = 0$ always from now on, and only allow Δ_r to vary. It will be made clear in what follows whether the postselection technique has been used and the choice of Δ_r.

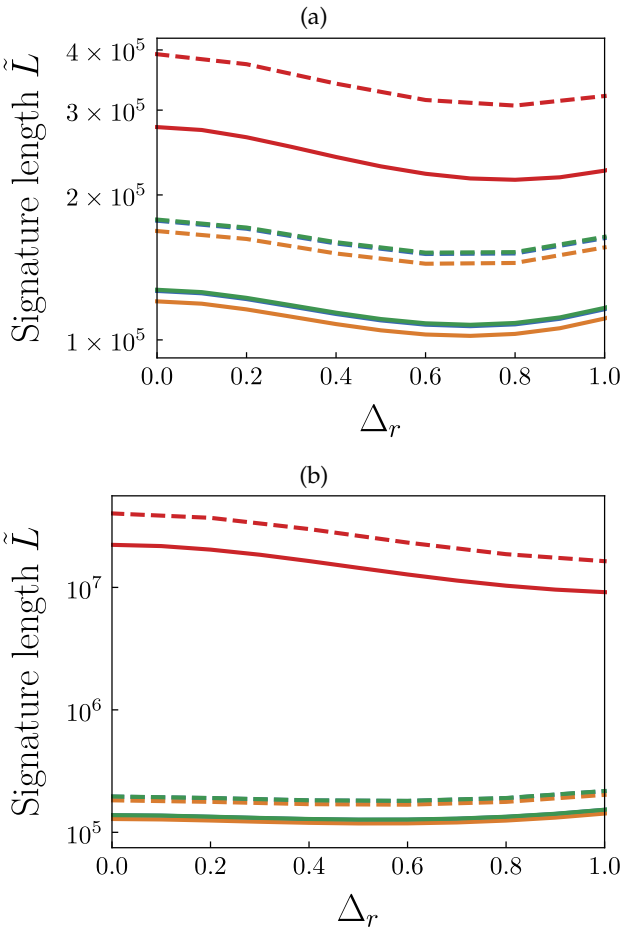


Figure 3.16: The key figure of merit, $\tilde{L}$, depends strongly on postselection region $\mathcal{R}_{PS}$. Solid: $\Delta_\theta = 0$. Dashed: $\Delta_\theta = 0.3$. Green: BS0. Orange: BS1. Red: EC. (a) $\alpha = 0.5, T = 0.5$ and (b) $\alpha = 0.2, T = 0.5$. In both graphs attacks BS1 and EC have $\xi = 0.1\%$. In all cases it is optimal to choose $\Delta_\theta = 0$

3.9 PROTOCOL PERFORMANCE

Let us apply the analysis performed in the previous few sections and calculate our main figure of merit, the signature length L, under several different attacks. We plot the signature length L required to sign a 1 bit message under attacks BS0 (black) and EC (red) in Fig. 3.17, for several different α. An entangling cloner attack with $\xi = 0.1\%$ has vastly increased signature length for $\alpha = 0.2$ (dotted), while for larger $\alpha = 0.5, 0.8$, entangling-cloner causes the signature length to increase by more modest amounts when compared to BS0. Note that in Fig. 3.17 the transmissions T at which the lines stop should be interpreted as being close to the smallest T attainable before L begins to diverge, and signing a message becomes impractical (in the case of BS0) or impossible (in the case of EC).

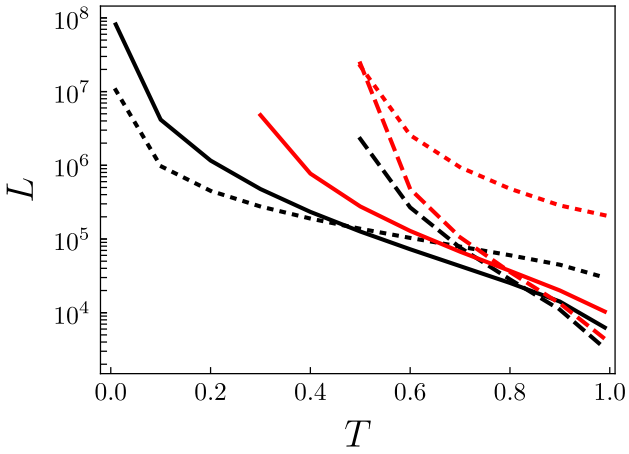


Figure 3.17: Signature lengths L varying with channel transmission T for attacks BS0 (black) and EC (red). Solid: $\alpha = 0.5$. Dashed: $\alpha = 0.8$. Dotted: $\alpha = 0.2$. Entangling cloner attack has excess noise $\xi = 0.1\%$ at all T. A non-optimal choice of α can lead to much larger signature lengths. No postselection is used.

Even when attack BS0 is used and $\xi = 0\%$, a sub-optimal choice of coherent state amplitude α can drastically worsen the performance of the protocol. To investigate optimal amplitudes, we plot the security parameter g_{sec} varying with α under attack BS0 in Fig. 3.18. We observe that the optimal α decreases with increasing loss (smaller T). Intuitively, at $T = 1.0$ Eve gains no information and so one should pick $\alpha \gg 1$ so as to minimize the mismatch rate between honest players.

We also compare our current protocol to a recent CV QDS protocol [73] which did not allow for the presence of an eavesdropper on the quantum channels. The security parameter under Ref. [73] is displayed as red, dot-dashed lines in Fig. 3.18 at $T = 0.47$ (top) and $T = 0.19$ (bottom). We see that for larger T, and almost all α at smaller T, our current protocol outperforms Ref. [73], despite our relaxing the requirement of secure quantum channels. This surprising

improvement in performance comes directly from the fact that in the current protocol, Alice distributes different signatures to each recipient, whereas in Ref. [73] she distributed identical signatures.

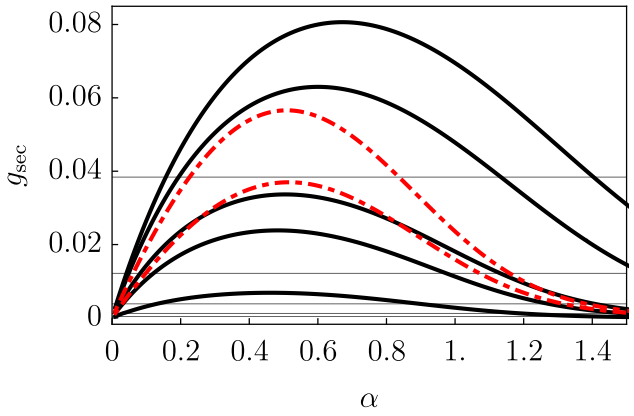


Figure 3.18: Security parameter g_{sec} under attack BS0 as it varies with α for $T = 0.61, 0.47, 0.19, 0.11, 0.01$ (solid, black, top to bottom). The optimal α which should be chosen to maximize g_{sec} (minimize L) decreases as T decreases. Horizontal gridlines denote $\mathcal{O}(L)$ starting from $L \sim 10^5$ at $g_{sec} = 0.038$ (top), with L increasing by a factor of 10 at subsequent lower gridlines. Red, dot-dashed: g_{sec} calculated via the protocol described in Ref. [73] for $T = 0.19$ and $T = 0.47$.

We optimize over α and postselection region Δ_r in Fig. 3.19. The figure thus represents the smallest attainable L for our protocol under attacks BS0 (solid, blue), BS2 (dashed, orange) and EC (solid, red). Attack BS1 gives smaller L than even BS0, and so we do not show it. Even at the $T \sim 0.4$ corresponding to a fiber length ~ 20 km, the attainable L are very modest at only $\mathcal{O}(10^5)$ under BS0 and $\mathcal{O}(10^6)$ for EC attacks.

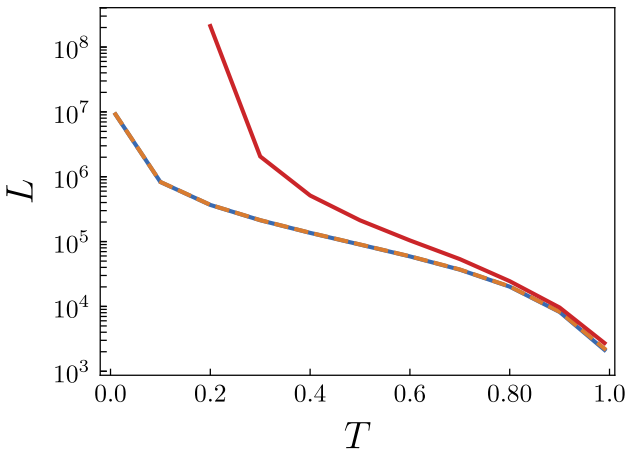


Figure 3.19: Signature lengths under protocols BS0 (blue, solid), BS2 (orange, dashed) and EC (red, solid). At each point L is optimized over α and postselection parameter Δ_r. EC attack with $\xi = 0.1\%$.

Finally, in Appendix C we extend the protocol discussed in this chapter to allow for larger alphabet sizes. These alphabets, which we denote as NPSK alphabets, consist of N coherent states equally distributed around the origin of phase space. The case $N = 4$ is equivalent to the QPSK alphabet which we have used until now. For NPSK alphabets with $N = 2$, $N = 4$, $N = 6$, $N = 8$ we plot their signature lengths optimized over α in Fig. 3.20, and the required optimal α's are displayed in the inset.

Surprisingly, although for larger alphabets the optimal α is decreased, the minimal L is slightly increased. As has been found elsewhere [143], the biggest leap in behaviour should occur between $2 \to 4$, and indeed this is what we see[11]. As N increases, with $\alpha \ll 1$ we tend closer towards a Gaussian mixture of coherent states (c.f. Fig. 1.4b). We may therefore reasonably expect the attack strategies BS0 and EC to become increasingly optimal in this Gaussian limit, which explains the slight increase in L for larger alphabets.

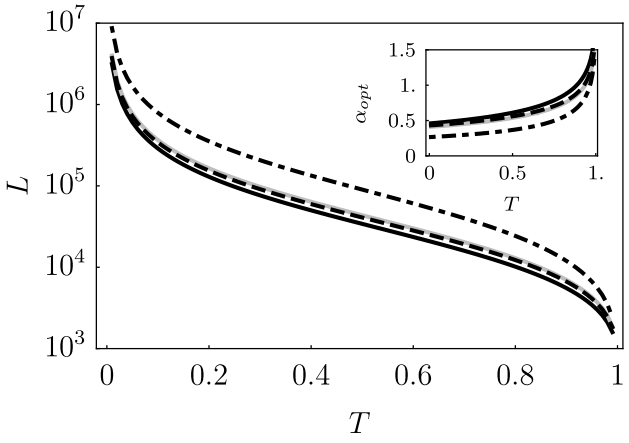


Figure 3.20: Signature length L under attack BS0. At each T, length L has been optimized over amplitude $|\alpha|$ of the alphabet. We have considered NPSK alphabets with $N = 2, 4, 6, 8$. Dot-dashed: $N = 2$. Black, solid: $N = 4$. Dashed: $N = 6$. Gray, solid: $N = 8$. Inset: the corresponding optimal α_{opt}.

3.10 OUTLOOK

Quantum digital signatures, which use quantum resources to allow for secure authentication of a classical message, have only recently been proven secure against a quantum eavesdropper on the channels [47, 55, 64]. In this Chapter, we have progressed continuous-variables QDS by providing security against an eavesdropper performing one of several beamsplitter attacks, or an entangling-cloner attack, on the quantum channels. Surprisingly, short signature signature lengths are sufficient

11 Noting that for the case $N = 2$ we no longer need to think about an eliminated signature and we may simply consider optimal guessing probabilities.

to perform secure QDS over metropolitan distances, and we require even shorter signatures than a comparable scheme in Ref. [73] which assumed secure quantum channels. Our security proof has enabled us also to take into account the fact that for each eliminated signature element there are multiple "correct" declarations which a dishonest player can make.

Our security proof has relied on several assumptions which reflect the state-of-the-art of CV quantum cryptography with our chosen alphabet of discrete-modulated coherent states, but which future work should strive to relax. First, the eavesdropping attacks permitted by a dishonest player in this chapter do not give them the full power of quantum mechanics, and there are additional attacks which could be performed which may prove additionally effective. For example, a dishonest player could begin to induce and exploit quantum correlations between subsequent distributed states. There may also be additional attacks on individual signature elements which are more powerful than the ones considered here. The non-Gaussianity of our alphabet is restrictive, and the entangling-cloner attack is only expected to be optimal as a limiting case that the QPSK alphabet becomes Gaussian, i.e. $\alpha \to 0$ [144, 145]. One possible route towards a fuller security analysis could be an extension of results known for QKD with two-state [146] and three-state [147] alphabets to our four-state alphabet, noting recent progress in Ref. [137]. We expect that such an extension, if even possible, will be challenging.

One may begin to further consider the finite-size effects [18] which are intrinsic to any QDS scheme, noting the operational links between the guessing probabilities p_e considered in this Chapter, and the smooth min-entropy [51]. Calculations of the smooth min-entropy have been used to good effect for DV QDS in Refs. [47, 64], where we note that a full calculation also allows for security against coherent attacks. Advances in calculating optimal lower bounds for the smooth min-entropy under a discrete-modulated coherent state alphabet will have immediate and direct application to CV QDS, and may be readily incorporated into our security proof. Recent work [148] has allowed for direct calculations of smooth min-entropy for an alphabet of Gaussian-modulated coherent states via the covariance matrix formalism, and recent QKD work [96] has successfully handled the QPSK alphabet in the asymptotic regime only by assuming that it is Gaussian, i.e. $\alpha \ll 1$, allowing the mixture of states to be completely described by a covariance matrix. In our case, however, choosing α such that this criterion is met and any bounds are tight enough to be useful, also gives very large p_{err} rendering our protocol insecure.

The work by Lin *et. al.* [141] has removed the Gaussian assumption by applying new reformulations of the Devetak-Winter key rate bounds and the related semi-definite programming optimizations [72, 149], but they are still forced to make the assumption to truncate

their Hilbert space sizes in order to make the problem numerically tractable. While this does provide a high level of security, it further demonstrates that the ideal methods to provide general coherent QKD security for the QPSK alphabet–even in the asymptotic case–are by no means settled. Further work is needed.

A fully Gaussian CV QDS protocol is conceivable, in which Alice distributes coherent states chosen from a Gaussian probability distribution. It is likely that the resulting analysis could proceed almost entirely in the covariance matrix formalism [13, 14], for which good bounds for smooth min-entropy are known [148]. One should take care in the analysis to correctly define p_{err} however, as there is now no natural partitioning of phase-space. One may therefore also need to optimize over the best choice of phase-space partition with which to define an eliminated signature, and it will be interesting to observe how this partitioning is affected by channel parameters T, ξ, the variance of the underlying Gaussian probability distribution, and the choice of postselection region $\mathcal{R}_{\text{PS}}$.

The security of our QDS protocol and the short L required to sign a message, stemming both from our security proof and the practical advantages of the CV platform, make CV QDS an attractive scheme for secure communications in a quantum future. We further explore this protocol in Chapter 5 where we investigate its practical experimental implementation alongside related cryptographic protocols. We demonstrate, there, that the short signature lengths obtained for this protocol result in small times required to sign a message in a practical implementation. Thus, to our knowledge, this QDS protocol is the fastest protocol over comparable distances.

A brief discussion of the numerical methods which are used for this current Chapter may be found in Appendix B, where we also display the full quantum states used for attacks BS0, BS1 and EC.

4

QUANTUM SECRET SHARING

In this chapter we introduce and investigate a continuous-variable Quantum Secret Sharing (QSS) protocol, which allows for secure distribution of a classical secret among multiple potentially dishonest recipients. Crucially, recipients are forced to collaborate in order to reconstruct the secret, and a dishonest player should not be able to access the secret by themselves.

We describe the protocol and its similarities and differences to recent QSS protocols from the literature in Sec. 4.1, and then prove its security against several different attack strategies in Secs. 4.2, 4.3. In Sec. 4.4 we analyse the performance of our protocol. Although the QSS task has been around for many years, many of the existing protocols are not suitable for implementation, despite their high level of security. We present the implementation of our protocol in Chapter 5.

4.1 OUR QSS PROTOCOL

Our Quantum Secret Sharing (QSS) scheme allows for Alice to distribute a classical secret between two recipients, Bob and Charlie. To keep with convention we call Alice the "dealer". Either Bob or Charlie is dishonest, and Alice does not know which one. Bob and Charlie should be able to exactly reconstruct the secret when they work together, while the dishonest player should not be able to access the secret by themselves, or even if they work with an external Eve.

4.1.1 *QSS setup*

All QSS protocols follow essentially the same structure, Fig. 4.1:

1. Alice (A) uses quantum resources to distribute shares of classical key K_A among recipients Bob (B) and Charlie (C). These shares are labelled K_B, K_C and are such that $K_A = K_B \oplus K_C$.

2. Alice encrypts her secret $\Upsilon_A = K_A \oplus \sigma_A$ and makes the encrypted secret Υ_A publicly known.

The $\oplus$ operation corresponds to bitwise addition (XOR) of binary strings. Provided that K_A, K_B, K_C and σ_A are the same length, the above secret sharing operation is provably unconditionally secure[1] provided that key shares K_B, K_C are securely distributed [24].

1 Much like the One Time Pad [24].

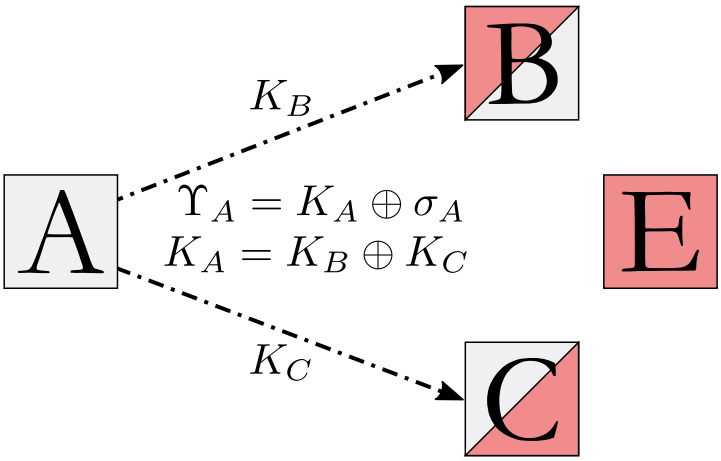


Figure 4.1: All quantum secret sharing schemes follow the same structure: Alice encrypts her classical secret σ_A with secret key K_A, and broadcasts the resulting Υ_A. Shares of K_A are distributed among recipients Bob and Charlie such that $K_B \oplus K_C = K_A$. Gray boxes denote honest players, while red denotes dishonest players. The half-red/half-gray boxes denote uncertainty about the honesty of a player.

This form of protocol is similar to QKD-based encryption, and it is for this reason that renowned cryptographer Gustavus Simmons wrote that

"Secret sharing is simply a special form of key distribution"

as his abstract to Ref. [150].

QSS protocols, then, only differ in the method used to generate and share the K_B, K_C forming the encryption key. One potentially attractive option would be for Alice to perform individual QKD protocols, first with Bob and then with Charlie, and then XOR the resulting secure keys together. Since QKD is provably secure against a quantum adversary, neither Bob nor Charlie can gain sufficient information about the other player's key, and the resulting QSS scheme is thus also secure. Alternatively, once the secure keys are shared between Alice-Bob and Alice-Charlie, they could implement one of several classical unconditionally secure schemes which are discussed in Sec. 2.3.

Other options for distribution of a secret using quantum resources are discussed in Sec. 2.3 and fall into one of two categories. The first category [97, 98, 100, 107, 108, 151] relies on large entangled states shared between all N players, while the second category [112, 113, 117, 118], involves distribution of a single (typically one-mode) quantum state between all N players, who each perform their choice of measurement on the state. In both forms, if $N-1$ players communicate and share their choice of measurement and their measurement outcomes, they have sufficient information to infer the measurement outcome of the N^{th} player. In this way, a key K_A is distributed between players.

4.1.2 *QSS protocol description*

We here propose a QSS protocol which will perform the task of quantum secret sharing without requiring the distribution of highly entangled states between players [108] and without requiring a dedicated hardware or network setup [118]. Instead, we rely on distribution of QPSK alphabet and heterodyne detection. Our QSS protocol guards against eavesdropping by choosing a QPSK alphabet with small coherent state amplitude α. This ensures that Eve cannot accurately guess Alice's heterodyne outcomes. The protocol also guards against the internal dishonesty of Bob or Charlie by ensuring that the key K_A, which Alice will use to encrypt her secret, is a function of *both* Bob and Charlie's information.

In our protocol, Bob and Charlie are chosen as the senders of the quantum states. This has advantage in that we may fully trust Alice's heterodyne detection[2] and its characterisation. A dishonest internal player will be forced to collaborate with Eve to attack the honest player's quantum channel, but by our choice of alphabet, this will not succeed. Since Alice will decide on the eventual shared key our protocol is analogous to a reverse-reconciliation (RR) QKD system, and so we may similarly expect the performance benefits of RR QKD at high loss. Indeed, we may interpret the entire QSS protocol as effectively a QKD protocol between Alice (dealer) and several recipient players.

Our QSS protocol runs in three stages, a Distribution stage, an Encryption stage and, finally, a Decryption stage. Distribution and Encryption stages are displayed in Fig. 4.2. The Distribution stage, Fig. 4.2a, involves distribution and measurement of quantum coherent states chosen from QPSK alphabet. At the end of Distribution, Alice will hold classical information which is correlated with both Bob and Charlie. In the Encryption stage, Fig. 4.2b, Alice will combine her classical information and use it to encode her sensitive classical secret. The encoded secret is then distributed to Bob and Charlie, who decode it during Decryption.

Distribution stage, Fig. 4.2a

STEP 1 Alice wishes to share a classical secret, σ_A. Bob forms a classical random variable $X_B = \{\phi_B\}$, where the ϕ_B are one of four complex phases independently chosen from the QPSK alphabet. Phases ϕ_B are assumed to be chosen uniformly at random, but we relax this assumption in Chapter 5. Charlie likewise forms classical random variable $X_C = \{\phi_C\}$.

2 Note that permitting Bob or Charlie to perform the heterodyne detection implicitly places trust in their heterodyning beamsplitter [88].

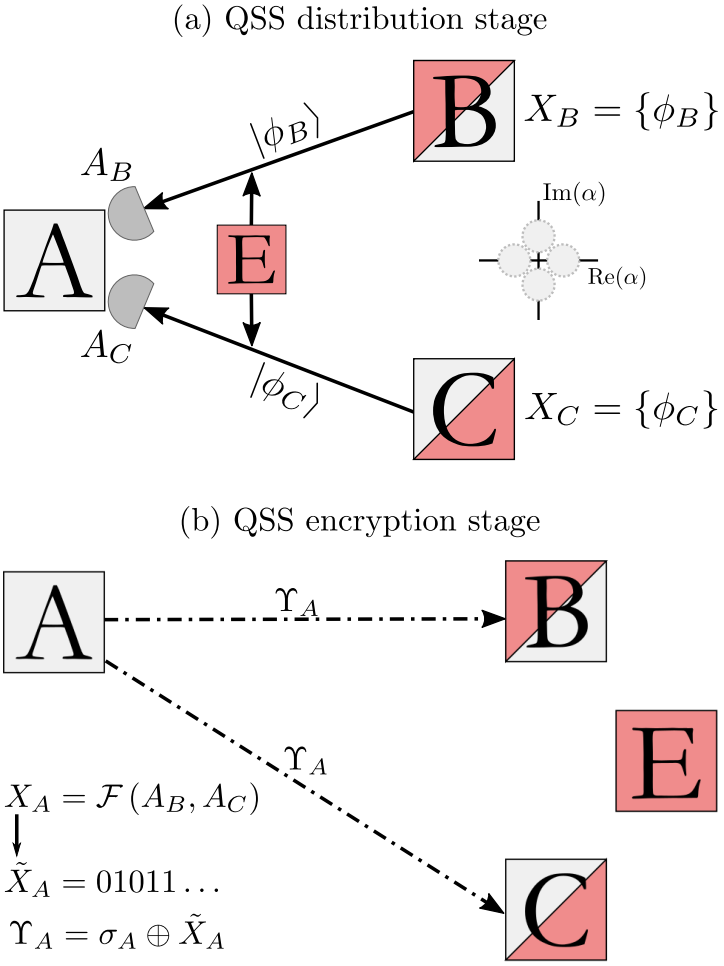


Figure 4.2: Distribution and Encryption stages of our QSS protocol. Alice (A) wishes to securely share her secret σ_A amongst potentially dishonest recipients Bob (B) and Charlie (C). (a) Distribution stage. B and C send coherent states chosen from QPSK alphabet to Alice, who heterodynes and obtains outcomes A_B, A_C. Eve eavesdrops on the quantum channels in order to gain information about Alice's outcomes A_B, A_C. (b) Encryption stage. Alice forms variable X_A using her chosen function $\mathcal{F}$ with her heterodyne measurement outcomes as input variables. She converts X_A to a binary $\tilde{X}_A$ and encrypts the secret with it to reach $\Upsilon_A = \sigma_A \oplus \tilde{X}_A$. The encrypted secret is then broadcast. Dishonest players are shown in red and honest players in gray. A combination of red and gray denotes uncertainty about the honesty of a player.

STEP 2 Bob and Charlie form sequences of coherent states based on their random variables

$$\rho\left[X_{(B,C)}\right] := \otimes\rho\left[\phi_{(B,C)}\right], \tag{4.1}$$

where $\rho\left[\phi_{(B,C)}\right]$ denotes a coherent state with phase $\phi_{(B,C)}$. These sequences of states are sent to Alice through quantum channels. Alice performs heterodyne detection on each of her received states and records her outcomes. We denote the strings of Alice's measurement outcomes as A_B, A_C, where A_B corresponds to measurement outcomes on states sent by Bob, and A_C corresponds to those on states sent by Charlie. Alice keeps the A_B and A_C separate and secret, and Bob and Charlie should retain their information X_B, X_C.

Encryption stage, Fig. 4.2b

STEP 3 Alice creates a new string of complex variables,

$$X_A = \mathcal{F}(A_B, A_C), \tag{4.2}$$

from her measurement outcomes. The function $\mathcal{F}$ is freely chosen by Alice to optimize security. In this Thesis we will pick a simple form for $\mathcal{F}$ which allows us to make concrete predictions about protocol security, although in general $\mathcal{F}$ may be as pathological as Alice desires.

STEP 4 Alice now holds random variable X_A of complex variables, which depends on both Bob and Charlie's choices X_B, X_C. Alice maps her string of complex variables onto a binary random variable $X_A \mapsto \tilde{X}_A$ [152], and uses $\tilde{X}_A$ to encode σ_A via an XOR operation. For notational ease we shall write this combined step in terms of an encryption function Enc:

$$\Upsilon_A = \mathrm{Enc}(\sigma_A, X_A), \tag{4.3}$$

which should be known to all players at the start of the protocol. Alice distributes Υ_A to Bob and Charlie, who are unable to access σ_A since they do not yet know X_A.

Decryption stage

STEP 5 Later, when Alice desires to allow Bob and Charlie access to σ_A, she broadcasts her choice of function $\mathcal{F}$, along with enough classical information to perform a reconciliation procedure between X_A and $\mathcal{F}(X_B, X_C)$. This stage is similar to CV QKD and so we refer the reader to Refs. [95, 152]. Bob and Charlie contribute their information X_B, X_C to form $\mathcal{F}(X_B, X_C)$ and reconcile it to X_A and thus to $\tilde{X}_A$. They are now able to access Alice's original secret σ_A.

Critical to the protocol is the fact that Alice forms a secret key based on a degree of freedom which is shared between Bob and Charlie.

This forces collaboration. If either one of Bob or Charlie is dishonest, they are forced to work with an honest player and so our scheme has succeeded. In this way, our protocol is a natural extension of the protocol from Kogias *et. al.* [108], while having much simpler physical requirements (e.g. no entanglement is required).

4.2 SECURITY AGAINST EVE

The QSS protocol presented above must be secure against both the actions of an external eavesdropper and those of a dishonest Bob or Charlie who may be collaborating with Eve. We will first consider security against Eve in order to illustrate key steps from the security analysis. For this section we assume that Bob and Charlie are honest, Fig. 4.3. In Sec. 4.3 we will begin to allow for dishonesty in recipients Bob and Charlie.

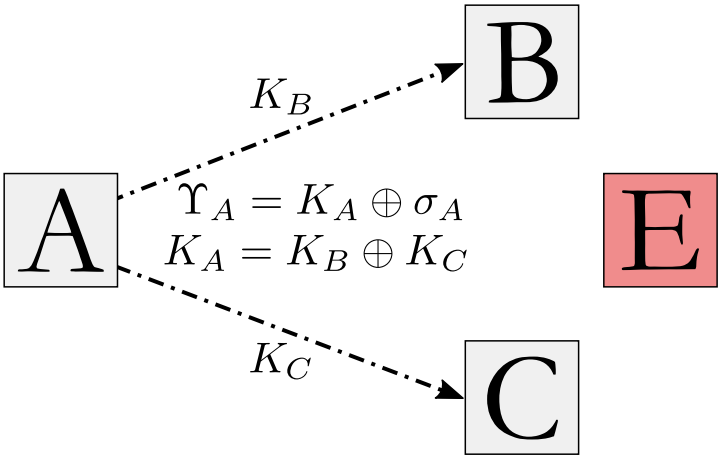


Figure 4.3: Alice distributes her secret σ_A to Bob and Charlie who are assumed honest. Dishonest Eve will try to attack the protocol and gain information about σ_A. Gray: honest. Red: dishonest. See Fig. 4.1 for further information.

The starting point for our security analysis is the following Devetak-Winter bound [153] for the asymptotic key rate under collective attack, Fig. 3.7b:

$$\kappa_{\text{Eve}} \geqslant I(X_A : X_B, X_C) - \chi(X_A : \mathbb{E}). \tag{4.4}$$

This equation describes the key rate in terms of the difference between the mutual information, I, shared between Alice and a Bob-Charlie collaboration, and the Holevo information χ between Eve's quantum system $\mathbb{E}$ and Alice. The $X_A = \mathcal{F}(A_B, A_C)$ is Alice's variable based on her heterodyne measurement outcomes.

We would like to calculate the lower bound for key rate given by Eq. 4.4 and so we will consider each term, and demonstrate how they may be calculated in our protocol.

4.2.1 *Mutual information*

Using Eq. 1.81, the mutual information I may be written as

$$I(X_A : X_B, X_C) = H(X_B, X_C) - H(X_B, X_C \mid X_A), \tag{4.5}$$

where the first term on the right hand side is the joint Shannon entropy of X_B and X_C, and the second term is the conditional Shannon entropy of X_B, X_C given X_A, Sec. 1.5.3. Intuitively, this second term encodes the uncertainty one has about which X_B, X_C were chosen, once Alice has formed X_A. The first term encodes the *a priori* entropy about Bob and Charlie's choice of sent coherent states, and is purely a function of their sending probabilities.

The joint Shannon entropy may be written

$$H(X_B, X_C) = \sum_{X_B=\phi_B, X_C=\phi_C} -P(\phi_B, \phi_C) \log P(\phi_B, \phi_C), \tag{4.6}$$

where ϕ_B, ϕ_C are individual instances of variables X_B, X_C. We take ϕ_B, ϕ_C as phase elements of the QPSK alphabet, but it is easy to generalize to larger NPSK alphabets if desired. Since ϕ_B, ϕ_C are taken to be independently and randomly chosen, each with probability[3] $1/4$, we see that the joint probability

$$P(\phi_B, \phi_C) = P(\phi_B) \times P(\phi_C) = \frac{1}{16}, \tag{4.7}$$

and so $H(X_B, X_C) = 4$.

Expanding the conditional entropy in terms of particular outcomes for X_A, via Eq. 1.80, we reach

$$H(X_B, X_C \mid X_A) = \int_{\alpha \in \mathbb{C}} d^2\alpha \, P(X_A = \alpha) \, H(X_B, X_C \mid X_A = \alpha). \tag{4.8}$$

Each term in Eq. 4.8 can be calculated once function $\mathcal{F}$ is known. The conditional entropy $H(X_B, X_C \mid X_A = \alpha)$ expands as

$$H(X_B, X_C \mid X_A = \alpha) = -\sum_{\phi_B, \phi_C} P(X_B = \phi_B, X_C = \phi_C \mid X_A = \alpha) \times \log P(X_B = b, X_C = c \mid X_A = \alpha) \tag{4.9}$$

and so all that remains to calculate are the probabilities

$$P(X_A = \alpha) \quad \text{and} \tag{4.10}$$

$$P(X_B = \phi_B, X_C = \phi_C \mid X_A = \alpha) \tag{4.11}$$

once $\mathcal{F}$ is known.

3 We relax this in Ch. 5.

Function $\mathcal{F}$

We have no requirement that the function $\mathcal{F}$ should be injective. This implies, for example, that $S\left(\rho_{\mathbb{E}\,|\,A_B,A_C}\right) \neq S\left(\rho_{\mathbb{E}\,|\,X_A}\right)$, i.e. the entropy of Eve's quantum state conditioned on Alice's heterodyne outcomes A_B, A_C is not equal to the entropy of Eve's quantum state conditioned on Alice's variable X_A. So, we must carefully consider the action of $\mathcal{F}$ early on in our analysis.

To be concrete, in what follows we assume that $\mathcal{F}$ is linear,

$$\mathcal{F}(x,y) := gx + hy \quad \text{with} \quad g,h \in \mathbb{R}\setminus\{0\}, \tag{4.12}$$

which will enable us to make some predictions about the performance of the protocol. Although we make no claims about the optimality of this choice of $\mathcal{F}$, Alice is free to optimize the key rate over g, h.

Expanding classical probabilities

Applying Bayes' formula Eq. 1.74 to probability Eq. 4.11 we see that

$$\begin{aligned} P(X_B = \phi_B, X_C = \phi_C \mid X_A = a) = P(X_A = a \mid X_B = \phi_B, X_C = \phi_C) \\ \times \frac{P(X_B = \phi_B, X_C = \phi_C)}{P(X_A = a)}. \end{aligned} \tag{4.13}$$

Now, we can access $P(X_A = a \mid X_B = \phi_B, X_C = \phi_C)$. We take

$$X_A = \mathcal{F}(A_B, A_C) = gA_B + hA_C, \tag{4.14}$$

as in Eq. 4.12, and so we rearrange:

$$A_C = \frac{X_A - gA_B}{h}. \tag{4.15}$$

Since our $\mathcal{F}$ is not injective we must average over all of the possible ways to reach a given X_A. Therefore, once X_A, g and h are fixed, the choice of A_B, A_C reduces to a one-variable problem. So

$$\begin{aligned} P(X_A \mid X_B = \phi_B, X_C = \phi_C) = \int_{A_B \in \mathbb{C}} d^2 A_B \\ P\left(A_B, \frac{X_A - gA_B}{h} \,\middle|\, X_B = \phi_B, X_C = \phi_C\right), \end{aligned} \tag{4.16}$$

which may be calculated once we know how the channel acts on input states[4].

4 Note that an analogous expression would be reached by rearranging Eq. 4.14 as $A_B = (X_A - hA_C)/g$, but it will make no difference to the resulting quantities which we derive from Eq. 4.16

Assuming that the two channels, one from Charlie→Alice and one from Bob→Alice, are independent[5] from each other allows us to write

$$P(A_B, A_C \mid X_b = \phi_B, X_C = \phi_C) = P(A_B \mid X_B = \phi_B) \times P(A_C \mid X_C = \phi_C) \tag{4.17}$$

for the probabilities that Alice's heterodyne measurement outcomes are A_B, A_C, given that coherent states with phases ϕ_B, ϕ_C are sent.

Let us assume for now that each channel is noiseless but lossy. The probability that Alice measures a particular heterodyne outcome $\alpha = q_{out} + ip_{out}$ when a coherent state of complex amplitude β is sent through a lossy channel, transmission T, is

$$P(\alpha \mid \beta, T) = \frac{1}{\pi} \exp\left(-\left|\alpha - \sqrt{T}\beta\right|^2\right), \tag{4.18}$$

which we have used previously in Ch. 3. The required changes to include thermal noise of the channel can be readily made, c.f. Appendix. A.

The integral in Eq. 4.16 may now be calculated analytically to reach

$$P(X_A \mid X_B = \phi_B, X_C = \phi_C) = \frac{1}{\pi}\frac{1}{g^2 + h^2} \exp\left(-\frac{\left[\phi_B^R g\sqrt{T_B} + \phi_C^R h\sqrt{T_C} - X_A^R\right]^2}{g^2 + h^2}\right) \times \exp\left(-\frac{\left[\phi_B^I g\sqrt{T_B} + \phi_C^I h\sqrt{T_C} - X_A^I\right]^2}{g^2 + h^2}\right). \tag{4.19}$$

Here ϕ_B, ϕ_C are Bob and Charlie's coherent state amplitudes, X_A is Alice's final variable after applying $\mathcal{F}$ (Eq. 4.12) to her heterodyne outcomes, T_B, T_C are the transmissions of the Bob→Alice channel and Charlie→Alice channel, respectively, and a superscript R (I) denotes the real (imaginary) part of the corresponding quantity. The probability $P(X_A = \alpha)$ Eq. 4.10 may now be found by summing over Eq. 4.19:

$$P(X_A) = \sum_{\phi_B, \phi_C} P(X_A \mid X_B = \phi_B, X_C = \phi_C). \tag{4.20}$$

Finally, the mutual information Eq. 4.5 may be calculated. We perform the integration over X_A in Eq. 4.8 numerically and display the mutual information I in Fig. 4.6.

4.2.2 *Holevo information*

We will now detail how the Holevo information term, χ in Eq. 4.4, may be calculated. In doing so we will point to areas where future work might strengthen the security analysis to consider wider classes of attack. This should illuminate the contexts to which our security

5 We shall see later what this means for their combined action on an input quantum state

proof may be applied. For illustrative convenience, in this section we consider a dishonest Eve performing attack BS0, as detailed above in Sec. 3.6.1, though the analysis follows readily for the other attacks described in Sec. 3.6.

Bob and Charlie prepare a state from the QPSK alphabet, and each state is chosen randomly and with equal probability. Before the channel, Bob and Charlie hold the joint state

$$\rho_{\text{before}} = \rho_B \otimes \rho_C \tag{4.21}$$

with

$$\rho_B = \frac{1}{4}\sum_{k=0}^{3} |\beta_k\rangle\langle\beta_k|_B \quad \text{and} \quad \rho_C = \frac{1}{4}\sum_{k'=0}^{3} |\gamma_{k'}\rangle\langle\gamma_{k'}|_C \tag{4.22}$$

where β, γ are the amplitudes of Bob's and Charlie's coherent state alphabets.

We assume that the channel acts separately on each mode, and that modes ρ_B, ρ_C undergo independent evolution. In other words, we assume that the channel has the following structure:

$$\Phi[\rho] = \Phi_B[\rho] \otimes \Phi_C[\rho] \tag{4.23}$$

where $\Phi_{B,C}$ denote the lossy channels described by attack BS0, Sec. 3.6.1, and the subscript B, C denotes which mode of ρ_{before} each channel acts on. The total channel Φ preserves the tensor-product structure of the input state.

Physically Φ corresponds to the case where Eve performs separate beamsplitter attacks on each channel and retains two output modes $\mathbb{E}_{B,C}$, Fig. 4.4.

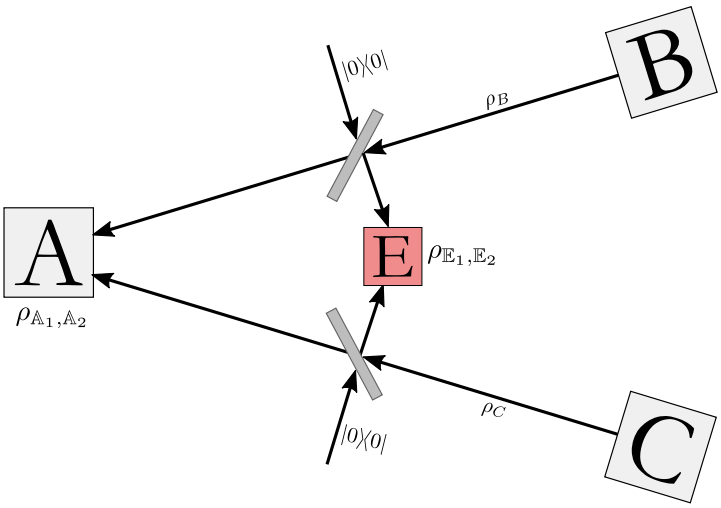


Figure 4.4: We model the channel Φ as two independent beamsplitter attacks of type BS0, Sec. 3.6.1. This preserves the tensor-product structure of ρ_{before}.

The total state after the channel becomes

$$\rho_{\text{after}} = \rho_{\mathbb{A}_B,\mathbb{E}_B} \otimes \rho_{\mathbb{A}_C,\mathbb{E}_C}, \tag{4.24}$$

with $\mathbb{A}_{B,C}$ denoting Alice's two modes and where

$$\rho_{\mathbb{A}_B,\mathbb{E}_B} = \frac{1}{4}\sum_{k=0}^{3} \left|\sqrt{T_B}\beta_k\right\rangle\!\left\langle\sqrt{T_B}\beta_k\right|_{\mathbb{A}_B} \otimes \left|\sqrt{1-T_B}\beta_k\right\rangle\!\left\langle\sqrt{1-T_B}\beta_k\right|_{\mathbb{E}_B}, \tag{4.25}$$

and similarly for $\rho_{\mathbb{A}_C,\mathbb{E}_C}$. Now, Alice heterodynes and measures A_B from $\rho_{\mathbb{A}_B,\mathbb{E}_B}$ and A_C from $\rho_{\mathbb{A}_C,\mathbb{E}_C}$. Eve's total state conditioned on these outcomes becomes

$$\rho_{\mathbb{E}\,|\,A_B,A_C} = \rho_{\mathbb{E}_B\,|\,A_B} \otimes \rho_{\mathbb{E}_C\,|\,A_C}, \tag{4.26}$$

with

$$\rho_{\mathbb{E}_B\,|\,A_B} = \frac{1}{4\pi}\sum_{k=0}^{3} P_B\left(A_B \mid \beta_k, T_B\right)\left|\sqrt{1-T_B}\beta_k\right\rangle\!\left\langle\sqrt{1-T_B}\beta_k\right|_{\mathbb{E}_B}, \tag{4.27}$$

and similarly for $\rho_{\mathbb{E}_C\,|\,A_C}$. The probability $P_B\left(A_B \mid \beta_k, T_B\right)$ is calculated analogously to Eq. 4.18, and similarly for A_C.

To proceed, we take $X_A = gA_B + hA_C$ as usual, with g, h fixed, and write $A_C = \left(X_A - gA_B\right)/h$. Therefore the state $\rho_{\mathbb{E}\,|\,A_B,A_C}$, Eq. 4.26, becomes

$$\begin{aligned}\rho_{\mathbb{E}\,|\,X_A,A_B} = \frac{1}{16\pi^2}\sum_{k,k'=0}^{3} P_B\left(A_B \mid \beta_k, T_B\right) P_C\left(\frac{X_A - gA_B}{h}\,\middle|\,\gamma_{k'}, T_C\right) \\ \times \left|\sqrt{1-T_B}\beta_k\right\rangle\!\left\langle\sqrt{1-T_B}\beta_k\right|_{\mathbb{E}_B} \otimes \left|\sqrt{1-T_C}\gamma_{k'}\right\rangle\!\left\langle\sqrt{1-T_C}\gamma_{k'}\right|_{\mathbb{E}_C}.\end{aligned} \tag{4.28}$$

Once again, since Alice's function $\mathcal{F}$ is in general not injective, we must mix over outcomes A_B, A_C in order to find Eve's state $\rho_{\mathbb{E}\,|\,X_A}$:

$$\rho_{\mathbb{E}\,|\,X_A} = \int_{A_B\in\mathbb{C}} d^2A_B\; P\left(A_B\right)\rho_{\mathbb{E}\,|\,X_A,A_B}. \tag{4.29}$$

Mixing over X_A we finally reach

$$\rho_{\mathbb{E}} = \int_{X_A\in\mathbb{C}} d^2X_A\; P\left(X_A\right)\rho_{\mathbb{E}\,|\,X_A}. \tag{4.30}$$

We may identity Eq. 4.29 as Eve's *a prosteriori* state and Eq. 4.30 as Eve's *a priori* state and so Eve's Holevo information is given by the usual formula Eq. 1.87:

$$\chi = S\left(\rho_{\mathbb{E}}\right) - \int_{X_A\in\mathbb{C}} d^2X_A\; P\left(X_A\right) S\left(\rho_{\mathbb{E}\,|\,X_A}\right). \tag{4.31}$$

We note that we can no longer simplify the second term in Eq. 4.31, like we did in Sec. 3.6, for example, since in general the entropy of each state depends on X_A. We perform the integration in Eq. 4.31 numerically, and display the output Holevo information in Fig. 4.7.

4.3 SECURITY AGAINST A DISHONEST PLAYER

Of course, if Alice only had to guard against an external Eve, and both Bob and Charlie could be assumed honest, then the QSS task becomes much easier. She could, for example, simply send the same information to each recipient. Or send her secret just to the recipient she is interested in, with no need to "split" it or share it. The task of secret sharing, however, assumes dishonest recipients. In this section we will adapt the analysis of Sec. 4.2 to this case. Our method will be to take the final key rate as the minimum of key rates under dishonest Bob and dishonest Charlie, which therefore secures against both possibilities [108, 118].

4.3.1 *Dishonest Bob*

Let us translate the analysis from Sec. 4.2 to the case where either Bob or Charlie is dishonest, but Alice does not know which one, Fig. 4.1. Including a dishonest recipient in the above security proof requires us to re-calculate several quantities. For concreteness we will first assume that Bob is dishonest and Charlie is honest, Fig. 4.5, and we will allow Bob to collaborate with Eve. Later we will discuss how to account for the fact that we do not know *which* player is dishonest.

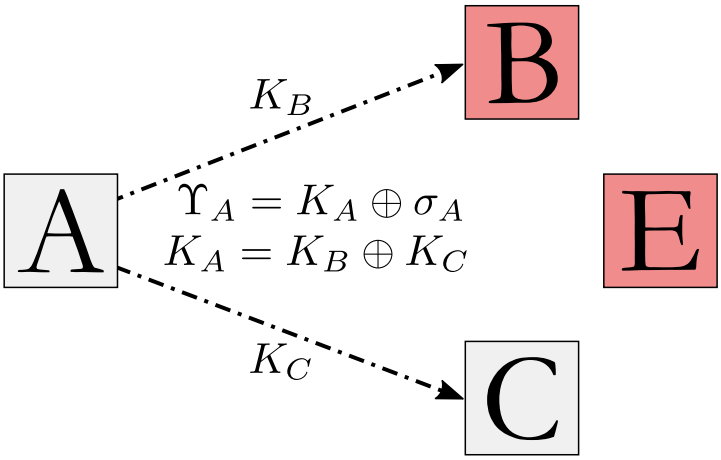


Figure 4.5: A dishonest Bob gains an advantage since he knows which coherent state he chose to send to Alice. He may additionally choose to collaborate with Eve in order to gain information about Alice's measurement on Charlie's state. c.f. Fig. 4.1.

The main effect of permitting dishonesty from Bob is that he knows precisely which coherent states he sent to Alice. This reduces his uncertainty about Alice's variable X_A. Bob might also wait and see which coherent state was sent by Charlie before choosing his own, in order to preference a certain outcome X_A, but the advantage that this might give may be reduced by assuming that $\mathcal{F}$, g and h are not disclosed by Alice at the start of the protocol. We will discuss this further in Sec. 4.5. We will additionally assume that Bob sends states only from the QPSK alphabet, though in principle this could be relaxed in future work.

Since Bob knows which coherent state he sent, we must re-calculate several expressions from Sec. 4.2. The main change is that we no longer mix over Bob's alphabet. The quantities which this influences are $P(X_A = a)$ and $H(X_B, X_C \mid X_A = a)$, which now become

$$P(X_A = a) = \sum_c P(X_A \mid X_b = b, X_C = c), \tag{4.32}$$

and

$$H(X_B, X_C \mid X_A = a) = -\sum_c P(X_B = b, X_C = c \mid X_A = a) \times \log P(X_B = b, X_C = c \mid X_A = a). \tag{4.33}$$

The mutual information may now be calculated as in the previous section.

The Holevo information is also calculated analogously to the previous section, the key change being that Eve's state conditioned on X_A, A_B, Eq. 4.28, is now given by

$$\rho_{\mathbb{E} \mid X_A, A_B} = \frac{1}{4\pi^2} \sum_{k'=0}^{3} P_B(A_B \mid \beta_k, T_B) P_C\left(\frac{X_A - gA_B}{h} \,\middle|\, \gamma_{k'}, T_C\right) \left|\sqrt{1-T_B}\beta_k\right\rangle\!\left\langle\sqrt{1-T_B}\beta_k\right|_{\mathbb{E}_B} \otimes \left|\sqrt{1-T_C}\gamma_{k'}\right\rangle\!\left\langle\sqrt{1-T_C}\gamma_{k'}\right|_{\mathbb{E}_C} \tag{4.34}$$

and the *a posteriori* and *a priori* states calculated by integrating Eq. 4.34 identically to Eqs. 4.29, 4.30.

Since we no longer mix over Bob's coherent state β_k, the mutual information I and Holevo information χ have themselves become functions of β_k. In this chapter we assume that each state in the QPSK alphabet is equally likely and has equal magnitude and so both I and χ will be identical for each of Bob's alphabet states. We will relax this in Chapter 5.

The final key rate is now

$$\kappa_{\text{Eve, Bob}} = I(X_A : X_B, X_C) - \chi(X_A : \mathbb{E}|\mathbb{B}) \tag{4.35}$$

with mutual information and Holevo information terms calculated as described above. In using Eq. 4.35 we are treating Bob as a dishonest eavesdropper who collaborates with Eve. This key rate formula thus provides security against general collective eavesdropping strategies, provided the mutual information and Holevo information terms can be bounded. In this Chapter we will allow the same range of attacks as in Ch. 3. We discuss additional attack strategies unique to our QSS protocol in Sec. 4.5.

4.3.2 *Dishonest Bob or Dishonest Charlie*

If Alice is certain that Bob is the dishonest player then she has no need for a secret sharing scheme. Equivalently, she can set $g = 0$ in her function $\mathcal{F}$. If she is correct about Bob's dishonestly, then she has successfully prevented him from gaining any information about her secret. However, if Alice turns out to be wrong and it is Charlie who is the dishonest player then she has accidentally given Charlie the secret! It is precisely this uncertainty about which player is dishonest which makes a QSS scheme necessary.

In order to take into account this uncertainty over which player is dishonest, Fig. 4.1, we proceed as in the recent QSS works Refs. [108, 118] and calculate the minimum over all possible dishonest configurations. That is, we take

$$\kappa \geqslant \min\left\{\kappa_{\text{Eve, Bob}}, \kappa_{\text{Eve, Charlie}}\right\} \tag{4.36}$$

where $\kappa_{\text{Eve, Charlie}}$ is calculated analogously to Eq. 4.35. This expression makes explicit the close links between QSS and QKD, as explored further in Refs. [108, 118]. The work by Grice [118] generalizes this expression to N players, and directly comments that their setup can perform both QSS and 2-party QKD with key rate calculated analogously.

4.4 PROTOCOL PERFORMANCE

We plot the mutual information (Eq. 4.5) in Fig. 4.6, taking honest recipients in (a) and dishonest recipients in (b). Coherent state amplitude α and channel transmission T are varied. We here take Bob and Charlie's states as having equal amplitudes and channel transmissions, but in principle they can vary independently from one another. Unless $T = 0$, the mutual information between Alice and Bob-Charlie always increases with α as the states at Alice become increasingly distinguishable. The mutual information with honest recipients is bounded by 4, while in the case of dishonest recipients it is bounded by 2.

The Holevo information χ under identical conditions to Fig. 4.6 is plotted in Fig. 4.7. We see that there is a clear maximum of χ at $T = 0.5$, which is when dishonest parties have maximum fidelity to Alice's

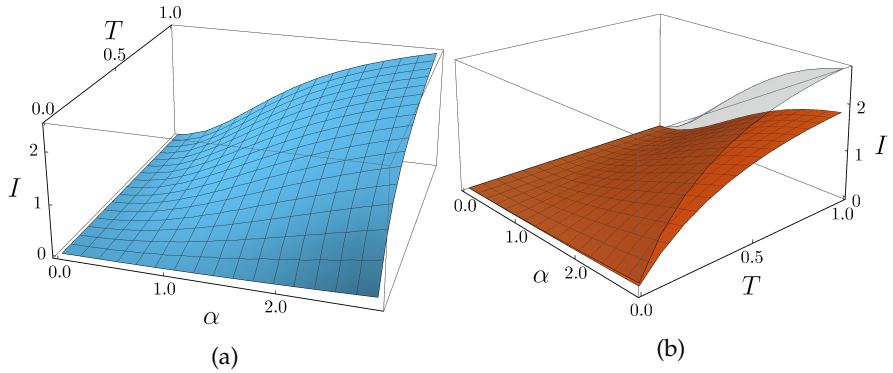


Figure 4.6: Mutual information Eq. 4.5 as it varies with coherent state amplitude α and channel transmission T. (a) Honest recipients. (b) Orange: dishonest recipients. Blue, clear: honest recipients, same surface as (a). In both figures we have taken linear $\mathcal{F}$, with parameters $g = h = 0.5$.

received state. Our QSS protocol leverages the power of cryptographic protocols constructed in the reverse-reconciliation regime. As $T < 0.5$, even though Eve receives a greater share of the sent state than Alice[6], the overlap between Eve's and Alice's states begins to decrease as T decreases, meaning χ also decreases.

Curiously, Fig. 4.7b demonstrates a reduction in the Holevo information when Bob or Charlie is dishonest. Since Holevo information is directly related to the efficacy of an attack, this might suggest that dishonesty gives no advantage, and even makes things worse. We note however that the mutual information is also reduced in this case, and a consideration of the key rate in Fig. 4.8 demonstrates that such dishonesty of Bob or Charlie does indeed yield a marked reduction in the key rate κ.

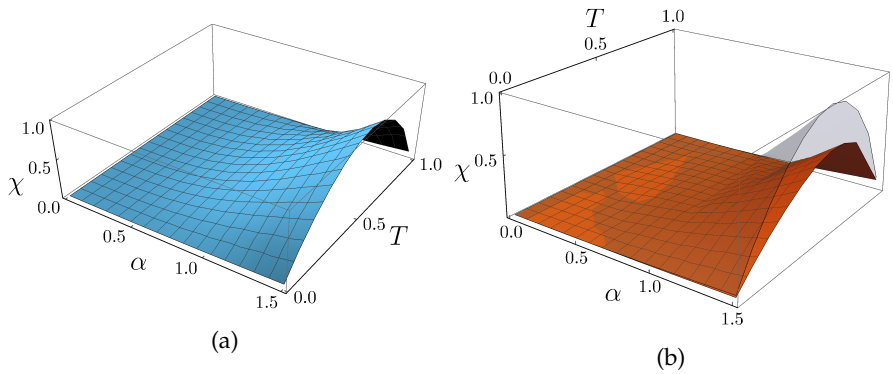


Figure 4.7: Holevo information Eq. 4.31 as it varies with coherent state amplitude α and channel transmission T. (a) Honest recipients. (b) Orange: dishonest recipients. Blue, clear: honest recipients, same surface as (a). In both figures we have taken linear $\mathcal{F}$, with parameters $g = h = 0.5$.

6 This would be fatal for direct-reconciliation cryptography.

The key rate κ is plotted in Fig. 4.8. Comparing Fig. 4.8(a) and (b), we see that in all cases the presence of dishonesty in Bob or Charlie causes a reduction in the obtained key rate. Each figure takes Bob and Charlie to have the same coherent state amplitude α and channel transmission T. At the loss levels considered here, $\alpha = 0.8$ yields larger κ, but for larger losses (not shown) $\alpha = 0.5$ performs better. Indeed, the best α reduces as the loss level increases. We found a similar result for our QDS protocol, Fig. 3.18.

We see that a symmetric choice $g = h = 0.5$ is clearly optimal when both Bob and Charlie are honest (green and blue lines in (a) outperform red and orange), while the best choice of g, h in (b) depends on which player is assumed dishonest. For example, assuming that Bob is dishonest gives much larger κ for $g = 0.2$, $h = 0.8$ (orange in (b)) than for $g = h = 0.5$ (blue in (b)). By lowering g we are effectively reducing the amount of information which Bob has access to, and his knowledge of which state was sent matters less and less. Conversely, the choice $g = 0.2$, $h = 0.8$ causes a large reduction in κ when Charlie is dishonest. Since the final key rate κ is a minimum over these two key rates, Eq. 4.36, we see that when either party can be dishonest the optimal choice should be the symmetric choice $g = h$. It would however be interesting to see how optimal parameter choices vary with the number of players and potential adversarial collaborations.

Allowing for Bob and Charlie to experience different loss levels, or use different input alphabet amplitudes, we plot the resultant key rates in Fig. 4.9. In (a) we let $g = 0.2$, $h = 0.8$ (blue, green) and $g = 0.3$, $h = 0.7$ (orange, red) and vary the channel loss of Bob, while Charlie's is fixed at -1.5 dB. Bob is assumed dishonest. We see that the loss variation in the player who contributes little to the key, in this case Bob as $g < h$, leads to only small changes in the resultant κ. However, when Charlie's loss varies and Bob's remains constant, for equivalent parameters, we see (b) large variations in κ. Black lines denote $g = h = 0.5$ with only Bob's loss (a) or Charlie's loss (b) varying. Gray, dashed lines denote $g = h = 0.5$ when Bob and Charlie's losses vary equally. We see from this Figure 4.9 that when $g \neq h$, the channel parameters of the player who contributes most to the key (Bob if $g < h$ or Charlie if $h < g$) make the most significant impact. Interestingly, for the symmetric case $g = h$, which we have already noted is the optimal choice, it is the largest amount of loss which controls κ. Little is to be gained by having one high quality channel if the other one is poor.

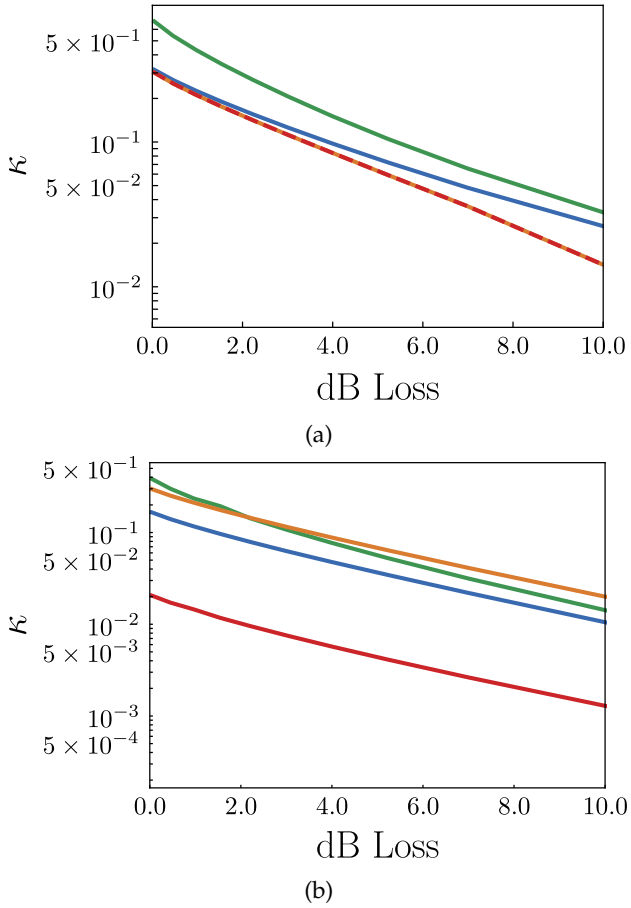


Figure 4.8: QSS key rates varying with dB loss. Bob and Charlie experience the same loss, and begin with the same input alphabet amplitude. (a) Honest Bob and Charlie. (b) Dishonest Bob and Charlie. (a) and (b) - blue: $\alpha = 0.5$, $g = h = 0.5$; green: $\alpha = 0.8$, $g = h = 0.5$; orange: $\alpha = 0.5$; $g = 0.2$, $h = 0.8$ Bob dishonest; red: $\alpha = 0.5$; $g = 0.2$, $h = 0.8$ Charlie dishonest.

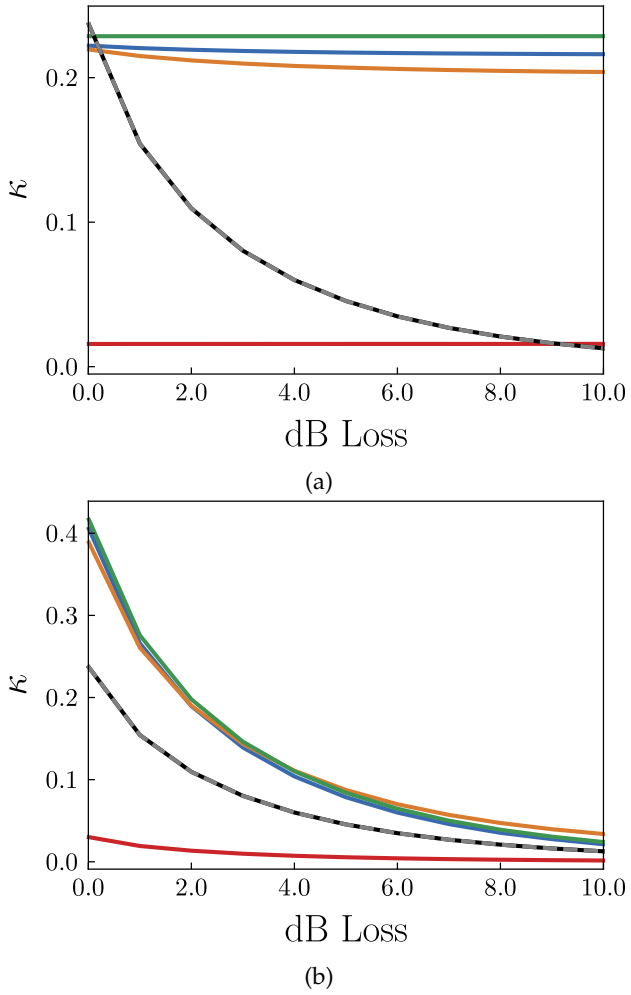


Figure 4.9: QSS key rates varying dB loss asymmetrically. (a) Bob's loss varies, while Charlie's remains at -1.5 dB. (b) Charlie's loss varies, while Bob's remains at $T = 0.7$. (a)-(b): We have taken $g = 0.2, h = 0.8$ (blue, green); $g = 0.3, h = 0.7$ (orange, red). Blue and orange lines: both Bob and Charlie are honest. Green and red lines: Bob is dishonest. Varying the loss of the dishonest player (a) results in negligible variation of κ, while varying loss of honest player (b) results in large variation. Black: $g = h = 0.5$ varying loss of honest player. Gray, dashed: $g = h = 0.5$ varying loss of honest and dishonest player equally.

4.5 OUTLOOK

We have introduced and demonstrated a fully continuous-variables protocol which performs the QSS task. Our protocol relies only on distribution of QPSK coherent states and phase measurement via heterodyne detection. Our protocol is proven secure against collective attacks for which the Holevo information χ may be bounded, and we have explicitly demonstrated how this may be estimated under beamsplitter attacks (Sec. 3.6). In principle our analysis may readily include entangling cloner attacks, as we did in Ch. 3 for the QDS protocol, but as we shall see later in Ch. 5 the QSS protocol is not very robust to channel excess noise. This might have been expected, as QKD protocols with similar resources [137, 146] allow only very small amounts of noise in the reverse-reconciliation configuration before a secure key cannot be formed.

We will revisit this QSS protocol in Chapter 5, where we shall investigate its experimental implementation alongside other cryptographic schemes with identical hardware requirements, and we shall see in particular that this QSS protocol requires fewer quantum resources than pairwise-QKD followed by a classical unconditionally secure secret sharing scheme, Sec. 5.6.3.

The classical post-processing of the above protocol is inherently very similar to Ref. [108], in which a secret key is generated between Alice and a shared Bob-Charlie degree of freedom via incompatible homodyne measurements on a tripartite entangled state. We have several reasons to expect that our protocol will be secure against a more restricted set of attacks, but over a wider range of channel parameters. Firstly unlike Ref. [108] which relies in generation and distribution of large multipartite entangled states, our scheme has more modest quantum requirements which are easier to generate and manipulate, and which are much more robust to channel loss and channel noise than a large entangled state. Quantum cryptography (QKD, QDS) using continuous-variables typically operates over metropolitan distances of tens of kilometers, and so we might reasonably expect similar performance of our QSS protocol. Performance of our protocol over a realistic fiber channel is analysed in Chapter 5. Secondly, the protocol from Ref. [108] takes a form analogous to direct-reconciliation (DR) QKD, while ours is analogous to reverse-reconciliation (RR) QKD. RR QKD is known [95, 99, 138] to be much more resilient to loss and noise than DR QKD without modifications [140].

Ref. [108] has potentially dishonest players Bob and Charlie performing homodyne measurements on incompatible observables (i.e. switching between q and p quadratures). No assumptions are made about the measurement devices used and they are each treated as a "black-box". Security there comes inherently because of a Heisenberg-type relation between incompatible observables, and the security proof

relies on an Entropic Uncertainty Relation which has had success in many parts of quantum cryptography [135, 154]. However, since we desire to use heterodyne detection we are forced to adopt a different approach and explicitly model the states' evolution and measurement during the protocol. We note that this matches the current state-of-the-art of QPSK-based QKD [137], but should be improved in future work. One approach might be to use an Entropic Uncertainty Relation designed with heterodyne detection in mind [155, 156], but a preliminary analysis has been pessimistic.

We have assumed that a dishonest Bob or Charlie still sends a state from the QPSK alphabet. It is yet unclear whether they could gain an advantage by sending something exotic and potentially highly entangled, perhaps in order to force Alice to reach a certain key X_A. This should be explored and potentially included in future work. One solution might be for Alice to wait until after Distribution to declare her choice of $\mathcal{F}$ and its parameters, which in the worst-case scenario should lead to a final security bound based on assumptions about the power of existing quantum memory devices. This approach was used in recent proofs for security of quantum oblivious transfer [124, 154]. We anticipate also that applying methods from quantum bit commitment [124] might prove fruitful here, since bit commitment also allows for possible dishonest distribution of the quantum state from an untrusted player. Finally, we note that our assumption that the channel between Alice and Bob-Charlie takes a tensor-product structure, Eq. 4.23, Fig. 4.4, should be relaxed.

Finally, we note that the QSS protocol presented in this section, in which both Bob and Charlie send coherent states to a central Alice, is intrinsically similar in its setup to twin-field QKD systems which have recently been proposed in order to overcome the rate-loss bound for repeaterless QKD [79, 80], see Sec. 2.2.10. In the TF-QKD protocol discussed in Ref. [81], for example, Alice and Bob independently and randomly pick states from the QPSK alphabet and send them to Eve through their separate quantum channels. Eve receives the states, interferes them on a balanced beamsplitter, and then performs a single-photon detection on each of her two output ports Fig. 2.6. By Eve's declaration of which of her detectors clicked, Alice and Bob are able to distill a key. Since Eve is given full control over the central node, TF-QKD is also inherently MDI.

All of this raises the possibility of a future TF-QSS protocol. The close similarities between the systems are remarkable, and should be explored in detail in future work. In the first instance we will replace Alice's two heterodyne detectors with an interference measurement and single-photon detection, which gives her information about the relative phase of Bob and Charlie's distributed states. This will open up several security concerns which should be addressed, since the trust assumptions for the QSS presented here differ significantly from

TF-QKD. As with all QKD protocols, TF-QKD assumes that Alice and Bob, the senders of the quantum states, are honest. Eve, the receiver of the states, is dishonest. Our QSS however has an honest reciever, Alice, and at most one potentially dishonest sender, Bob and Charlie. We must carefully consider the advantage which a dishonest sender gains in TF-QSS. A initial naïve approach to the TF-QSS seems entirely plausible, since the interference at Alice's beamsplitter forces Bob and Charlie to cooperate to predict which of Alice's detectors clicked, though we must be careful to fully explore the potential for trojan horse attack [114, 115].

Despite these theoretical security and design challenges, this modified TF-QSS protocol will have the same hardware requirements as the TF-QKD proposed in Ref. [81], and similar hardware requirements to those proposed elsewhere [80, 82, 83], thereby opening up the possibility for the same physical system to perform multiple quantum cryptographic protocols. This is a theme which we will discuss at length in the next Chapter for the cryptographic protocols proposed in this Thesis.

5

AGILE QUANTUM CRYPTOGRAPHY

In this chapter we introduce and investigate a framework within which quantum communications protocols may be combined and implemented. In particular, we examine two "quantum agile" systems (Sec. 5.3, 5.4) which are capable of performing several cryptographic tasks with security against a quantum adversary. Crucially the tasks differ only at the level of classical postprocessing, and so the choice of protocol to implement is reduced to just a firmware upgrade. The agile framework allows us to unite the QDS protocol (Ch. 3) and the QSS protocol (Ch. 4), which we have examined already in this Thesis, in a common hardware platform. We additionally introduce a new QDS protocol, and integrate an existing QKD protocol from the literature into our system.

These protocols are then investigated in an experiment (Sec. 5.5) which is inherently compatible with installed telecommunications hardware. We show that a quantum distribution stage may run while remaining completely ignorant to the secure task being accomplished. In our experiment, coherent states are distributed and measured with a clock rate of 1 GHz, and so we find that our QDS protocol is the fastest known protocol over comparable distances, Sec. 5.6.3.

5.1 INTRODUCTION

We have observed over the past two chapters, and in our overview of quantum cryptography in Chapter 2, that several quantum cryptographic protocols are intimately related. We have seen close connections between QKD and QSS, and noted that QSS may be interpreted simply as QKD performed between one player (dealer) and several players (recipients of the secret). We have also remarked that the secret sharing task may be performed pseudo-classically, by first encrypting channels using QKD and then using an unconditionally secure classical secret sharing protocol, of which there are many [24, 34, 35]. It was noted in Refs. [97, 104, 107, 111] that QSS is related to quantum conferencing, and often the same hardware setup may be used to perform both tasks. And in Ref. [118] it was explicitly demonstrated that a sequential round-robin QSS protocol can also be used to perform QKD between any two players.

Moving to the QDS literature, ever since discovery of practical QDS requiring neither quantum memory, entanglement, nor an optical multiport it has been accepted that there are close links between QDS and QKD. Reference [45] explicitly builds a QDS protocol to use QKD

hardware, while Ref. [65] realises a setup which can, with minimal hardware modification, perform either QDS or QKD with additional MDI[1] capabilities. References [54, 56, 65, 66, 69] remark that QDS differs from QKD only in the classical postprocessing, and Ref. [157] designs a quantum secret sharing scheme using the same principles as differential-phase-shift based QKD [158]. Indeed, many QDS papers even build their security proofs on techniques designed first for QKD [108, 109, 118, 157, 159].

It should be clear, then, that the field of quantum cryptography is far broader and more interesting than just QKD [124]. As the field moves closer towards practical implementation of diverse quantum cryptographic protocols, one must consider not only the unconditional security of the underlying protocol but also its ease of implementation. As protocols are designed with minimal and often overlapping hardware requirements we may ask the following questions:

Q1: *given a particular hardware setup, which quantum protocols can I perform?*

Or, desiring a large-scale quantum cryptographic network:

Q2: *given a deployed network architecture, which quantum protocols can I perform with minimal disruption?*

Both of these questions will have deep impacts on the success of a future large-scale quantum network.

We have already even seen several quantum routes to perform the same task. For example, by utilizing prior QKD between all players it is possible to perform digital signatures [45, 77] or secret sharing [24, 34, 35] using unconditionally secure classical algorithms, and indeed this may sometimes be preferable to protocols requiring large entangled states [39, 97]. Alternatively, in a distributed quantum computing setup which can easily generate and distribute entanglement, protocols such as Refs. [108, 122] may be advantageous if they take advantage of already accessible hardware, for example as an additional security layer for a distributed quantum computation. The comparison between the many different routes to the same task is rarely straightforward and is often more involved than a simple comparison of key rates.

In addition to considering the performance of unconditionally secure protocols, the questions Q1 and Q2 push us to consider practical quantum cryptographic protocols which may perform well but not yet offer full unconditional security against an infinitely powerful eavesdropper. This may particularly be the case as new side-channel attacks are designed and discovered in existing quantum cryptographic protocols. Indeed, throughout the history of *classical* cryptography,

1 Measurement Device Independent, Ch. 2.

development of new cryptosystems have often occurred in response to the breaking of a system which was previously believed secure. Perhaps cynically, one could even view cryptographic history has a "cat-and-mouse" race between cryptographers and cryptanalysists.

The replacement of a newly-insecure cryptosystem is difficult, expensive and time-consuming. In response to this problem in conventional (classical) cryptography there has recently been a push towards so-called *crypographic aglity* (crypto-agility) [29, 160] with a key motivator being the threat of quantum computers.

5.1.1 *(Quantum) crypto-agility*

One of the main ideas of crypto-agility is the existence of a middleware which interacts both with the software application layer (user) and the underlying cypto-core (algorithm). This is accomplished in Ref. [160], for example, by ensuring that written code is kept as abstract as possible without hard-coding the secure protocols which are used. This allows for flexible switching between underlying algorithms, and keeps the top-level code agnostic as to which secure algorithms are being used. When the security of the underlying algorithm is weakened it becomes easy to simply replace the algorithm with a new or modified one, without changes to the rest of the architecture. Failures to allow a system to respond to new cryptographic threats like this can be at best embarrassing, and at worst costly or life-threatening [161, 162]. The key idea of classical crypto-agility is depicted in Fig. 5.1a.

The framework of crypto-agility seems ideal to help us answer Q1 and Q2. It is natural to separate the application layer (the task to be performed) from the underlying algorithm (which we may call a "quantum crypto-core"). One might even envisage a future library of quantum security software, in which one can select between the appropriate underlying algorithm based on the desired task and the available network hardware. We are then motivated to explore the quantum analogue of classical crypto-agility as a step towards efficient and flexible quantum communications networks.

There are two potential ways to translate the idea of classical crypto-agility into the quantum realm. We depict them both in Figs. 5.1b, 5.1c. The first we refer to as "QKD-assisted crypto agility," which may be seen as a generalization of the unconditionally secure classical secret sharing protocols, Sec. 2.3.1, and signatures protocols [45, 77] which implicitly require QKD first in order to remain secure. In this approach, a QKD system delivers fresh secure random keys which may be used for many different protocols. This is the stance taken by the ETSI QKD ISG 004 [164] and 014 [165] standardization efforts, which specify interface design between a QKD system (hardware) and the key management system (software). We expect that this QKD-

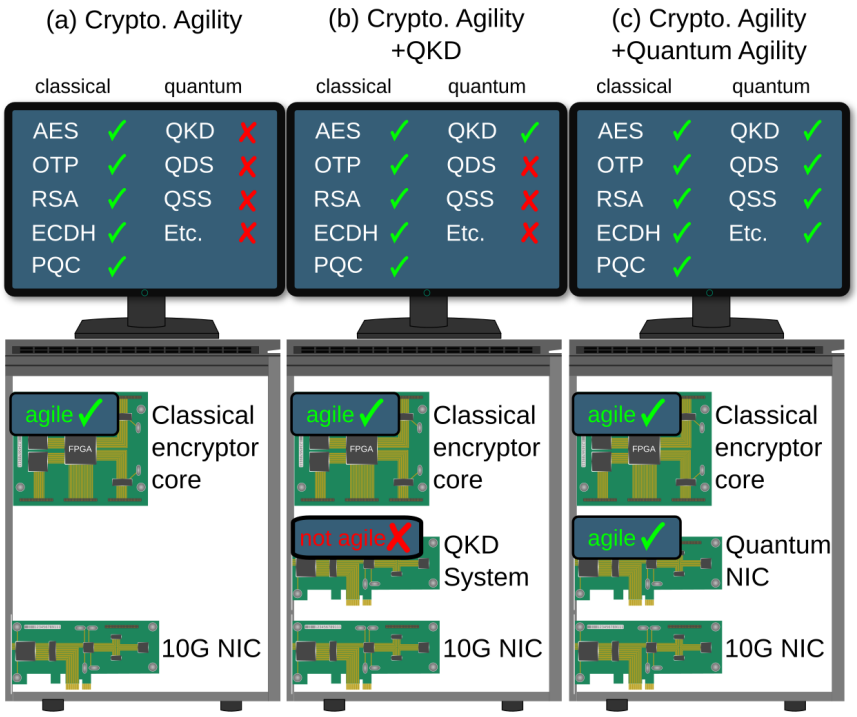


Figure 5.1: An agile cryptographic system involves a middleware which interacts between the user and the underlying crypto-core. The crypto-core (algorithm) may be readily replaced without affecting the rest of the software architecture. (a) Currently implemented classical crypto-agility. (b) QKD-assisted crypto-agility, in which several classical protocols may be run over secure channels first encrypted via a QKD link. (c) Full quantum crypto-agility which can choose interchangably between many different quantum protocols. A so-called Quantum Network Inferface Card (NIC) is used to send and receive quantum states. Classical algorithms and quantum algorithms can be replaced as necessary. The classical protocols displayed are: Advanced Encryption Standard (AES), One-time Pad (OTP), Rivest-Shamir-Adleman (RSA), Elliptic-Curve Diffie-Hellman (ECDH) and post-quantum cryptography (PQC). 10G NIC: classical Network Interface Card. *Picture credit: Stefan Richter in Ref. [163]*

assisted crypto agility will form an important cornerstone for future quantum networks.

However, as was shown in Ref. [47] in the context of QDS, it is not always optimal to perform QKD and then a classical protocol. There may be channels over which QKD is not possible, or hardware setups over which the costly reconciliation procedures are difficult. The second viewpoint of quantum crypto-agility may thus be referred to as a "fully quantum crypto agility," Fig. 5.1c. Rather than building upon an underlying fixed QKD system, such a setup should have the capability to perform multiple quantum communication protocols. This should use the so-called *quantum network interface card* in Fig. 5.1. This viewpoint explicitly recognises the fact that multiple quantum cryptographic protocols differ only in classical postprocessing while sharing a quantum stage and so a full QKD protocol may not be required. In a deployed system the ability to perform new quantum cryptographic protocols may then be reduced to a mere upgrade of classical firmware to control the postprocessing.

In Fig. 5.2 we present an example of an agile quantum communications stack which expresses the viewpoint of Fig. 5.1c. The stack provides clear separation between the user (software layer) and the physical hardware layer, and may be interpreted as analogous to recent work on compilers for quantum computers [166–168].

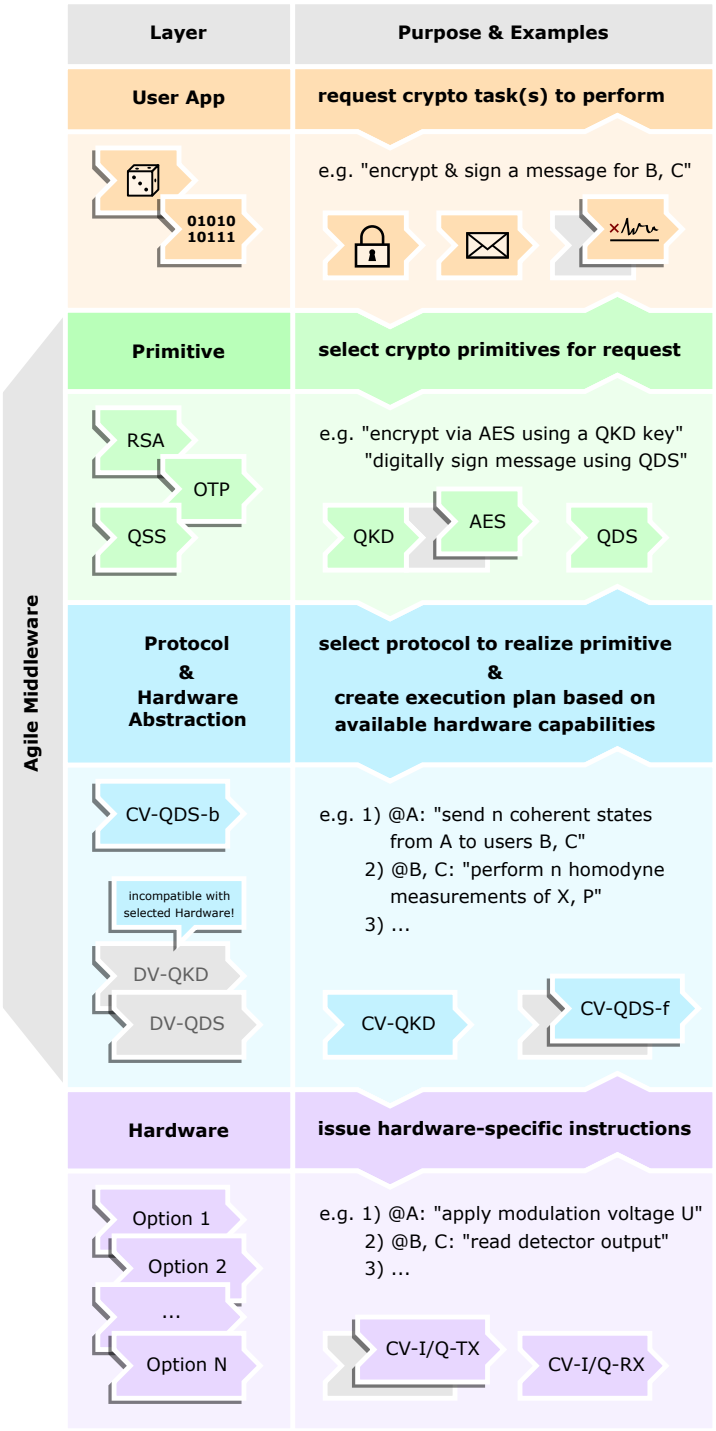


Figure 5.2: Agile quantum communications stack following the viewpoint of Fig. 5.1c. The *user app* layer allows a user to select a task they wish to perform, (e.g. message encryption, message authentication, secret sharing). The agile middleware provides a separation between the user (software) and underlying quantum crypto-system (hardware). The *primitive* layer selects the desired cryptographic primitive (e.g. QKD, QDS, QSS, RSA), and instructs the *protocol & hardware abstraction* layer to run the protocol via a library of known functions (e.g. "send coherent state," "perform heterodyne detection"). These commands are interpreted by the *hardware* layer and sent to the physical hardware setup. The agile system should be flexible and allow for switching between different tasks, different protocols and different hardware setups. *Picture credit: Stefan Richter in Ref. [163]*

5.2 CV AGILE QUANTUM SYSTEMS

To illustrate the above discussion, in this section we will introduce and analyse two quantum systems which are capable to implement multiple protocols over the same hardware setups. Within an agile system, the protocols differ only at the level of classical postprocessing. Our hardware setup is explicitly designed with question Q2 in mind. The systems therefore are fully continuous-variable, and rely on distribution of phase-modulated QPSK coherent states and their heterodyne phase detection [169]. This renders each system highly compatible with deployed telecommunications infrastructure, and paves the way to an integration between our agile systems into deployed communication links which can run with up to 100 GHz sending rate [170, 171]. In Sec. 5.5 we describe and analyse an experimental implementation of the agile systems discussed here.

We will consider the following tasks:

QDS - quantum digital signatures: allows for secure authentication of a classical message. It has been explicitly demonstrated that because of its small overhead, QDS may run over channels for which QKD is insecure [47].

QSS - quantum secret sharing: allows for secure distribution of a classical secret among a conspiracy of potentially dishonest recipients.

QKD - quantum key distribution: allows for secure key distribution of identical randomly-generated bits between players. These keys may then be used for encryption via one-time pad [7, 24].

The tasks QDS and QSS are discussed in Chapters 3, 4 above, while the reader is referred to Refs. [95, 172] for reviews of QKD. The tasks QDS and QSS are inherently multipartite, while QKD is inherently bipartite[2]. In what follows we will use quantum networks with three players to allow for multipartite tasks, while also allowing for bipartite QKD to be performed.

We therefore propose two separate agile quantum systems, one which may perform tasks QDS and QSS, and the other which may perform tasks QDS and QKD. We display these two systems in Fig. 5.3. The crucial aspect is the separation between the abstract user layer defining the roles performed in the protocols, and the hardware layer. For example, the task QDS can be performed in either of the two systems, and Alice can either choose to be the sender of the quantum states or their receiver, depending on available hardware. We denote our two systems as QDS-b-QSS-b-CV-QPSK and QDS-f-QKD-f-CV-QPSK. The labels indicate which tasks are supported; the underlying quantum states which they use (QPSK alphabet), and in which direction the quantum states are exchanged ("f" - forward, Alice sends quantum states to Bob and Charlie; or "b" - backward, Bob and Charlie

2 Though note the existence of its multipartite generalization - quantum conferencing [111, 173]

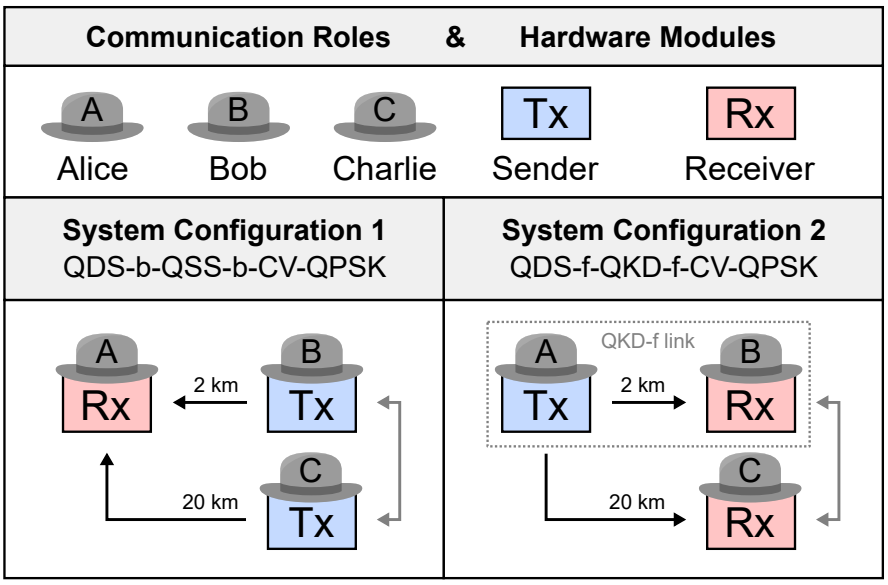


Figure 5.3: Our two agile quantum systems. Depending on the setup configuration and the chosen task, the hardware modules (Tx, Rx) perform either as Alice or as Bob/Charlie. Tx: hardware sender module. Rx: hardware receiver modules. Hardware specifications are discussed in Sec. 5.5. *Picture credit: Stefan Richter in Ref. [163]*

send quantum states to Alice). The forward- or backward- distinction can be seen as related to[3] direct- or reverse-reconcilition in QKD [95], in which quantum and classical information flow either in the same direction or in opposite directions.

5.3 AGILE SYSTEM QDS-b-QSS-b-CV-QPSK

The first agile system we consider runs in the b-configuration, Fig. 5.3, in which Bob and Charlie are the senders of quantum states while Alice is their receiver. We immediately see that the QSS protocol proposed and analysed in Chapter 4 may be inherited into this agile system, c.f. Fig. 4.2. For consistency with notation we will now refer to this QSS protocol as QSS-b, and we will analyse it further, below.

We also propose a second cryptographic protocol which fits into the system QDS-b-QSS-b-CV-QPSK, which performs the QDS task. We refer to the second protocol as QDS-b, and will analyse it below in Sec. 5.3.1. Unlike the QDS protocol analysed in Chapter 3, for QDS-b it is Bob and Charlie who are the senders of quantum states, while Alice is the recipient. Our first agile system QDS-b-QSS-b-CV-QPSK is thus able to perform both QSS and QDS tasks using identical quantum resources.

3 but not equivalent to

5.3.1 *Protocol QDS-b*

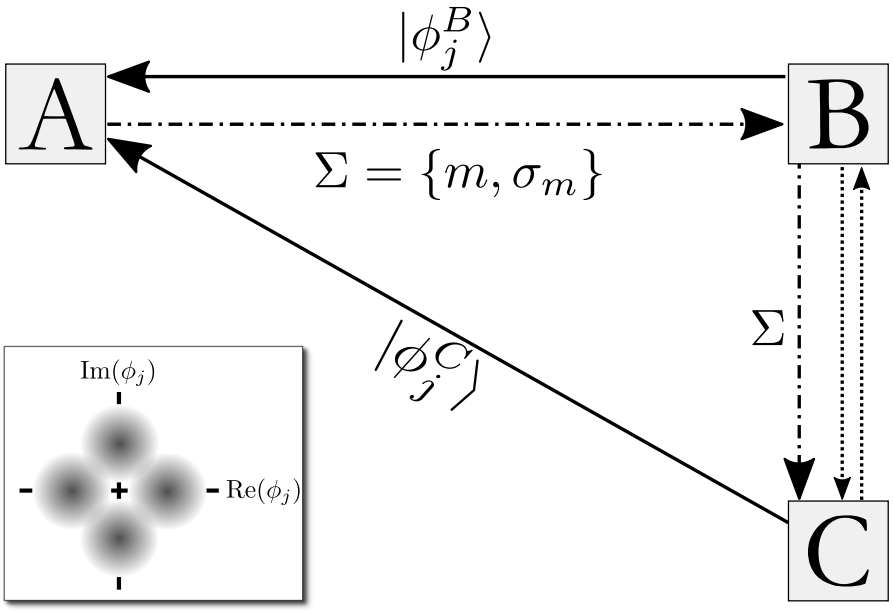


Figure 5.4: Setup of protocol QDS-b, c.f. Fig. 3.3. Alice (A) wishes to securely sign a 1 bit message m. Bob (B) and Charlie (C) distribute quantum coherent states $|\phi_j^{(B,C)}\rangle$ to Alice along insecure quantum distribution channels (solid lines) during the Distribution stage. B and C swap elements of their classical signatures elements via a securely encrypted classical channel (dotted lines). During the Messaging stage A sends Σ, containing her message m and her corresponding eliminated signature σ_m along a classical broadcast channel (dot-dashed line). Inset: QPSK alphabet.

Recall that a QDS scheme must fulfill the requirements from List 3.1 and provide security against a dishonest forger, security against repudiation, and should be robust and succeed when all parties behave honestly, Fig. 3.2. We will first outline how protocol QDS-b runs, and then prove that it fulfills each of these requirements.

The protocol QDS-b runs as follows:

Distribution stage

STEP 1. For each future message $m \in \{0, 1\}$ which Alice wishes to securely sign, Bob and Charlie create the classical strings

$$\Phi_m^{(B,C)} = \left\{ \phi_{j,m}^{(B,C)} \right\}_{j=1}^{L} \tag{5.1}$$

of length L, where the ϕ_j are complex phases chosen from the QPSK alphabet. The ϕ_j are assumed to be chosen uniformly at random.

STEP 2. Bob and Charlie form sequences of quantum coherent states corresponding to elements of $\Phi_m^{(B,C)}$ and distribute them through the

quantum channels to Alice. Bob and Charlie each keep a record of $\Phi_m^{(B,C)}$.

STEP 3. Alice performs heterodyne detection on each received state and receives phase outcomes which we denote $x_{B,C} = q_{out} + ip_{out}$, with the subscript denoting which player sent the coherent state. Since measurement is performed immediately on receipt of the state, Alice does not require quantum memory and the remainder of the protocol is entirely classical. Bob and Charlie will each send different sequences of coherent states, which allows security against forgery.

At the end of the quantum stage of the protocol, Alice possesses two classical strings, each of length L, which contain her complex phase measurements. She now forms eliminated signatures $A_{B,C}^m$ by writing down which two states from the QPSK alphabet are least-compatible with Alice's measurement. The eliminated signatures are formed identically to Fig. 3.5.

STEP 4. *symmetrization:* Bob and Charlie swap a random half of their $\Phi_m^{(B,C)}$ in order to guard against a dishonest Alice. Bob (Charlie) now possesses signature $X_B^m, \left(X_C^m\right)$ which consists of two halves of length $L/2$, one of which was generated by Bob (Charlie), and one of which was received during the swapping. We denote the first half by $Y_m^{(B)}$ and the second half by $Z_m^{(B)}$ in analogy with Chapter 3, and similarly for Charlie. Contrary to Chapter 3, strings $Y_m^{(B)}$ and $Z_m^{(B)}$ contain phase information, while $A_{B,C}^m$ are eliminated signatures. This swapping step will ensure security against repudiation.

Messaging stage

Messaging may occur any time after distribution.

STEP 5. Alice sends the classical information $\Sigma = (m, \sigma_m)$ to Bob. The m is the message she would like to convey, and her signature is $\sigma_m = \left(A_B^m, A_C^m\right)$.

STEP 6. Bob rearranges $\sigma_m \to \tilde{\sigma}_m := \left(\tilde{A}_{Y,m}^B, \tilde{A}_{Z,m}^B\right)$ by selecting elements from Alice's declaration which correspond to the two halves of his signature. Bob compares $\tilde{\sigma}_m$ to his two halves and counts the number of mismatches. Message m is accepted as genuine provided that

$$\mathcal{M}\left(Y_m^B, \tilde{A}_{Y,m}^B\right) \leqslant s_B \frac{L}{2} \quad \text{and} \quad \mathcal{M}\left(Z_m^B, \tilde{A}_{Z,m}^B\right) \leqslant s_B \frac{L}{2}, \tag{5.2}$$

otherwise the protocol aborts.

STEP 7. If Bob has accepted m then he forwards Σ to Charlie, who similarly checks for mismatches between Alice's eliminated signature and his signature. Charlie accepts the message if

$$\mathcal{M}\left(Y^C_m, \tilde{A}^C_{Y,m}\right) \leqslant s_C \frac{L}{2} \quad \text{and} \quad \mathcal{M}\left(Z^C_m, \tilde{A}^C_{Z,m}\right) \leqslant s_C \frac{L}{2}, \tag{5.3}$$

otherwise it aborts. If both Bob and Charlie accept m then the protocol has succeeded.

It is worth noting some key similarities and differences between QDS-b and the protocol described in Ch. 3. While both protocols rely on QPSK alphabet, heterodyne detection, and the construction and comparison of eliminated signatures, the security analysis required for the two protocols differs. Crucially, while in Ch. 3 the j^{th} element of a dishonest forger's declaration is a single phase chosen from QPSK, for QDS-b Bob must effectively declare *two* phases from QPSK in the form of an eliminated signature element. Additionally, while QDS in Ch. 3 shares similarities with reverse-reconciliation QKD, since a forging Bob had to guess Charlie's measurement outcomes, here QDS-b shares similarities with direct-reconciliation QKD: a forging Bob will have to guess Charlie's sent state. We will later see how this affects performance of the protocol.

5.3.2 *QDS-b security*

Let us consider the security of QDS-b and check how it fulfils the requirements for a QDS protocol.

Security against repudiation

Recall that during a repudiation attack Alice will try to force Bob and Charlie to disagree about whether her message is genuine. Proof of security against repudiation follows identical lines to Sec. 3.2. We assume that Alice is free to manipulate her declared $A^m_{B,C}$ and she has full control over the mismatch rates p_B (p_C) with respect to states she originally received from Bob and Charlie. Alice may even choose p_B or p_C to be zero. Security against repudiation arises from the Symmetrizaton step of the protocol. After Bob and Charlie have swapped classical information, they each possess two half-signatures, length $L/2$, consisting either of information which they held originally or which they received during swapping. Alice succeeds in her repudiation attack if Bob accepts both of his halves as genuine while Charlie rejects at least one of his halves as fake. Therefore the probability of successful repudiation is given by

$$\varepsilon_{\text{repudiation}} = P\left[(E_A \cap E_B) \cap (E_C \cup E_D)\right], \tag{5.4}$$

where the events E_A, E_B, E_C, E_D are defined as

$$\begin{aligned}
\mathcal{M}\left(Y_m^B, \tilde{A}_{Y,m}^B\right) &\leqslant s_B \frac{L}{2}, \\
\mathcal{M}\left(Z_m^B, \tilde{A}_{Z,m}^B\right) &\leqslant s_B \frac{L}{2}, \\
\mathcal{M}\left(Y_m^C, \tilde{A}_{Y,m}^C\right) &> s_C \frac{L}{2}, \quad \text{and} \\
\mathcal{M}\left(Z_m^C, \tilde{A}_{Z,m}^C\right) &> s_C \frac{L}{2},
\end{aligned} \tag{5.5}$$

respectively.

Applying probability inequalities Eq. 3.9, 3.10 and Hoeffding's inequalities Eq. 1.75, 1.76, following the analysis from Sec. 3.2 we see that

$$\varepsilon_{\text{repudiation}} \leqslant \min\left\{2\ \exp\left(-\left[p - s_B\right]^2 L\right), 2\ \exp\left(-\left[s_C - p\right]^2 L\right)\right\}, \tag{5.6}$$

provided that $s_B \leqslant s_C$. The probability $\varepsilon_{\text{repudiation}}$ is maximized when

$$p = \frac{s_B + s_C}{2}. \tag{5.7}$$

Finally we arrive at

$$\varepsilon_{\text{repudiation}} \leqslant 2\ \exp\left(-\frac{\left[s_C - s_B\right]^2}{4} L\right), \tag{5.8}$$

identically to Ch. 3. We have seen that repudiation is only affected by the relative mismatch rates between players' signatures and not by who actually possesses the signatures. This is perhaps unsurprising, since in both QDS protocols it is assumed that Alice has complete control over mismatch rates with respect to states held by players before swapping.

Robustness

The robustness of the protocol depends only on parameters s_B and p_{err}. Using Hoeffding inequality Eq. 3.14 identically to Sec. 3.3 we may derive

$$\varepsilon_{\text{honest abort}} \leqslant 2\ \exp\left(-\left[s_B - p_{\text{err}}\right]^2 L\right) \tag{5.9}$$

provided that $p_{\text{err}} \leqslant s_B$. The probability p_{err} of honest mismatch may be modelled as in Sec. 3.3.1, and does not change here.

5.3.3 *Security against forgery*

Since Bob already knows half of Charlie's signature elements (those which Bob himself forwarded) and since $s_B \leqslant s_C$, the most dangerous

forger is a dishonest Bob. He is therefore assumed to be the eavesdropper on Charlie's distribution of quantum states, and tries to gain information about the $L/2$ signature elements which Charlie generated himself.

Using Hoeffding's inequalities Eq. 3.13 as in Sec. 3.4 we see that a forging attack succeeds with probability

$$\varepsilon_{\text{forgery}} \leqslant 2 \exp\left(-\left[p_e - s_C\right]^2 \frac{L}{2}\right) \tag{5.10}$$

provided that $p_e \geqslant s_C$.

5.3.4 *Bounding p_e*

All that remains is to bound p_e. This will expose several of the differences between QDS-b and QDS from Chapter 3.

Consider the j^{th} signature element. Charlie holds some c_j denoting which state from the QPSK alphabet he sent. During Messaging, Bob will declare an eliminated signature element, $B_j = \left\{b_j^1, b_j^2\right\}$ which is chosen to minimize p_e and should be the outcome of some optimal strategy on his system, denoted $\mathbb{B}$. The b_j^1, b_j^2 correspond to adjacent elements of the QPSK alphabet, with a mismatch occurring if $b_j^1 = c_j$ or $b_j^2 = c_j$.

We define an error variable $\mathcal{E}$ such that

$$\mathcal{E}_j = \begin{cases} 1 & \text{if a mismatch occurs between } \mathcal{F}_j \text{ and } \mathcal{G}_j \\ 0 & \text{otherwise} \end{cases}$$

which measures whether a mismatch has occurred between $\mathcal{F}_j$ and $\mathcal{G}_j$ (c.f. Eq. 3.2). The $\mathcal{F}$ is Charlie's list of phases, while $\mathcal{G}$ is the declared eliminated signature. Then $p_e \equiv P\left(\mathcal{E}_j = 1\right)$, and the Shannon entropy $H\left(\mathcal{E}_j\right) = h\left(p_e\right)$ is the binary entropy, since $\left|\mathcal{E}_j\right| = 2$.

Now, consider the conditional entropy $H\left(\mathcal{E}_j, b_j^1, b_j^2 \,\middle|\, c_j\right)$. Via the chain rule for conditional entropies,

$$H\left(\mathcal{E}_j, b_j^1, b_j^2 \mid c_j\right) = H\left(b_j^1, b_j^2 \mid c_j\right)$$

where we have used the fact that once b_j^1, b_j^2 and c_j are known, $\mathcal{E}_j$ is uniquely determined. Using the chain rule on $H\left(\mathcal{E}_j, b_j^1, b_j^2 \,\middle|\, c_j\right)$ again, but for a different variable, we get

$$\begin{aligned} H\left(\mathcal{E}_j, b_j^1, b_j^2 \mid c_j\right) &= H\left(b_j^1, b_j^2 \mid \mathcal{E}_j, c_j\right) + H\left(\mathcal{E}_j \mid c_j\right) \\ &\leqslant H\left(b_j^1, b_j^2 \mid \mathcal{E}_j, c_j\right) + h\left(p_e\right) \end{aligned}$$

since conditioning can never increase entropy. Therefore, by expanding the variable $\mathcal{E}_j$,

$$H\left(b_j^1, b_j^2 \mid c_j\right) \leqslant (1-p_e) H\left(b_j^1, b_j^2 \mid \mathcal{E}_j = 0, c_j\right) + p_e\, H\left(b_j^1, b_j^2 \mid \mathcal{E}_j = 1, c_j\right) + h\left(p_e\right).$$

Now, $H\left(b_j^1, b_j^2 \,\middle|\, \mathcal{E}_j = 0, c_j\right) \leqslant \log_2(2) = 1$, and similarly for $\mathcal{E}_j = 1$, and so

$$H\left(b_j^1, b_j^2 \mid c_j\right) \leqslant 1 + h\left(p_e\right). \tag{5.11}$$

Finally, we expand the conditional entropy in terms of the joint entropy and the mutual information,

$$\begin{aligned} H\left(b_j^1, b_j^2 \mid c_j\right) &= H\left(b_j^1, b_j^2\right) - I\left(b_j^1, b_j^2 : c_j\right) \\ &\geqslant 2 - \chi\left(b_j^1, b_j^2 : c_j\right), \end{aligned} \tag{5.12}$$

where we have used the fact that *a priori* there are four choices for the pair b_j^1, b_j^2, and where χ is the Holevo information. Combining Eqs. 5.11, 5.12 we arrive at

$$h\left(p_e\right) \geqslant 1 - \chi\left(b_j^1, b_j^2 : c_j\right). \tag{5.13}$$

Surprisingly this equation has similar form to Eq. 3.40, but with a Holevo information calculated differently, as shown below.

Once p_e and p_{err} are bounded for the protocol, the probability ε_{fail} that the protocol fails can be found. For concreteness, we assign equal probability to the failure of the protocol either by allowing a forging or repudiation attack, or by aborting when all players are honest, that is

$$\varepsilon_{\text{fail}} = \varepsilon_{\text{honest abort}} = \varepsilon_{\text{repudiation}} = \varepsilon_{\text{forgery}},$$

and by choosing $s_B = p_{err} + (p_e + p_{err})/4$; $s_C = p_{err} = 3(p_e - p_{err})/4$, in order to satisfy the second two equalities, we arrive at

$$\varepsilon_{fail} \leqslant 2\exp\left[-\frac{(p_e - p_{err})^2}{16} L\right] \tag{5.14}$$

when $p_{err} < s_B < s_C < p_e$.

Calculating Holevo information

Finally, we note that under a beamsplitter attack BS0 Bob's *a priori* state is

$$\rho_B = \frac{1}{4}\sum_{k=0}^{3} |\sqrt{1-T}\alpha_k\rangle\langle\sqrt{1-T}\alpha_k| \tag{5.15}$$

when states $|\alpha_k\rangle$ from the QPSK alphabet are sent through lossy channel with transmission T. Bob's *a posteriori* state is simply $\rho_B^k =$

$|\sqrt{1-T}\alpha_k\rangle\langle\sqrt{1-T}\alpha_k|$, from which his Holevo information is calculated as

$$\chi = S(\rho_B) - \sum_{k=0}^{3} p(k)\, S\left(\rho_E^k\right) \tag{5.16}$$

with S the von Neumann entropy. Under attack BS0 state ρ_B^k is pure and so $\chi = S(\rho_B)$. Other attacks may be readily considered using the techniques from Appendix B. Bob's mismatch rate p_e may now be calculated and we obtain figure of merit signature length L via Eq. 5.14.

5.3.5 *QDS-b postselection*

Let us apply the postselection technique described in Sec. 3.8 to protocol QDS-b. We shall see that while previously postselection was mainly used to improve efficiency of the protocol over parameters in which it was already secure, here it is absolutely necessary in order to sign a message for even short distances. We define the region $\mathcal{R}_{PS}(\Delta_r, \Delta_\theta)$, as in Fig. 3.13, and allow honest recipients to only accept $x \in \mathbb{C} \setminus \mathcal{R}_{PS}$.

The crucial quantity to consider is $g_{sec} := p_e - p_{err}$, measuring the advantage which an honest player has over a dishonest one. The protocol is secure provided that $g_{sec} > 0$, Eq. 5.14. For protocol QDS-b, the probability p_e does not depend on Alice's heterodyne measurement, since a dishonest player attacks the sender of the quantum states. Therefore, p_e is unaffected by postselection.

Probability p_{err} on the other hand is strongly affected by our choice of $\mathcal{R}_{PS}$. Given the probability $P\left(re^{i\theta} \mid \alpha, T\right)$ to obtain complex outcome $re^{i\theta}$ when state $|\alpha\rangle$ is sent through a noiseless channel with transmission T, we see that when no postselection is used

$$p_{err} = \int_{r=0}^{\infty} dr\, r \int_{\theta=\pi/2}^{3\pi/2} d\theta\, P\left(re^{i\theta} \mid \alpha, T\right). \tag{5.17}$$

Incorporating the postselection technique here corresponds to changing the limits of integration, and so when postselection is used we have

$$p_{err}(\Delta_r, \Delta_\theta) = \frac{1}{\mathcal{N}} \int_{r=\Delta_r}^{\infty} dr\, r \left[\int_{\theta=\pi/2+\Delta_\theta}^{\pi-\Delta_\theta} d\theta\, P\left(re^{i\theta} \mid \alpha, T\right) + \int_{\theta=\pi+\Delta_\theta}^{3\pi/2-\Delta_\theta} d\theta P\left(re^{i\theta} \mid \alpha, T\right) \right]. \tag{5.18}$$

Finally, we note that, just as in Sec. 3.8, we must rescale our figure of merit to

$$\tilde{L} = \frac{L}{\mathcal{N}}, \tag{5.19}$$

where normalization factor $\mathcal{N}$ is calculated in the usual way. Since $\tilde{L}$ (with postselection) is directly comparable to L (without postselection) as a figure of merit, in the remainder of this chapter we will not distinguish between the two. However, it must always be understood that if postselection has been used then we are implicitly dealing with $\tilde{L}$.

5.3.6 *QDS-b performance*

We plot signature length as it varies with T under protocol QDS-b in Fig. 5.5. At each T we have optimized over coherent state amplitude α and postselection parameter[4] Δ_r, and the resulting signature lengths are displayed as the solid lines in Fig. 5.5. Black: BS0 attack, Red: EC attack with constant $\bar{n} = 0.02$. Non-solid lines are specific choices of α which are close to optimal only at specific T. We see that choosing an α which is not optimal for a given channel transmission can drastically affect the signature length, and for some transmissions can even result in an increase similar to allowing a different class of attack. Since in a practical realization of the protocol, Δ_r may feasibly be chosen after the distribution of quantum states, we have optimized over Δ_r at each point in the figure.

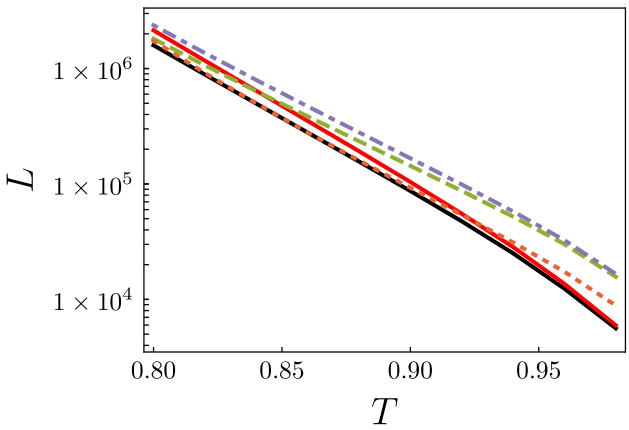


Figure 5.5: QDS-b signature lengths. Black: BS0 attack. Red: EC attack with constant $\bar{n} = 0.02$. Green, dashed: BS0 attack with $\alpha = 0.5$. Orange, dotted: BS0 attack with $\alpha = 0.7$, Blue, dot-dashed: EC attack with constant $\bar{n} = 0.02$, $\alpha = 0.5$. All lines have optimal Δ_r chosen at each point. Solid lines: optimal choice of α and Δ_r at each point.

4 As in Ch. 3, choosing $\Delta_\theta > 0$ worsened performance.

To summarise, our first agile system, QDS-b-QSS-b-CV-QPSK, is capable of performing the secure tasks QDS and QSS. We have incorporated the QSS protocol discussed in Ch. 4 and labelled it QSS-b, for consistency of notation. The new protocol QDS-b may be viewed as a direct-reconciliation analogue of the QDS protocol discussed in Ch. 3. We will implement each protocol and discuss performance in Sec. 5.6.3.

5.4 AGILE SYSTEM QDS-f-QKD-f-CV-QPSK

In addition to the first agile system described above, which is capable of performing both QDS and QSS tasks, we here introduce and demonstrate a second agile system, QDS-f-QKD-f-CV-QPSK, which runs in the f-configuration, Fig. 5.3. Here, Alice is the sender of quantum states, while Bob and Charlie are the recipients. This system is capable of performing both QDS and QKD tasks.

The QKD protocol contained in QDS-f-QKD-f-CV-QPSK already exists in the literature [137, 143] and has been an active direction of research for many years. Its inclusion here illustrates that pre-existing protocols may be interpreted through an agile lens. We denote the QKD protocol QKD-f. The QDS protocol in f-configuration was analysed above in Chapter 3, and here we rename it as QDS-f.

Let us briefly consider each protocol in turn.

5.4.1 *Protocol QDS-f*

We bring the QDS protocol considered in Chapter 3 into the system QDS-f-QKD-f-CV-QPSK. The protocol QDS-f requires no modification to run over hardware in the f-configuration and so the reader is referred to Ch. 3 for details, security proof, and performance analysis. Our earlier security analysis assumed ideal behaviour. In Sec. 5.6.1 we relax some of these assumptions and make the protocol analysis more realistic to experimental implementation.

5.4.2 *Protocol QKD-f*

QKD using heterodyne detection of a discrete-modulated alphabet of coherent states has long been proposed and analysed, owing to its ease of implementation and high compatibility with installed telecommunications infrastructure [96, 137, 141, 143, 146, 147]. Despite its practical ease of use, theoretical work has lagged behind other CV QKD protocols, which rely on a Gaussian modulation of coherent states. Unlike DV systems, CV systems live in an infinite dimensional Hilbert space and so many of the computational methods available for QKD with single-photons are not immediately transferable [52], and unlike Gaussian-modulated CV systems, coherent states with a

discrete-modulation cannot be reduced to calculations on the finite-sized covariance matrix.

Attempts to prove security of discete-modulated CV QKD protocols have made simplifying assumptions in either of these directions. For example, in Refs. [96, 143] it is assumed that since the amplitude α of coherent states in the chosen QPSK alphabet is small, the *a priori* states in the protocol are approximately Gaussian. This allows covariance-matrix based methods to be used for the analysis. This assumption is only strictly true in the limit $\alpha \to 0$, and it is as yet unproven whether an attack could exploit higher order statistical moments of the *a priori* state which are not captured by the covariance matrix.

Another direction has been to truncate the size of the Hilbert space [96, 137, 141]. This is perhaps a reasonable approach, since for many of the infinite-dimensional states used in the QKD protocols one can find a nearby state which lives in a large but finite-dimensional Hilbert space. This becomes increasingly true for small α.

A QKD protocol relying on a QPSK alphabet and heterodyne detection is analysed in Ref. [137], and it is their analysis which we lean on in this section. Alice distributes coherent state $|\alpha\rangle$ from her QPSK alphabet through the quantum channel to Bob[5]. Assuming, for now, attack BS0, Bob recieves $|\sqrt{1-T}\alpha\rangle$ and performs heterodyne measurement, obtaining outcome x with probability

$$P(x \mid \alpha, T) = \frac{1}{\pi} \exp\left(-\left[x - \sqrt{T}\alpha\right]^2\right). \tag{5.20}$$

We denote Alice's variable containing information of which coherent state she chose by X_A, and Bob's variable containing his measurement outcome by X_B. Alice and Bob then perform a reverse-reconciliation procedure [95, 99, 138] to form a secret key.

The starting point for the analysis is the Devetak-Winter key rate formula [153]

$$\kappa \geqslant I(X_A : X_B) - \chi(X_B : \mathbb{E}), \tag{5.21}$$

where $\mathbb{E}$ denotes Eve's quantum system. Let us calculate each term.

Mutual information I

The mutual information I is calculated in a similar fashion to the protocol QSS-b discussed in Chapter 4. Using Eq. 1.81 we expand I as

$$I(X_A : X_B) = H(X_A) - H(X_A \mid X_B). \tag{5.22}$$

The Shannon entropy of Alice's variable is equal to $\sum_{X_A = a} -P(a) \log P(a)$ and is equal to 2 in the ideal case.

We may expand the conditional entropy in Eq. 5.22 as

$$H(X_A \mid X_B) = \int_{b \in \mathbb{C}} d^2b \, P(X_B = b) \, H(X_A \mid X_B = b), \tag{5.23}$$

5 Alice could also perform QKD with Charlie, and the discussion follows identically.

where the integration is performed over all possible outcomes b which Bob can obtain. The mutual information I may then be calculated by expanding $H(X_A \mid X_B = b)$ and then using Bayes's formula.

Holevo information χ

We will derive the Holevo information χ which Eve has about Bob's variable X_B under attack BS0. Her Holevo information under other attacks may be calculated likewise, using steps from Sec. 3.6.

When a coherent state α_k is chosen uniformly at random, the two-mode output state from the channel is

$$\rho_{B,E} = \frac{1}{4} \sum_{\alpha_k} \left[\left| \sqrt{T}\alpha_k \right\rangle \left\langle \sqrt{T}\alpha_k \right|_B \otimes \left| \sqrt{1-T}\alpha_k \right\rangle \left\langle \sqrt{1-T}\alpha_k \right|_E \right], \quad (5.24)$$

and so after Bob's heterodye measurement, outcome $b \in \mathbb{C}$, Eve's conditional state is

$$\rho_{E \mid b} = \frac{1}{4} \frac{1}{P(b)} \sum_{\alpha_k} P(b \mid \alpha_k, T) \times \left| \sqrt{1-T}\alpha_k \right\rangle \left\langle \sqrt{1-T}\alpha_k \right|_E \quad (5.25)$$

where $P(b) = \sum_{\alpha_k} P(b \mid \alpha_k, T)$ denotes the total probability that Bob measures b. Eve's *a posteriori* entropy is then

$$S_{\text{aposteriori}} = \int_{b \in \mathbb{C}} d^2 b \, P(b) \, S\left(\rho_{E \mid b}\right), \quad (5.26)$$

and we note that each state $\rho_{E \mid b}$ has in general a different entropy, so Eq. 5.26 cannot be simplified further.

Eve's *a priori* entropy is

$$S_{\text{apriori}} = S\left[\int_{b \in \mathbb{C}} d^2 b \, P(b) \, \rho_{E \mid b} \right], \quad (5.27)$$

from which the Holevo information χ may be calculated. Attacks BS1, BS2 and EC may be implemented following an identical analysis to this section. The performance of protocol QKD-f is discussed at length in Ref. [137] and so we refer the reader there.

5.5 EXPERIMENTAL IMPLEMENTATION

An experiment which investigates the above two agile systems was performed at the Max Plank Institute for the Science of Light in Erlangen (MPL) [163], Fig. 5.6. Specifically, optical sender and receiver modules were used to implement the four protocols which are described above. A sender module (Tx) generates and distributes phase-encoded

coherent states chosen from the QPSK alphabet, while a receiver module (Rx) performs heterodyne detection of the received states' phase. Depending on the required configuration, the modules Tx, Rx are variously interpreted as playing roles of Alice or Bob/Charlie, Fig. 5.3. Crucially, the hardware setup is identical for every protocol within an agile system.

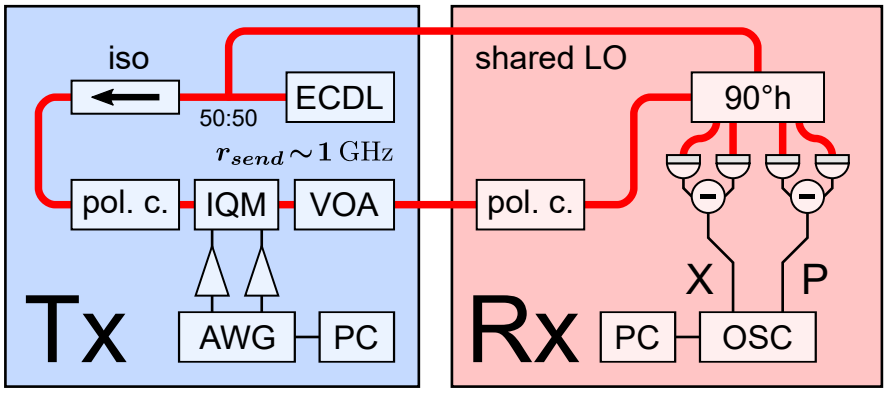


Figure 5.6: The sender (Tx) and receiver (Rx) modules which are used to implement each of the four cryptographic protocols considered in this Chapter. During distribution and measurement of the quantum states, hardware modules are ignorant about the roles which they are playing, and so identical experimental stages may be interpreted for different cryptographic tasks, Fig. 5.3. ECDL: external-cavity diode laser; iso: isolator; VOA: variable optical attenuator; IQM: I/Q modulator; pol.c: polarization controller; AWG: arbitrary waveform generator; LO: local oscillator; 90°h: 90° hybrid; OSC: oscilloscope. *Picture credit: Stefan Richter in Ref. [163]*

Sender module (Tx):

The sender module is depicted in Fig. 5.6. An external cavity diode laser (PurePhotonics PPCL-300) with a linewidth of 15 kHz is tuned to standard telecom wavelength 1550 nm and acts as the optical carrier. The carrier beam impinges on a 50 : 50 beamsplitter which allows for a shared local oscillator (LO) between modules from one output port. From the other output port coherent state pulses, chosen randomly from QPSK alphabet $\{|+\alpha_0\rangle, |i\alpha_0\rangle, |-\alpha_0\rangle, |-i\alpha_0\rangle\}$, are prepared by using an integrated I/Q modulator (Fujitsu DP-QPSK 40 Gbps $LiNbO_3$) which is driven at a rate of 1 GHz by an arbitrary waveform generator (AWG; Keysight M8195A). Finally, a variable optical attenuator (VOA) attenuates the coherent states to a final amplitude of either α or α', with $\alpha \leqslant \alpha' \leqslant \alpha_0$. Coherent states with ampltude α' will be used as phase reference states, while the signal states used for the quantum communication protocols have amplitude α. The coherent states are then sent through the quantum channel to receiver module Rx.

Receiver module (Rx):

Module Rx interferes the received states with the shared local oscillator using the integrated Kylia COH24-X 90°s. The two modules use a shared local oscillator which provides a frame of reference against which heterodyne phase measurement is performed using two balanced optical receivers (Discovery DSC-R412) with analog 3 dB bandwidth of 20 GHz. In principle the Tx and Rx modules do not need to share a local oscillator and bright phase-reference pulses[6] could instead be used [175].

Outputs from the optical receivers are digitized using a digital sampling oscilloscope (Tektronix DPO77002SX) with a sampling rate of 25 GS/s. Proprietary digital signal processing (DSP) algorithms, designed by MPL, are applied to the quadrature time traces. The DSP includes a high-pass filter which eliminates low-frequency noise contributions to the signal. Finally, a phase-recovery step is performed using phase-reference states which originally had amplitude α'.

The Tx and Rx modules were connected by either a 2 km or 20 km SMF-28 optical fiber link which contributes to a total loss of 0.65 dB or 4.75 dB, respectively. This implements the realistic metropolitan distances over which the CV platform is expected to be effective. Experiments were performed for several different signal state modulation amplitudes α. For each run of the experiment a total of 1.92×10^6 states were sent in frames of 64 which consisted of four bright reference pulses (α') followed by 60 signal pulses (α). After the DSP step there remained information on 1.54×10^6 states. An example of some raw output data is displayed in Fig. 5.7. The top of the figure displays raw time trace data, while the bottom displays data after the DSP.

6 Though note that this may open up additional security issues [174].

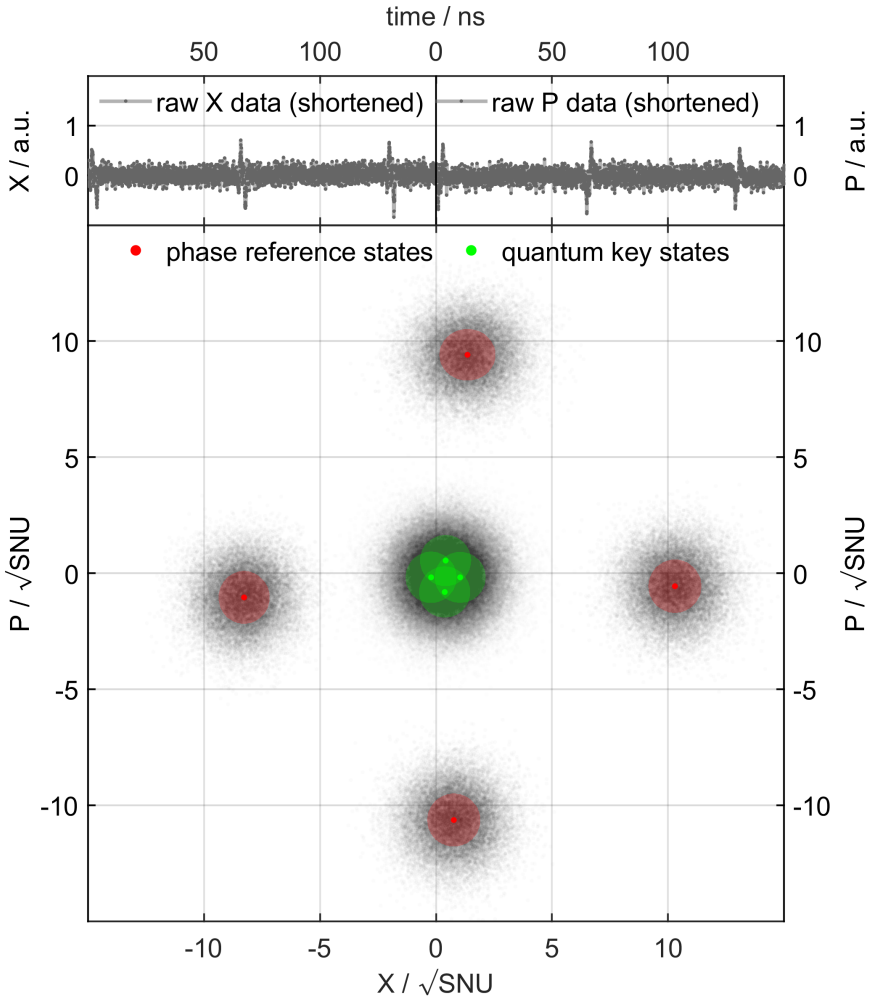


Figure 5.7: Top: raw data trace. Bottom: data after DSP. Red: heterodyne outcomes on bright phase-reference states, amplitude α' which are sent at the start of each frame, and allow the phases of the remaining states to be reconstructed. Green: heterodyne measurement outcomes on signal states amplitude $\alpha < \alpha'$. The cryptographic tasks are performed with signal (green) data points only. *Picture credit: Stefan Richter in Ref. [163]*

5.6 DATA ANALYSIS

In this section we will analyse the data which was obtained in the experiment detailed in the previous section. Our starting point is the signal data points[7] which we received from MPL. In Sec. 5.6.1 we will examine how the cryptographic protocols detailed above may be altered to more closely match the realistic data which includes experimental imperfections. In Sec. 5.6.2 we will closely examine the data which we have received from MPL and which forms the basis for our demonstration of two quantum agile systems. We will demonstrate how it may be used to estimate protocol performance and figures of merit[8], and then discuss how the experiment provides an agile interpretation.

5.6.1 *Protocol modifications*

Throughout this Thesis it has been assumed that an ideal QPSK alphabet has been distributed, with states chosen uniformly and at random. This has allowed us to make several simplifying assumptions. For example in protocol QDS-f, these assumptions allowed us to simplify Eq. 3.47 as follows

$$\sum_{e_k} P(e_k)\, S\left(\rho_{B\,|\,e_k}\right) \to S\left(\rho_{B\,|\,e_1}\right). \tag{5.28}$$

Similarly, in QSS-b we repeatedly used the fact that each QPSK state was equally likely, in order to write Eq. 4.7, for example, as

$$P(b,c) = \frac{1}{16}. \tag{5.29}$$

Realistically the states are not sent with identical sending probabilities, nor are they sent with identical amplitudes. The actual sending amplitudes for each experimental run are displayed in Tab. 5.1. Non-uniform sending probabilities may also be directly measured from a disclosed subset of data. These imperfections must be taken into account in our bounds for key rate and signature length, which we now do.

QDS-b

In QDS-b the key parameter to calculate is $g_{sec} = p_e - p_{err}$, which is related to the signature length figure of merit via Eq. 5.14. Bob's mismatch probability p_e is made more realistic by changing several steps in the derivation of Holevo information χ.

7 Green in Fig. 5.7

8 Of which the ideal figures of merit obtained in previous chapters are an upper bound.

For example, under attack BS0 we update Bob's *a priori* state, c.f. Eq. 5.15, to be

$$\rho_B = \sum_{\alpha_k} P(\alpha_k) \left|\sqrt{1-T}\alpha_k\right\rangle\left\langle\sqrt{1-T}\alpha_k\right| \tag{5.30}$$

where the amplitudes α_k and sending probabilities $P(\alpha_k)$ are directly derived from the received data. Bob's *a posteriori* states

$$\rho_B^k = \left|\sqrt{1-T}\alpha_k\right\rangle\left\langle\sqrt{1-T}\alpha_k\right| \tag{5.31}$$

and *a posteriori* entropy

$$\sum_{\alpha_k} P(\alpha_k)\, S\left(\rho_B^k\right) \tag{5.32}$$

now also depend on the measured data. For attacks BS1 and EC, they must be calculated without the simplifications afforded by ideal sending probabilities and equal $|\alpha_k|$'s. For attack BS0 Bob's *a posteriori* entropy vanishes identically because his state is assumed pure.

The honest mismatch probability p_{err} may be measured directly from the data by observing the probability that a state is eliminated. We demonstrate this in Sec. 5.6.3.

QSS-b

We will demonstrate the necessary alterations which should be made to mutual information I and Holevo information χ in protocol QSS-b.

MUTUAL INFORMATION I, EQ. 4.5 The joint Shannon entropy of Bob and Charlie's variables is given by

$$H(X_B, X_C) = -\sum_{X_B=b, X_C=c} P(b,c) \log P(b,c) \tag{5.33}$$

where X_B, X_C denote the states from QPSK which Bob and Charlie sent, and $P(b,c)$ their sending probabilities. We have observed that

$$P(b,c) = P(b) \times P(c) \tag{5.34}$$

and when variations in the sending probabilities are considered this is no longer equal to 1/16.

Secondly, the probability $P(X_A = a \mid X_B = b, X_C = c)$, Eq. 4.11, should be updated to match the actual amplitudes of the sent coherent states.

HOLEVO INFORMATION χ The initial states Eq. 4.22 should be updated to

$$\rho_B = \sum_{k=0}^{3} P(\beta_k) |\beta_k\rangle\langle\beta_k|_B \quad \text{and} \quad \rho_C = \sum_{k'=0}^{3} P(\gamma_{k'}) |\gamma_{k'}\rangle\langle\gamma_{k'}|_C \tag{5.35}$$

and therefore Eq. 4.28 becomes

$$\rho_{\mathbb{E}\,|\,X_A,A_B} = \frac{1}{\pi^2}\sum_{k,k'=0}^{3} P(b,c)\,P_B(A_B \mid \beta_k, T_B)\,P_C\left(\frac{X_A - gA_B}{h}\,\middle|\,\gamma_{k'}, T_C\right) \left|\sqrt{1-T_B}\beta_k\right\rangle\!\left\langle\sqrt{1-T_B}\beta_k\right|_{\mathbb{E}_B} \otimes \left|\sqrt{1-T_C}\gamma_{k'}\right\rangle\!\left\langle\sqrt{1-T_C}\gamma_{k'}\right|_{\mathbb{E}_C} \tag{5.36}$$

from which Holevo information χ is calculated.

QDS-f

Protocol QDS-f requires us to recalculate $g_{sec} = p_e - p_{err}$ with these experimental imperfections. Probability p_{err} may be estimated directly from data and is equivalent to the analysis performed above for QDS-b.

Probability p_e requires us to reconsider certain steps in the calculation of Holevo information χ. We consider attack BS0, and other attacks follow similarly. After the channel, the state held by Charlie and dishonest Bob is, c.f. Eq. 3.42,

$$\sum_{\alpha_k} P(\alpha_k)\left[\left|\sqrt{T}\alpha_k\right\rangle\!\left\langle\sqrt{T}\alpha_k\right|_C \otimes \left|\sqrt{1-T}\alpha_k\right\rangle\!\left\langle\sqrt{1-T}\alpha_k\right|_B\right], \tag{5.37}$$

and so Bob's conditional state becomes, c.f. Eq. 3.43

$$\rho_{B\,|\,c} = \frac{1}{P(c)}\sum_{\alpha_k} P(\alpha_k)\,P(c \mid \alpha_k, T) \times \left|\sqrt{1-T}\alpha_k\right\rangle\!\left\langle\sqrt{1-T}\alpha_k\right|_B, \tag{5.38}$$

where $P(c \mid \alpha_k, T)$ is Charlie's probability to measure c and $P(c) = \sum_{\alpha_k} P(c \mid \alpha_k, T)$ which is now no longer symmetric.

Each of Bob's states conditioned on an eliminated signature element e_k now have different entropies and different probabilities $P(e_k)$ and so we must write the Holevo information out in full, c.f. Eq. 3.49,

$$\chi = S\left(\sum_{e_k} P(e_k)\,\rho_{B\,|\,e_k}\right) - \sum_{e_k} P(e_k)\,S\left(\rho_{B\,|\,e_k}\right). \tag{5.39}$$

QKD-f

Finally, we consider how the protocol QKD-f may be updated to allow for non-uniform QPSK alphabets.

MUTUAL INFORMATION I, EQ. 5.22 The Shannon entropy $H(X_A)$ of Alice's variable is easily modified with the new probability distribution $P(X_A)$, and is given by

$$H(X_A) = -\sum_{X_A = a} P(a)\log P(a) \tag{5.40}$$

which is easily calculated using the measured $P(a)$. The conditional entropy $H(X_A \mid X_B)$ is readily calculated following the discussion[9] beneath Eq. 5.23.

HOLEVO INFORMATION χ Eve's conditional state after Bob's heterodyne measurement becomes, c.f. Eq. 5.25,

$$\rho_{E\mid b} = \frac{1}{P(b)} \sum_{\alpha_k} P(\alpha_k)\, P(b \mid \alpha_k, T) \times \left|\sqrt{1-T}\alpha_k\right\rangle\!\left\langle\sqrt{1-T}\alpha_k\right|_E , \tag{5.41}$$

with $P(b) = \sum_{\alpha_k} P(b \mid \alpha_k, T)$ also changing and becoming asymmetric.

Eve's *a posteriori* and *a priori* entropies are calculated identically to Eqs. 5.26, 5.27 using Eq. 5.41 as a starting point.

5.6.2 *Received data*

From our experimental collaborators at MPL we received four datasets output from the experiment detailed in Sec. 5.5. Figure 5.7 displays raw data before and after the action of the experimental collaborators' proprietary digital signal processing (DSP) algorithm. The data we have received is of the form of bottom figure of Fig. 5.7, and we received only the signal data (green circles) once the phase-reference data (red circles) were removed. Each of the received datasets consisted of 1.54×10^6 elements of pairs of measured phase outcomes (x_{out}, p_{out}), along with information about which element from the QPSK alphabet Alice sent. The received datasets have parameters detailed in Tab. 5.1.

We calculate the parameters entering Tab. 5.1 directly from the received data sets. The amplitude α sent by Alice is calculated by a rescaling of phase measurement data, as follows. For data when a particular $|\alpha\rangle$ was sent, we calculate the means $\bar{x}_{out}$, $\bar{p}_{out}$ of measured output data. The mean coherent state amplitude which was received at Rx is then given by

$$\alpha_{Rx} = \frac{\bar{x}_{out} + i\bar{p}_{out}}{\sqrt{2}}. \tag{5.42}$$

From Tx to Rx, the distributed state has undergone two primary sources of loss: trusted loss and untrusted loss. Untrusted loss must be attributed to Eve, and is a combination of propagation losses in the fiber, and coupling losses into and out of the fiber. We write this as a single number which corresponds to the loss of the channel (or channel transmission T), and is -0.65 dB for the 2 km channel and -4.75 dB for the 20 km channel. These values were given to us by our experimental collaborators and were measured using their proprietary methods. The trusted loss occurs in the detector Rx and

9 See also the discussion for alterations to protocol QSS-f, which is analogous.

an eavesdropper is assumed to not have access to this. The quoted value is $\approx 50\%$ loss due to Rx.

The amplitude sent by Tx may then be calculated as

$$\alpha_{Tx} = \frac{\alpha_{Rx}}{\sqrt{0.5}\sqrt{T}}. \tag{5.43}$$

This scaling procedure was done for each run and each distributed QPSK state, and the re-scaled values are displayed in Tab. 5.1.

The excess noises corresponding to measurements in each quadrature ξ_x, ξ_p are calculated separately, and the value of excess noise which we use to estimate the power of the eavesdropper is $\xi = \max\{\xi_x, \xi_p\}$. Maximizing ξ in this way gives the eavesdropper additional power, since it assumes that they have used a state with a higher degree of entanglement. We might reasonably expect that affording Eve this power should loosen the bounds which we calculate in this chapter, and tighter bounds with an analysis which includes this asymmetry in noise profiles are left for future work.

The variance in measurement outcome in each x and p for each distributed state was measured, and the final excess noise is given by

$$\xi_x = \mathrm{Var}(x) - \frac{1}{2} - \mathrm{Var}(x)_{\text{trusted}}, \tag{5.44}$$

and similarly for p. The contribution $\mathrm{Var}(x)_{\text{trusted}}$ represents system detector noise which is assumed to be outside of Eve's control, and which was fully characterised by our experimental collaborators. The final excess noise values are then averaged over each distributed QPSK state, and then maximized over x, p. These final values ξ are displayed in Tab. 5.1. The excess noise values were quoted to us by experimental collaborators.

To illustrate our received data, we plot the first $100,000$ elements of raw data for run 1 in Fig. 5.8. In (a) we display data corresponding to the input state $|\alpha\rangle$ with $\alpha = 0.615$, and in (b) we display data corresponding to the entire QPSK alphabet, which is highly non-orthogonal.

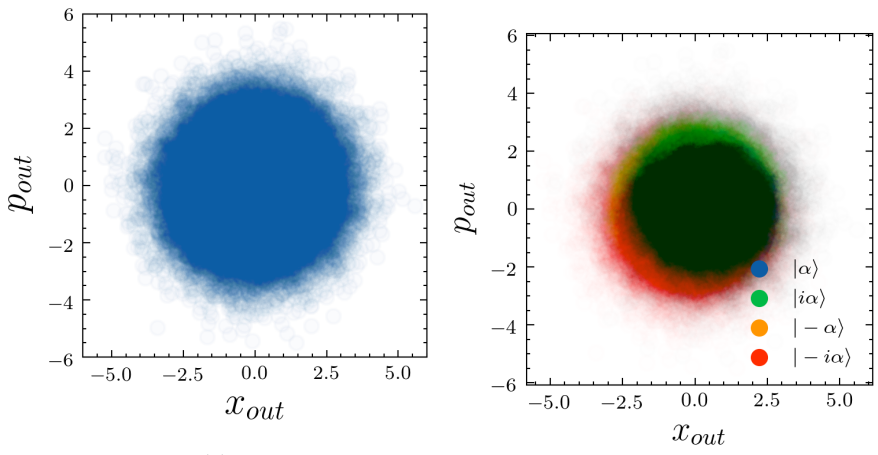
In Fig. 5.9 we demonstrate for protocols QDS-f and QDS-b how p_{err} may be calculated on a particular dataset. Having isolated the elements for which a particular alphabet state was sent, the data is partitioned into groups which will induce a mismatch or not. In this case, $|\alpha\rangle$ was sent and so data with $x_{\text{received}} \geqslant 0$ will not induce a mismatch, while data with $x_{\text{received}} < 0$ will. The mismatch probability p_{err} is then calculated as

$$p_{err} = \frac{\text{Number of data points which cause a mismatch}}{\text{Total number of data points}}, \tag{5.45}$$

where the numerator is calculated including all four of the distributed QPSK states, with their respective mismatch criteria.

Experiment		**QPSK amplitudes** $[\sqrt{\text{snu}}]$					**Excess noise** [%]
Run	Fiber [km]	α	$i\alpha$	$-\alpha$	$-i\alpha$	$\bar{\alpha}$	$\max\{\xi_x, \xi_p\}$
1	2	0.615	0.676	0.620	0.620	0.64	2.7
2	20	0.624	0.754	0.629	0.717	0.67	1.9
3	20	0.493	0.626	0.499	0.606	0.55	2.1
4	20	0.578	0.716	0.579	0.688	0.64	1.7

Table 5.1: Parameters of received datasets. Each of the four experimental runs had slightly asymmetric amplitudes for each of the QPSK alphabet states α, $i\alpha$, $-\alpha$, $-i\alpha$. The mean amplitude for each run is $\bar{\alpha}$. Each of the states was sent with probability close to 1/4. Excess noise differs between x and p quadratures, and for our analysis the largest of these was chosen, i.e. $\xi = \max\{\xi_x, \xi_p\}$. The loss level corresponding to the 2 km channel is -0.65 dB, and the loss level corresponding to 20 km channel is -4.75 dB. This includes the channel and additional losses due to coupling inefficiencies, but does not include trusted detector loss of 50%.



(a)

Figure 5.8: Datasets received from experimental collaborators, corresponding to x_{out} and p_{out} phase measurement outcomes when (a) state $|\alpha\rangle$ was sent, run 1 and (b) states $|\alpha\rangle$, $|i\alpha\rangle$, $|-\alpha\rangle$, $|-i\alpha\rangle$ were sent, run 1. We plot only the first 100,000 points, for illustrative convenience. (b) At the amplitudes chosen, our QPSK alphabet is overlapping and highly non-orthogonal.

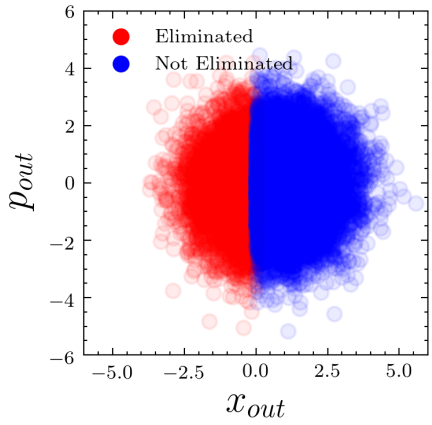
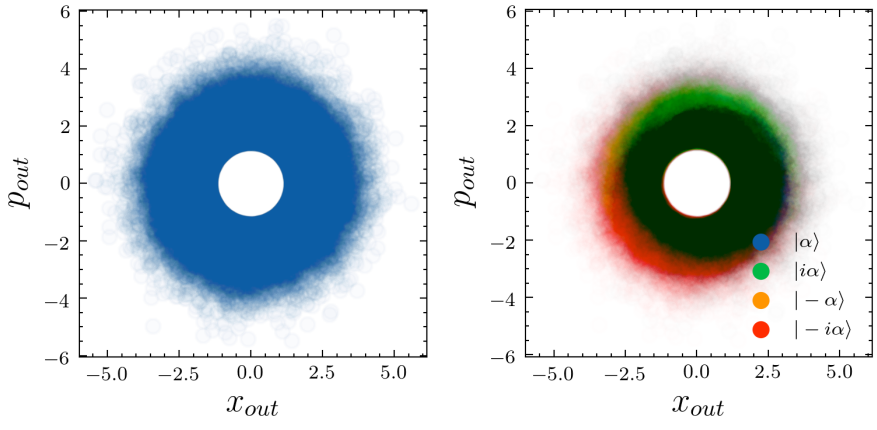


Figure 5.9: Illustration of received data points, coloured by whether they induce a mismatch in protocols QDS-f and QDS-b. State $|\alpha\rangle$ was sent, and data is taken from run 1. Blue: data points will not cause $|\alpha\rangle$ to be eliminated, and so do not cause a mismatch. Red: data points will cause $|\alpha\rangle$ to be eliminated, and so a mismatch occurs. For convenience we display only the first 100,000 data points.

In protocols QDS-f and QDS-b we also discussed the possibility to postselect on measurement outcomes, by ignoring datapoints which fall within $\mathcal{R}_{PS}$. As was discussed in their respective sections, we take $\mathcal{R}_{PS}(\Delta_r)$ and display examples of postselected data sets in Fig. 5.10. Data corresponding to distributed $|\alpha\rangle$ are displayed in Fig. 5.10a, while data for all elements of QPSK are displayed in Fig. 5.10b. For illustrative convenience we display only the first 100,000 elements. We may calculate p_{err} in an identical way to that discussed above, simply starting from the postselected data in order to reduce p_{err} and increase the advantage gained by an honest player.



(a) (b)

Figure 5.10: Postselection technique with region $\mathcal{R}_{PS}(\Delta_r = 1.0)$ applied to the datasets from Fig. 5.8.

	QDS - b		**QDS - f**		**QSS - b**	**QKD - f**
Run	L [bits^{-1}]	t [ms]	L [bits^{-1}]	t [ms]	2κ	κ
1	5.70×10^{6}	5.7	4.79×10^{4}	0.048	0.3726	0.3479
2	-	-	2.26×10^{9}	2260	0.1058	0.1024
3	-	-	1.37×10^{8}	137	0.0858	0.0840
4	-	-	2.08×10^{8}	208	0.1004	0.0976

Table 5.2: Protocol figures of merit for the experimental runs. QDS signature lengths (L) and signing times (t) required to sign a 1-bit message for security level of $\varepsilon = 0.01\%$. The QSS and QKD key rates correspond to the maximum estimated number of bits of secure key which may be generated per use of the quantum channel. In QSS-b, one channel use corresponds to distribution of *two* quantum states, one from Bob and one from Charlie, and so we display 2κ for fair comparison with QKD.

5.6.3 *Protocol performance*

The experiment detailed in Sec. 5.5 was performed and we have received four datasets from our experimental collaborators. The key parameters for these datasets are described in Tab. 5.1 and form the basis for an analysis of performance of each of our cryptosystems.

First agile system QDS-b-QSS-b-CV-QPSK

In the first agile system, QDS-b-QSS-b-CV-QPSK, the sender module Tx is understood to play the role of either Bob or Charlie, while Rx plays the role of Alice. Signature lengths under QDS-b are calculated using the data parameters from Tab. 5.1 with the postselection region[10] $\mathcal{R}_{PS}$ optimized. In the ideal case, honest mismatch probability p_{err} is calculated using Eq. 3.25 under the model described there (or including excess noise, Appendix A). We additionally include a detector efficiency of 50% which a dishonest player cannot exploit.

For QDS-b we allow dishonest Bob to perform the entangling cloner attack, and we estimate p_e using the models in Sec. 3.6, 5.3 once α and the worst-case excess noise ξ have been estimated from data. These ideal signature lengths for QDS-b are displayed in Fig. 5.11. The point at which run 1 (red) intersects the vertical gridline (2 km fiber length) corresponds to a point at which we have data. Other points in Fig. 5.11 are calculated by varying T in our model.

10 $\mathcal{R}_{PS} = \mathcal{R}(\Delta_r)$

We see that over metropolitan distances of up to several kilometers, which are favourable to the CV platform, the protocol QDS-b obtains modest signature lengths $\mathcal{O}\left(10^6\right)$. Even at these short distances however the excess noise ξ has strong impact on the required signature lengths.

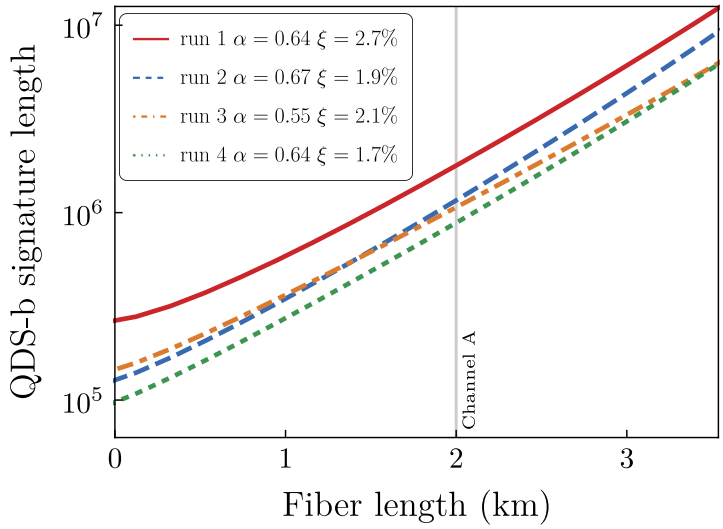


Figure 5.11: Signature lengths required to sign a single bit in protocol QDS-b, under entangling-cloner attack. The signature lengths at a distance of 2 km remain modest both in the ideal (above) and experimental (Tab. 5.2) realizations. Solid (red), dashed (blue), dot-dashed (orange) and dotted (green) lines correspond to performance deduced by parameters from experimental runs 1, 2, 3 and 4, respectively. The vertical grid line depicts the loss level over experimental channel A (0.65 dB loss).

We have so far not taken into account in the estimates of p_e and p_{err} the actual amplitudes and sending probabilities which Tx sent. These may be included using the changes outlined in Sec. 5.6.1. We may make our result more accurate still by measuring p_{err} directly from the output of Rx. The p_{err} calculated in this way automatically takes into account all sources of trusted detector loss and noise which will increase p_{err}. For example, for experimental run 1 over the 2 km channel (Channel A), a signature length of 5.7×10^6 is required to sign a single bit, Tab. 5.2, which is an increase in signature length over Fig. 5.11. However, even at 20 km protocol QDS-b could still be made secure by choosing a postselection region with $\Delta_r \ggg 1$, but for loss levels larger than ~ 2 dB the required signature length becomes impractically large.

For our secret sharing protocol QSS-b, Fig. 5.12, the Holevo information is calculated by estimating channel transmission T and excess noise ξ from the data and assuming that the dishonest players perform beamsplitter attack BS2 (Sec. 3.6). Results in Fig. 5.12 use the ideal analysis identically to Ch. 4. We may calculate more realistic

maximum key rates by using the modifications from Sec. 5.6.1 with experimental parameters in Tab. 5.1, to include non-uniform coherent state amplitudes and sending probabilities. We display these key rates in Tab. 5.2.

Notably, we see that twice the key rate, 2κ is greater than the comparable key rate κ for QKD-f (remembering that one channel use is defined differently between QKD and QSS). In other words, QSS-b outperforms pairwise QKD by consuming fewer quantum resources to obtain an equivalent key rate. We have observed therefore that a "direct" QSS can outperform the classical unconditionally secure secret sharing mediated by QKD. This is thus another case where our agile framework is preferable to the QKD-assisted crypto-agility.

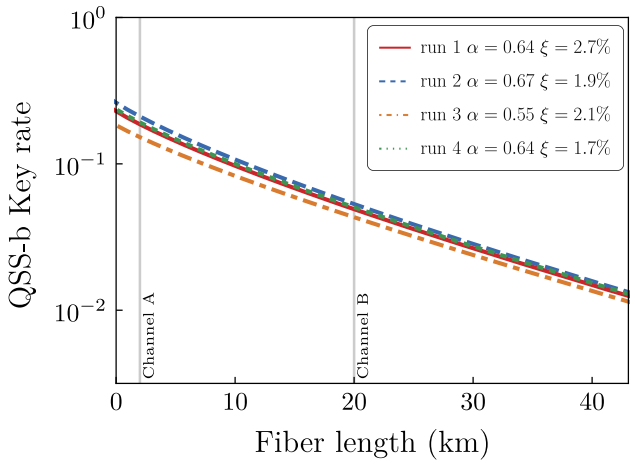


Figure 5.12: Maximum attainable key rates for protocol QSS-b. Dishonest Eve performs attack BS2, and either Bob or Charlie are also dishonest. The key rate is robust to variations in α, and remains large even for our 20 km channel. Solid (red), dashed (blue), dot-dashed (orange) and dotted (green) lines correspond to the ideal performance deduced by parameters from experimental runs 1, 2, 3 and 4, respectively. Vertical grid lines depict loss levels over experimental channels A and B, corresponding to fiber lengths 2 km (0.65 dB loss) and 20 km (4.75 dB loss)

We have investigated performance of the first agile system QDS-b-QSS-b-CV-QPSK which is capable of performing quantum digital signatures (QDS) and quantum secret sharing (QSS) tasks. Specifically, we have analysed the same experimental datasets under the two different protocols, demonstrating that they only differ at the level of classical postprocessing. Of particular note is that our QSS protocol outperforms qCSS while requiring identical resources in terms of hardware (for QPSK-based QKD) and quantum channels, while being secure against equivalent attacks.

Second agile system QDS-f-QKD-f-CV-QPSK

For the second agile system, QDS-f-QKD-f-CV-QPSK, Tx plays the role of Alice while Rx plays either Bob or Charlie. The performance under protocol QDS-f is displayed in Fig. 5.13 under attack BS2. The excess noise and detector efficiency from the experiment are included, and p_e and p_{err} are calculated using analogous methods to QDS-b, above. We see than in the ideal analysis of Fig 5.13 (using ideal models from Ch. 3) the protocol QDS-f allows for very small signature lengths $\mathcal{O}\left(10^4\right)$ at 2 km, while at 20 km the predicted lengths are still very modest at $\mathcal{O}\left(10^6\right)$.

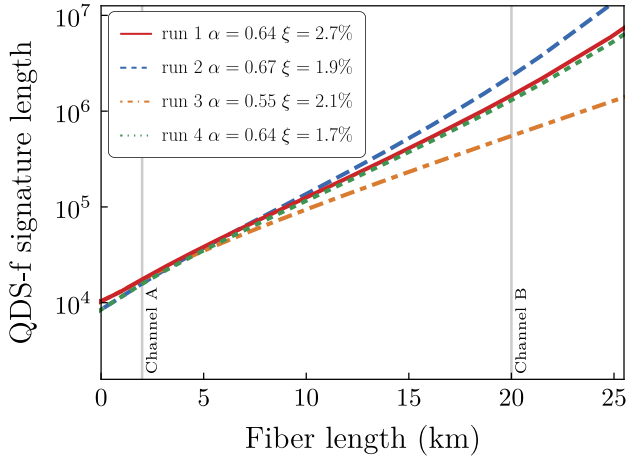


Figure 5.13: Signature lengths required to sign a single bit in protocol QDS-b, under attack BS2. The signature lengths at 20 km (Channel B) remain feasible under both ideal (above) and experimental (Tab. 5.2) realizations. At 2 km (Channel A) the protocol requires small signature lengths and is thus the fastest QDS protocol over comparable distances, Fig. 5.14. Solid (red), dashed (blue), dot-dashed (orange) and dotted (green) lines correspond to experiments 1, 2, 3 and 4, respectively. Vertical grid lines depict loss levels over implemented channels A and B, corresponding to fiber lengths 2 km (0.65 dB loss) and 20 km (4.75 dB loss), respectively.

For small channel loss the required L is roughly invariant over a broad range of α, ξ, which suggests that QDS-f is robust to experimental differences. Thus, it is easier to implement on an agile system alongside further alternative cryptographic protocols which may require a more restrictive choice of α. For large channel loss however, the choice of α becomes increasingly important, but using for example the mean $\alpha = 0.55$ and $\xi = 2.1\%$ from experimental run 3, QDS-f is predicted to remain secure even down to 20 dB loss with still-feasible signature lengths $\mathcal{O}\left(10^9\right)$. On our system this would allow a one-bit message to be signed in approximately one second.

A more realistic signature length may be calculated by using the p_{err} directly from Rx output, which includes all noise sources and detector

inefficiencies, and by using the models from Sec. 5.6.1 to take into account realistic coherent state amplitudes and sending probabilities. This results in larger signature lengths which are displayed in Tab. 5.2. Crucially, they remain highly feasible over the metropolitan distances where continuous-variable cryptography is expected to be effective. Of particular note is the $L = 47,887$ required to securely sign a 1 bit message over 2 km fiber, which to our knowledge makes QDS f the fastest ever demonstration of a QDS protocol, requiring just 0.047 ms to sign a message at our 1 GHz sending rate, Fig. 5.14.

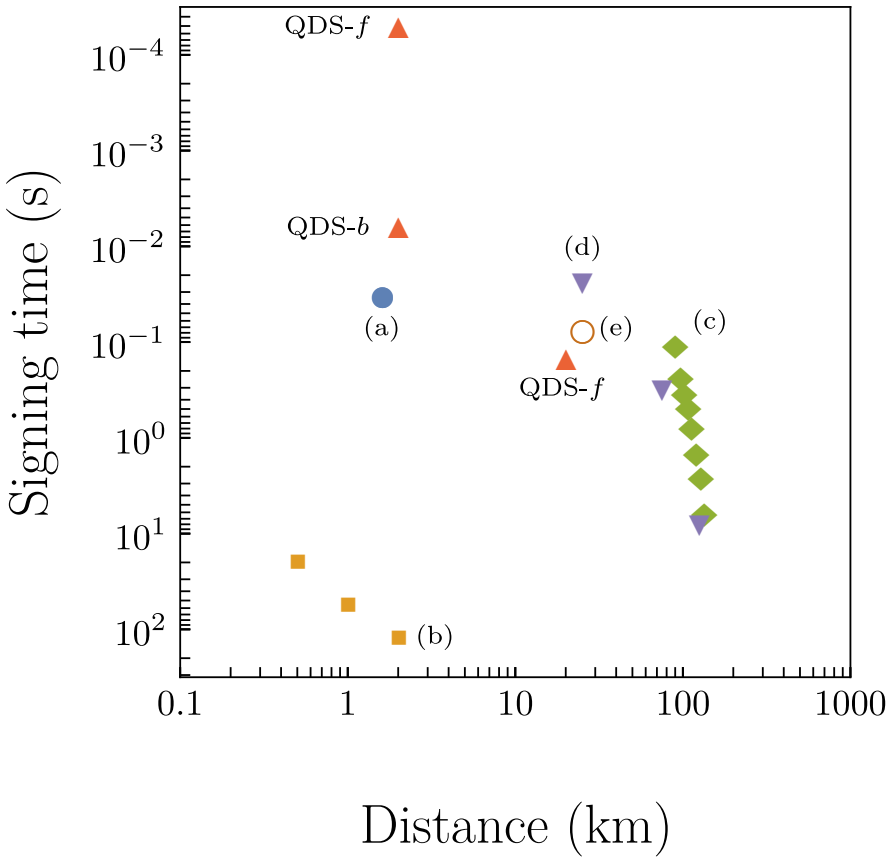


Figure 5.14: Time required to sign a one-bit message, and the corresponding channel lengths, for several recent QDS protocols. At the short distnaces (~ 2 km) favoured by the continuous-variable platform, our QDS-f and QDS-b protocols allow for signing times of less than 0.05 ms and 6 ms, respectively, improving on previous results in CV (a) and discrete-variable (DV) (b) systems. At 20 km, QDS-f has a signing time comparable to recent DV QDS systems (c)-(e). Protocols depicted: red triangles - QDS-b and QDS-f from this chapter and Ref. [163]. (a) Free-space CV QDS [73]. (b) Unambiguous-state-elimination-based QDS [46]. (c) Differential-phase-shift-based QDS [66]. (d) GHz BB84 QDS [56]. (e) Early QDS-QKD "agile" system with measurement-device-independent capabilities [65].

The calculated maximum secure key rates under protocol QKD-f are plotted in Fig. 5.15 under attack BS2. The performance of this protocol agrees with Ref. [137] over comparable parameter regimes (when we analyse under the BS0 and EC attacks considered in that Paper), while the QPSK amplitudes employed in our experiment are much closer to optimal. Calculated maximum key rates, deduced from experimental parameters with models Sec. 5.6.1, are displayed in Tab. 5.2.

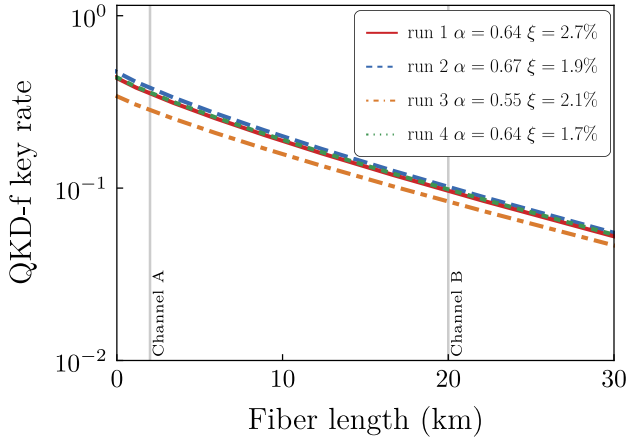


Figure 5.15: Calculated maximum attainable key rates for protocol QKD-f. The predicted key rates agree with Ref. [137] over equivalent parameters, while the key rates displayed here are close to optimal. Vertical grid lines denote loss levels over experimental channels A and B, corresponding to fiber lengths 2 km (0.65 dB loss) and 20 km (4.75 dB loss), respectively. Solid (red), dashed (blue), dot-dashed (orange) and dotted (green) lines correspond to experimental runs 1, 2, 3 and 4, respectively.

Our second agile system QDS-f-QKD-f-CV-QPSK is able to perform QDS and QKD tasks which differ only in classical postprocessing. Our key figure of merit for this system is the smallest time, 0.047 ms, to sign a 1 bit message over 2 km. This time is much smaller than for comparable protocols, and is due in part to the technological maturity and speed of our CV experiment, and in part to the fact that for QDS-f Alice uses different sequences of coherent states for each recipient (c.f. Ch. 3). Our inclusion of protocol QKD-f which exists already in the literature, and which has been extensively analysed [96, 137, 141, 143], demonstrates that existing protocols may be united in an agile platform.

5.7 OUTLOOK

We have observed efficient performance of each of our cryptographic protocols, QDS-b, QSS-b, QDS-f and QKD-f, when key rates and signature lengths are estimated from the experimental data. Crucially, the experiment detailed in Sec. 5.5 is performed without reference

to any particular protocol and so the experimental hardware layer of Fig. 5.2 is agnostic to the application for which it is being used. Therefore, each system QDS-b-QSS-b-CV-QPSK, QDS-f-QKD-f-CV-QPSK may accurately be denoted "agile".

The clear separation of hardware layers from the software layer which selects the desired task is beneficial for practical implementation, and we believe that an agile middleware which enforces the separation will function analogously to the quantum compilers recently investigated in the context of quantum computing [166–168]. Future quantum cryptographic protocols should be designed and optimized towards agility, and it should be possible to group additional existing cryptosystems into further agile systems for implementation.

The QDS protocols which we have investigated outperform their nearest competitors and allow for messages to be securely signed in (to our knowledge) the fastest observed times: less than 6 ms for QDS-b and less than 0.05 ms for QDS-f. The trade-off of requiring short distances is not a huge one, since it has long been accepted [76] that continuous-variables cryptography boasting very high key rates and sending rates should be used for intra-city communication over distances the order of kilometers, while discrete-variables cryptography should be preferred for long-distance quantum communication. Moreover, our QSS-b protocol is shown to require fewer quantum resources than an equivalent task accomplished via classical unconditionally secure secret sharing performed over pairwise encrypted QKD channels.

For our demonstrations, we have used experimental hardware which is almost entirely commercially available and is inherently compatible with existing classical communications infrastructure. In the future, this may render it possible to allow for quantum communications protocols to be performed over installed fibers with existing receivers, e.g. a home router, requiring merely an upgrade to their firmware. Our experiment was performed with a sending rate of 1 GHz, but with similar hardware it is even possible to reach tens or hundreds of GHz [170, 171], which would both improve the performance of our protocols, and make a practical eavesdropping attack increasingly difficult to perform.

It is important to note that while the security techniques used here mirror the state-of-the-art techniques available for analysing e.g. QKD [137] over similar setups, the requirement for QPSK states and heterodyne detection has proven restrictive to the amount of noise allowable on the channel under different attacks [146, 147]. Under EC attacks, protocols QDS-f, QSS-b and QKD-f remain insecure over the channels investigated, precisely because of the high level of excess noise ξ, which in a full treatment must be attributed to the eavesdropper. These protocols were therefore analysed in a "trusted-noise" model, BS2, in which excess noise adversely affects honest players, but cannot

be exploited by an eavesdropper. We believe that because of the high sending rates used in this experiment, and because of the the unknown (but assumed non-Gaussian) measurement which Eve performs in attack BS2, that the protocols still retain a high practical level of security, albeit technically not unconditional to all possible attacks. Future work should therefore endeavour to improve the security attainable for quantum cryptosystems relying on QPSK alphabet, and to improve the level of security proof for alphabets of coherent states modulated with a non-Gaussian distribution.

Part II

PHOG: GENERATION OF SUB-POISSONIAN LIGHT

6

PHOG: PHOTON GUN

In this chapter we introduce and model a device which aims to be a deterministic source of highly non-classical light. The device, which we call *PhoG* ("sub-Poissonian Photon Gun"), uses engineered dissipation to implement a so-called Nonlinear Coherent Loss (NCL), the steady state of which is a single-photon state. We first explore the properties of decay into a Markovian reservoir of an initial coherent state in a single-mode model, which involves one bosonic mode and a reservoir, Sec. 6.2. We explore the forms of dissipation required to deterministically generate useful quantum outputs, and show that although the ever-present linear (single-photon) loss prevents us from reaching perfect single-photon states, it is still possible to deterministically reach output states which are highly squeezed in photon number Sec. 6.3. These so-called sub-Poissonian states are obtained over the initial stages of the dynamics which is dominated by NCL and practically unaffected by linear loss. We then demonstrate that the NCL may be effectively realised by more complicated models involving multiple bosonic modes and the regular Kerr nonlinearity, Secs. 6.4-6.6. The desired state is created in "signal" modes which are not directly coupled to each other, and interact only dissipatively via coupling to a shared reservoir, which may be simulated by a long "tail" of further modes. Finally, we demonstrate that a modification in the coupling ratio between waveguides can lead to a device which will generate quadrature entanglement between modes. Since our proposed device takes merely a coherent state input, it should prove to be a cheap and flexible source of quantum sub-Poissonian and entangled states.

6.1 INTRODUCTION

Engineered loss has, in recent years, become a powerful tool and an intensely researched field of quantum physics. Rather than simply being an enemy of the quantum state and its applications, controlled dissipation can be a helpful ally for generation, protection, and application of quantum phenomena. Furthermore, there has been renewed interest in engineered and non-standard loss mechanisms for the potential to explore new regimes of physics in which unitary and non-unitary dynamics compete or balance [176, 177]. For example, in Refs. [178–181] dissipation is used both to generate quantum entanglement and dissipation can even protect it [182]. Ref. [180] provides a scheme in which entanglement is generated between atoms held in distant cavities which interact solely via dissipation, while Ref. [183] allows

for entanglement generation and stabilization against decay in systems of superconducting qubits.

The recent work by Cammack *et. al.* [184] demonstrates that dissipation can help prevent decoherence. Their work involves a nuclear spin coupled to an electron spin, which is then coupled to a reservoir. By exploiting a difference in characteristic system timescales it is possible to protect the nuclear spin against decoherence and thereby increase the length of time it remains in a superposition state. Remarkably, in this setup an increase in the reservoir temperature further protects coherence. In this Chapter we similarly exploit a separation of timescales, and we discuss this further in Sec. 6.4.

Dissipation can generate superposition states, for example the Ref. [185] proposes a dissipative scheme in which two-photon absorption drives a quantum state towards the Schrödinger cat superposition state, and confines the total quantum state to states close to their output state. Dissipation is even found to be useful for computation. In Ref. [186], Verstrate *et. al.* describe how discrete systems, coupled only locally to a set of reservoirs, can allow for universal quantum computation even when the system undergoes no coherent dynamics.

The use of dissipation to enact coupling between modes also has a long history. For example, in Braun *et. al.* [179] two modes coupled to the same Markovian reservoir are led to interact with each other through their correlated loss, and can generate entanglement. Such dissipative coupling may also be used to transport quantum states between separate modes in Refs. [187–191]. In Ref. [189], for example, it was found that dissipation can increase the rate at which a quantum state is transferred, and that dissipation can open up new types of transfer, for example between stationary eigenstates. Their scheme is particularly interesting and relevant for our work since they rely on networks of integrated waveguides. Interestingly, it is thought that such dissipatively coupled networks as Ref. [189] may even assist biological processes in nature.

6.1.1 *Engineering the loss*

A key requirement for enacting such dissipation-assisted protocols is that one should have precise control over both coherent and dissipative dynamics, and the system should possess the desired (engineered) dissipation while being relatively isolated from unwanted loss sources. Cavity QED has proven a useful platform [180], as have trapped ions [192, 193] which can allow for fine-tuning for master-equation simulation. Superconducting circuits may be another useful platform for precise and stable entanglement generation, quantum simulation and quantum error correction for computation [183, 194].

6.1.2 *Integrated photonic waveguides*

Each of the above systems allows for precisely controlled coupling strengths and interaction times, and crucially they allow for high effective nonlinearities to be realised. In photonic systems this is more difficult. While integrated photonic waveguides have proven useful for enacting tight-binding networks of modes, and therefore for simulating solid-state systems [195, 196], the glasses typically used have small nonlinearities and large linear (single-photon) loss. Larger effective nonlinearities can normally be obtained by choosing ultrashort pulses or by reducing the effective fiber mode area [169, 197], but this may lead to other problems of confinement or higher-order dispersion processes.

Despite these issues, integrated waveguides have recently become an exciting platform with which to marry unitary and non-unitary couplings between bosonic modes, and to use these to explore interesting quantum effects. For example, recent works Refs. [195, 196] exploit collective (nonlocal) losses on the system in order to simulate a solid-state flat-band (dispersion free) state, while the integrated-waveguide platform itself allows for precise control over coupling length and strength. In any case, the generated state in Ref. [195] was found to be robust to such imperfections. Such a system may be useful for long-distance communication since it is in principle capable of propagation without dispersion.

The recent work by Mukherjee *et. al.* [198] implements a chain of dissipatively coupled waveguides, and finds that the system acts as an effective equalizer of an input quantum state. The coupling to a common reservoir smooths out phase and amplitude fluctuations in the input state. The simultaneous action of both coherent unitary dynamics and diffusive non-unitary dynamics lead the authors to coin the term "Coherent Diffusive Photonics" to describe photonic systems in which both unitary and diffusive action plays a key role. In the paper it was also demonstrated that the CDP platform was very robust to imperfections in both coupling strength and effective coupling length.

6.1.3 *Our contribution: Coherent Diffusive Photonics for quantum state generation*

In this Chapter, our aim is to take the CDP platform, which consists of linear coupling and strong dissipation in an integrated waveguide network, and add nonlinear effects. We shall see that adding the Kerr nonlinearity, present in $\chi^{(3)}$ glasses for example, allows our CDP network to function as a deterministic generator of highly desirable quantum properties such as entanglement, photon-number squeezing and, in the ideal limit, single-photons. Our system, which we call a

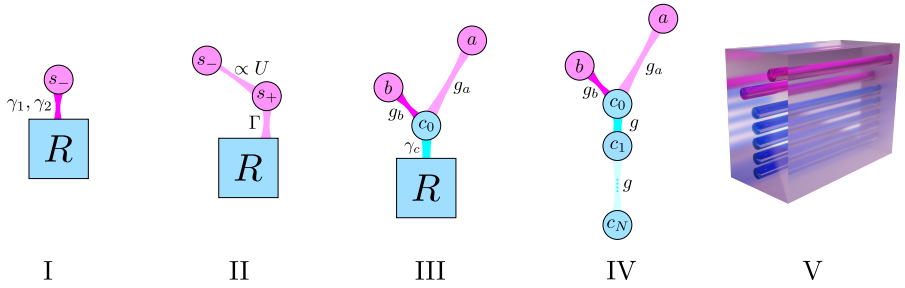


Figure 6.1: Hierarchy of models of the PhoG device, from principal basic model (left) to waveguide array of modes for implementation (right). We will discuss each model and relationships between them throughout the rest of this chapter. I: Single-mode model. II: Two-mode model. III: Three-mode model. IV: Multi-mode model. V Multi-mode model embedded in glass.

PhoG (Photon Gun) device, is thus a passive[1] system which is able to create highly non-classical output from a coherent state input.

Our ultimate goal in this chapter is to model a full PhoG system consisting of a network of integrated waveguides, laser-inscribed into IG2 glass [199], Fig. 6.1 V. The network geometry which we build up to is displayed in Fig. 6.1 IV, and consists of two "signal" modes (pink) coupled to each other only vicariously via a long "tail" structure (blue) of further modes. This tail effectively simulates a reservoir over short times. In order to gain traction and insight into our system we will initially consider simpler models of increasing complexity (Fig. 6.1, I, II, III), which each explicitly consider a Markovian reservoir R. We will explore key effects first under the single-mode model (Fig. 6.1 I, Sec. 6.2) which relies on an exotic form of loss called Nonlinear Coherent Loss (NCL). This single-mode model will prove illustrative, and is a foundational building block to which we will compare our more complicated models.

After demonstrating that the single-mode model with NCL suitably allows for our desired states at the output, we will then show how this model may be simulated using standard linear loss, linear coupling between modes, and Kerr nonlinearity, Sec. 6.4. The presence of linear loss on additional modes of the system will cause our ideal single-photon output state to decay to vacuum. Despite this, strongly photon-number squeezed light is still attainable if we restrict ourselves to short evolution times.

The requisite nonlinearity may be introduced into a real physical system by building our device in laser-inscribed waveguides in a $\chi^{(3)}$ glass, and with a future experiment in view we explore the relevant parameters in Sec. 6.5. In Sec. 6.6 we show that even these realistic parameters – low nonlinearity and high linear loss – are suitable to allow generation of highly sub-Poissonian output. With an experiment

1 In the sense that it requires no driving.

in mind we replace the Markovian reservoir with a long "tail" of further bosonic modes, which effectively simulates the reservoir over the short timescales of interest, and in Sec. 6.6 we show that this multi-mode model including realistic glass parameters is still capable to create a bright output state which is strongly squeezed in photon-number.

Finally, in Sec. 6.7 we show that tweaking the coupling ratio between the modes of our device can lead us to a different form of output state, and so the PhoG device can also be a deterministic source of entangled photons. We conclude in Sec. 6.8 with a short discussion of how the output of PhoG may be used, and an outline of necessary future work.

Throughout the Chapter we will use several different numerical methods to model the PhoG device. The two key methods – direct integration of the master equation, and quantum Monte Carlo – are discussed in Appendix E, and a comparison between the efficiency and utility of the methods is made there. Throughout the Chapter we will indicate when either of these methods has been used to generate specific results.

6.2 SINGLE-MODE MODEL

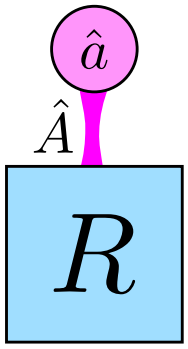


Figure 6.2: A single bosonic mode, a, decays into a Markovian reservoir R by decay operator $\hat{A}$.

Consider the single-mode model displayed in Fig. 6.2 (c.f. Fig. 6.1 I), which consists of a single bosonic mode, a, decaying into a reservoir R via operator $\hat{A}$. The annihilation (creation) operator for mode a is $\hat{a}$ $(\hat{a}^\dagger)$, and the density matrix[2] containing all information about the state of the mode is $\hat{\rho}_a$. This model will prove illustrative of several principles which we will develop throughout the chapter.

2 As discussed in Sec. 1.2.1, the density operator $\hat{\rho}$ is completely described by its equivalent density matrix ρ, and so we will not distinguish between $\hat{\rho}$ and ρ. It should be understood that the state ρ is an operator which admits a matrix representation. This will prove useful for modelling, Appendix E.

Assuming that reservoir R is Markovian, the evolution of mode a is given by the following quantum master equation in Lindblad form [15, 200]:

$$\frac{d}{dt}\rho_a = -i\left[\hat{H}, \rho_a\right] + \gamma\mathcal{L}\left[\hat{A}\right]\rho_a \tag{6.1}$$

where we take the Hamiltonian $\hat{H} = \omega\hat{a}^\dagger\hat{a}$ ($\hbar = 1$). Equation 6.1 then describes the decay of an initial state $\rho_a(t=0)$ into R with rate γ. The Lindbladian term $\mathcal{L}\left[\hat{A}\right]$ takes the usual form

$$\mathcal{L}\left[\hat{A}\right]\rho_a = \hat{A}\rho_a\hat{A}^\dagger - \frac{1}{2}\hat{A}^\dagger\hat{A}\rho_a - \frac{1}{2}\rho_a\hat{A}^\dagger\hat{A}. \tag{6.2}$$

In the remainder of this section, we examine the behaviour of an initially coherent state, $\rho_a(t=0) = |\alpha\rangle\langle\alpha|$ with amplitude α, as it decays into R. We examine several choices for decay operator $\hat{A}$ and demonstrate that suitable choices of $\hat{A}$ drive ρ_a towards highly non-classical output steady-states. In Sec. 6.2.1 we let $\hat{A} = \hat{a}$, in Sec. 6.2.2 we let $\hat{A} = \hat{a}^2$, and in Sec. 6.2.3 we examine the behaviour of decay operators of the form $\hat{A} = \hat{a}\left(\hat{a}^\dagger\hat{a} - p\right)$ for $p \in \mathbb{N}$.

6.2.1 $\hat{A} = \hat{a}$

First, we consider the case $\hat{A} = \hat{a}$, which corresponds to a single-photon loss with constant rate, which we denote γ. The evolution of ρ_a is described by

$$\frac{d}{dt}\rho_a = \gamma\left[\hat{a}\rho_a\hat{a}^\dagger - \frac{1}{2}\hat{a}^\dagger\hat{a}\rho_a - \frac{1}{2}\rho_a\hat{a}^\dagger\hat{a}\right], \tag{6.3}$$

where for convenience we have implicitly transformed into a rotating frame so the free Hamiltonian term $\omega\hat{a}^\dagger\hat{a}$ vanishes. Let us calculate the evolution of photon number expectation value $\langle\hat{a}^\dagger\hat{a}\rangle(t)$:

$$\begin{aligned}\frac{d}{dt}\langle\hat{a}^\dagger\hat{a}\rangle &= \gamma\left[\mathrm{Tr}\left(\hat{a}^\dagger\hat{a}\hat{a}\rho_a\hat{a}^\dagger\right) - \frac{1}{2}\mathrm{Tr}\left(\hat{a}^\dagger\hat{a}\hat{a}^\dagger\hat{a}\rho_a\right) - \frac{1}{2}\mathrm{Tr}\left(\hat{a}^\dagger\hat{a}\rho_a\hat{a}^\dagger\hat{a}\right)\right] \\ &= \gamma\left[\langle\hat{a}^\dagger\hat{a}^\dagger\hat{a}\hat{a}\rangle - \langle\hat{a}^\dagger\hat{a}\hat{a}^\dagger\hat{a}\rangle\right] \\ &= -\gamma\langle\hat{a}^\dagger\hat{a}\rangle \end{aligned} \tag{6.4}$$

and so

$$\langle\hat{a}^\dagger\hat{a}\rangle(t) = \langle\hat{a}^\dagger\hat{a}\rangle(0)\, e^{-\gamma t}. \tag{6.5}$$

The photon number exponentially decays in time with decay rate γ from its initial value. We may derive similar equations for quadrature expectations $\langle\hat{x}\rangle(t)$ and $\langle\hat{p}\rangle(t)$ and also find

$$\begin{aligned}\langle\hat{x}\rangle(t) &= \langle\hat{x}\rangle(0)\, e^{-\frac{\gamma}{2}t} \\ \langle\hat{p}\rangle(t) &= \langle\hat{p}\rangle(0)\, e^{-\frac{\gamma}{2}t}.\end{aligned} \tag{6.6}$$

Since each of these is exponentially decaying to zero, we might guess that the steady-state of Eq. 6.3 is the vacuum $|0\rangle\langle 0|$, and indeed we can deduce that this must be the case by noticing that $\frac{d}{dt}\rho_a = 0$ when ρ_a is vacuum. In Fig. 6.3a we plot the evolution of $\langle \hat{a}^\dagger \hat{a} \rangle, \langle \hat{x} \rangle, \langle \hat{p} \rangle$ which decay towards zero, while the variances in $\hat{x}$ and $\hat{p}$ remain constant throughout the evolution. This hints that the state $\rho_a(t)$ remains a coherent state with decreasing amplitude $\alpha \to 0$, until it reaches the vacuum state.

In Fig. 6.3b we plot the fidelities $\mathcal{F}$ between $\rho_a(t)$ and both the vacuum state $|0\rangle\langle 0|$ and the single-photon state $|1\rangle\langle 1|$. We also show fidelity between $\rho_a(t)$ and a coherent state $|\alpha'\rangle\langle\alpha'|$, which is defined to have the same photon-number expectation as ρ_a at all times. We observe that the fidelity to the vacuum state increases to 1 while the fidelity to coherent state $|\alpha'\rangle\langle\alpha'| = 1$ always. This confirms our intuition that ρ_a remains coherent $\forall t$ and that $|0\rangle\langle 0|$ is the steady state.

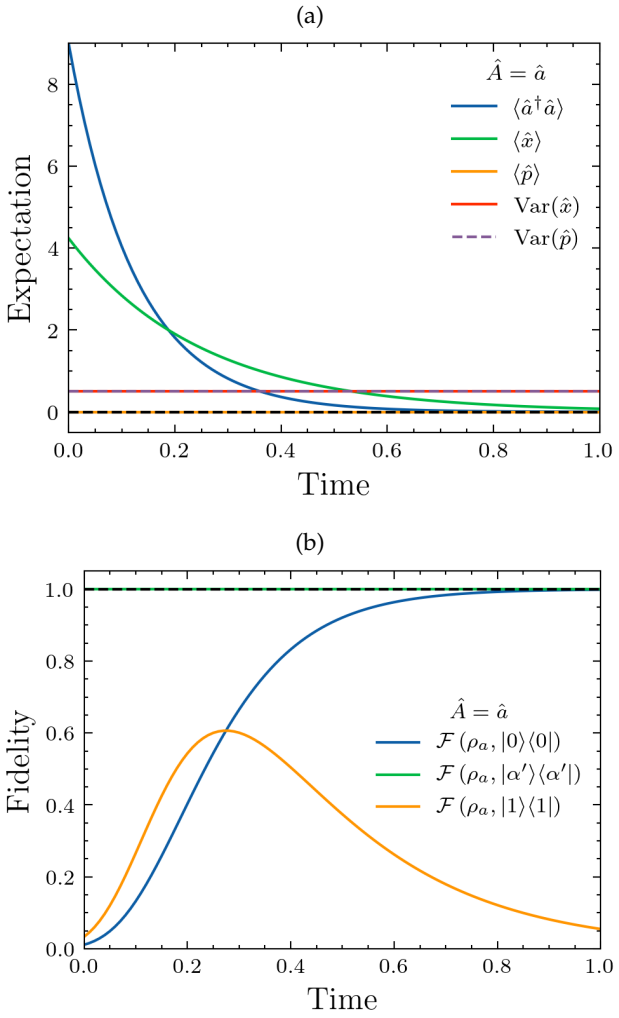


Figure 6.3: $\hat{A} = \hat{a}$. (a) Operator expectation values calculated for state $\rho_a(t)$ as it evolves under master equation 6.3. An initial coherent state with $\alpha = 3.0$ decays to vacuum state $|0\rangle\langle 0|$. Quadrature variances remain constant through time, implying that ρ_a remains a coherent state throughout its evolution. This is confirmed in (b) where the fidelity between ρ_a and $|\alpha'\rangle\langle\alpha'|$ is demonstrated to remain 1 for all time, while the fidelity to the vacuum state increases to 1. The amplitude α' is chosen to give a coherent state with equivalent photon-number expectation to $\rho_a(t)$. Horizontal gridlines are displayed in black, dashed. Numerical method: direct integration.

6.2.2 $\hat{A} = \hat{a}^2$

Next we consider a decay term $\hat{a}^2$, which describes two-photon loss into the reservoir. Two photon absorption has been extensively studied, for example in the context of light coupled to a non-interacting atomic gas [201–204], for which the concepts of antibunched light were first realised [205, 206]. The Lindblad equation describing two photon absorption is

$$\frac{d}{dt}\rho_a = \gamma\left[\hat{a}^2\rho_a\hat{a}^{\dagger 2} - \frac{1}{2}\hat{a}^{\dagger 2}\hat{a}^2\rho_a - \frac{1}{2}\rho\hat{a}^{\dagger 2}\hat{a}^2\right], \tag{6.7}$$

which gives the evolution of photon number expectation as

$$\frac{d}{dt}\langle\hat{a}^\dagger\hat{a}\rangle = -2\gamma\langle\hat{a}^\dagger\hat{a}^\dagger\hat{a}\hat{a}\rangle. \tag{6.8}$$

This equation does not take a closed form, and so we cannot yet directly calculate $\langle\hat{a}^\dagger\hat{a}\rangle(t)$ [201]. Similarly, equations for evolution of $\langle\hat{a}\rangle(t)$ require terms to the third power in $\hat{a}, \hat{a}^\dagger$, and so are also not yet closed. We will encounter some linearization techniques later in Sec. 6.6.2 which allow us to deal with this.

For now, let us try to deduce the steady-state of Eq. 6.7 when we begin with coherent state $|\alpha\rangle$. We observe that once again the vacuum $|0\rangle\langle 0|$ must be a steady state, since then $\frac{d}{dt}\rho_a = 0$. Surprisingly we now also have the single-photon state $|1\rangle\langle 1|$, and states of the form $|0\rangle\langle 1|, |1\rangle\langle 0|$ as steady states, since these also have $\frac{d}{dt}\rho_a = 0$. The general steady-state should be a mixture of these, and takes the form

$$\begin{aligned}\rho_{\text{steady}} &= c_1|\psi\rangle\langle\psi| + c_2|0\rangle\langle 0| + c_3|1\rangle\langle 1| \\ \text{with}\quad |\psi\rangle &= \frac{|0\rangle + e^{i\phi}|1\rangle}{\sqrt{2}}; \qquad c_1, c_2, c_3 \in \mathbb{C}.\end{aligned} \tag{6.9}$$

The state $|\psi\rangle$ is a so-called *phase-state*, and it has long been known that two-photon absorption will lead to a phase state [207] (plus additional mixing [208, 209] which reduces purity). The phase ϕ is related to the phase of the initial coherent state.

It turns out that a full analytic solution of the master equation 6.7 is possible [203, 207, 209] when, instead of calculating the evolution of expectations $\langle\hat{a}\rangle, \langle\hat{a}^\dagger\hat{a}\rangle$, we focus on direct solution in terms of $\rho_{n,m} = \langle m|\rho|n\rangle$. This is the approach taken by Simaan and Loudon in Refs. [203], and picked up again by the Yamamoto group in Ref. [207].

In the Fock basis, Eq. 6.7 may be rewritten as

$$\begin{aligned}\frac{d}{dt}\rho_{n,m} =& \gamma\left[(n+1)(n+2)(m+1)(m+2)\right]^{1/2}\rho_{n+2,m+2} \\ &- \frac{\gamma}{2}\left[n(n-1) + m(m-1)\right]\rho_{n,m}\end{aligned} \tag{6.10}$$

for all n, m.

The derivation now relies on the fact that the two-photon absorption operator $\hat{a}^2$ partitions the full Hilbert space into two separate subspaces, depending on whether the state contains an odd or an even number of photons. In other words, odd Fock basis elements couple only to odd Fock basis elements, and likewise for even Fock basis elements.

Operator $\hat{a}^2$ corresponds to photon subtracton, and can act on every $|n\rangle$ *except* $|0\rangle$ and $|1\rangle$: we have already seen that these must correspond to the steady state of the system. Considering only diagonal elements $\rho_{n,n}$, and noting that Eq. 6.10 couples diagonal elements only to diagonal elements, we deduce that

$$\rho_{0,0}(t\to\infty) = \sum_{n \text{ even}} \rho_{n,n}(t=0)$$
$$\rho_{1,1}(t\to\infty) = \sum_{n \text{ odd}} \rho_{n,n}(t=0)$$

Indeed, this is true more generally than just Eq. 6.7, and also occurs for dissipative coupling via $\hat{a}^2$ to a reservoir at finite temperature in which pairs of photons can be absorbed from the bath into system ρ_a [203]. When the initial state $\rho_a(t=0)$ is a bright coherent state $|\alpha\rangle\langle\alpha|$ with $\alpha = |\alpha| e^{i\phi}$ both $\rho_{0,0}$ and $\rho_{1,1}$ take the value 0.5 in the steady state.

What about the coherences $\rho_{0,1}, \rho_{1,0}$? We may return to Eq. 6.10 and apply an argument described in Ref. [204]. Let us rewrite $\rho_{n,m}(t) = \rho_{n,n+\mu}(t)$ where $\mu \in \mathbb{N} > 0$ measures the distance between the matrix element and the diagonal[3]. Because the operator $\hat{a}^2$ can only subtract two photons at a time, μ is preserved during the evolution, which we can see if we define the matrix element $\Theta_n(\mu, t)$ as

$$\rho_{n,n+\mu}(t) = \frac{n!}{(n+\mu)!}^{1/2} \Theta_n(\mu, t), \tag{6.11}$$

where the prefactor has been chosen to cancel with terms from Eq. 6.10. Therefore

$$\frac{d}{dt}\Theta_n(\mu,t) = \gamma(n+1)(n+2)\Theta_{n+2}(\mu,t) - \gamma\left[n(n-1) + \mu n + \frac{1}{2}\mu(\mu-1)\right]\Theta_n(\mu,t). \tag{6.12}$$

and in the steady state we may set the left hand side of this equation to zero. We have seen already that in the steady state the only nonzero coherence element must be $\Theta_0(1,\infty)$. In this case we may derive

$$\frac{d}{dt}\sum_{n \text{ even}} = \left[\frac{n!}{2^n\left(\left(\frac{1}{2}n\right)!\right)^2}\right]\Theta_n(1,t) = 0, \tag{6.13}$$

3 For elements on the other side of the diagonal, i.e. those requiring $m < n$, we note that $\rho_{n,n-\mu}$ is the complex conjugate of $\rho_{n,n+\mu}$

so this weighted sum of elements one position above the diagonal is unchanged by $\hat{a}^2$. Therefore, our nonzero coherence in the steady state may be written as

$$\Theta_n(1,\infty) = \sum_{n \text{ even}} \left[\frac{n!}{2^n \left(\left(\frac{1}{2}n\right)! \right)^2} \right] \Theta_n(1,0). \tag{6.14}$$

Considering again the specific example of a coherent state input, Eq. 6.14 simplifies to

$$\rho_{0,1}(\infty) = |\alpha|^2 \exp\left(-|\alpha|^2 - i\phi\right) I_0\left(|\alpha|^2\right) \tag{6.15}$$

where $I_0(x)$ is the modified Bessel function of the first kind [210]. In the limit of a bright coherent state input, Eq. 6.15 reduces to [204, 209]

$$\rho_{0,1}(\infty) = \frac{\exp(-i\phi)}{\sqrt{2\pi}} \tag{6.16}$$

which is approximately 0.399 for real $\alpha \gg 1$. For an input $\alpha = 3.0$, we arrive at $\rho_{0,1}(\infty) = 0.405$.

In Fig. 6.4a we plot the numeric evolution of $\langle \hat{a}^\dagger \hat{a} \rangle, \langle \hat{x} \rangle, \langle \hat{p} \rangle$ and the quadrature variances. The photon number expectation no longer decays to zero as it did for $\hat{A} = \hat{a}$. In Fig. 6.4b we observe the fidelity between $\rho_a(t)$ and the final steady-state increases to 1, and the coefficients of the steady state ρ_{steady} in Eq. 6.9 are $c_1 = 0.810$, $c_2 = c_3 = 0.095$, or in other words $\rho_{0,0} = \rho_{1,1} = 0.5$ and $\rho_{0,1} = \rho_{1,0} = 0.405$. This agrees with the analytical derivation based on Refs. [203, 204, 207, 209]. Our numerics thus confirm that two-photon loss operator induces a high degree of non-classicality in the system. We shall revisit this decay operator $\hat{a}^2$ in Sec. 6.7 where we will demonstrate that it is even capable of producing entanglement between spatially separated modes of a larger system.

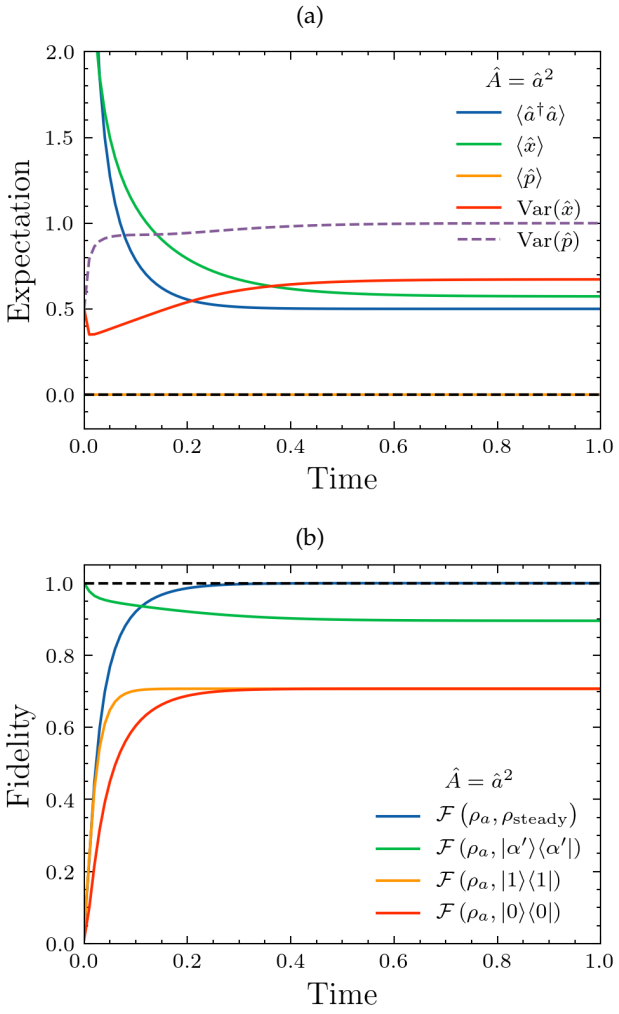


Figure 6.4: $\hat{A} = \hat{a}^2$. (a) Operator expectation values for state $\rho_a(t)$ as it evolves under Eq. 6.7. Unlike Fig. 6.3, an intially coherent state with $\alpha = 3.0$ no longer decays to the vacuum state, and the final photon-number expectation is 0.5. Quadrature variances no longer stay constant, which implies that the state is no longer a coherent state. This is confirmed in (b) where the fidelity between $\rho_a(t)$ and $|\alpha'\rangle\langle\alpha'|$ is plotted. The fidelity between $\rho_a(t)$ and steady state Eq. 6.9 increases to 1. Horizontal gridlines are displayed in black, dashed. Numerical method: direct integration.

6.2.3 $\hat{A} = \hat{a}\left(\hat{a}^\dagger\hat{a} - 1\right)$

We have seen that the choice of $\hat{A}$ can give drastically different steady states of ρ_a, from the uninteresting vacuum to the highly quantum phase-state. We therefore wish to consider which choices for $\hat{A}$ will drive an initially coherent state to a Fock state $|n\rangle\langle n|$.

The choice

$$\hat{A} = \hat{a}\left(\hat{a}^\dagger\hat{a} - 1\right) \tag{6.17}$$

may be interpreted as a single-photon loss at a rate which depends on photon number $\hat{n} = \hat{a}^\dagger\hat{a}$. The loss rate will go to zero when applied to state $|1\rangle\langle 1|$, and so we may suspect that the single-photon state $|1\rangle\langle 1|$ is a steady state of this loss mechanism.

The Lindblad equation which we solve is

$$\frac{d}{dt}\rho_a = \gamma\left[\hat{a}\,(\hat{n}-1)\,\rho\,(\hat{n}-1)\,\hat{a}^\dagger - \frac{1}{2}\rho\,(\hat{n}-1)\,\hat{n}\,(\hat{n}-1) - \frac{1}{2}\,(\hat{n}-1)\,\hat{n}\,(\hat{n}-1)\,\rho\right]. \tag{6.18}$$

We examine the evolution of ρ_a in Fig. 6.5 and plot the evolution of photon number and quadrature expectations $\langle\hat{x}\rangle$, $\langle\hat{p}\rangle$ in (a). We observe a non-exponential decay of photon-number expectation to 1, while in (b) the fidelity between $\rho_a(t)$ and $|1\rangle\langle 1|$ increases to 1. This choice of $\hat{A} = \hat{a}\left(\hat{a}^\dagger\hat{a} - 1\right)$ does indeed have a single-photon steady state.

Even after short times $t < 0.1$ the fidelity to an equivalent coherent state has rapidly decreased, and the quadrature variances sharply increase over similar timescale. This implies a rapid increase in non-classicality of the system, which we shall explore and quantify later.

We deduce that the decay operator $\hat{a}\left(\hat{a}^\dagger\hat{a} - 1\right)$ is a useful candidate for driving our system towards the highly nonclassical single-photon state. In the remainder of this Chapter our goal will be to find a physical system which can efficiently implement this decay operator.

To gain some insight into the action of $\hat{a}\left(\hat{a}^\dagger\hat{a} - 1\right)$, let us first write the Lindblad equation 6.18 in Fock basis for density matrix element $\rho_{m,n}$

$$\begin{aligned}\frac{d}{dt}\rho_{m,n} &= \langle m|\frac{d}{dt}\rho|n\rangle \\ &= \gamma\left[m\sqrt{m+1}n\sqrt{n+1}\,\rho_{m+1,n+1} - \frac{1}{2}(n-1)^2\,n\,\rho_{m,n} - \frac{1}{2}(m-1)^2\,m\,\rho_{m,n}\right],\end{aligned} \tag{6.19}$$

and consider some specific matrix elements. Immediately we see that Eq. 6.19 couples diagonal elements $m = n$ only to diagonal elements and so an analysis of the photon-number statistics is possible by only considering the diagonal elements. We obtain, for example $\frac{d}{dt}\rho_{1,1} = 2\gamma\rho_{2,2}$ which is greater than zero, and so $\forall t$ we expect the single-photon contribution $\rho_{1,1}$ to monotonically increase, c.f. Fig. 6.5b. The elements $\rho_{0,0}$, $\rho_{0,1}$ and $\rho_{1,0}$ each give

$$\frac{d}{dt}\rho_{0,0} = 0, \qquad \frac{d}{dt}\rho_{0,1} = 0, \quad \text{and} \quad \frac{d}{dt}\rho_{1,0} = 0, \tag{6.20}$$

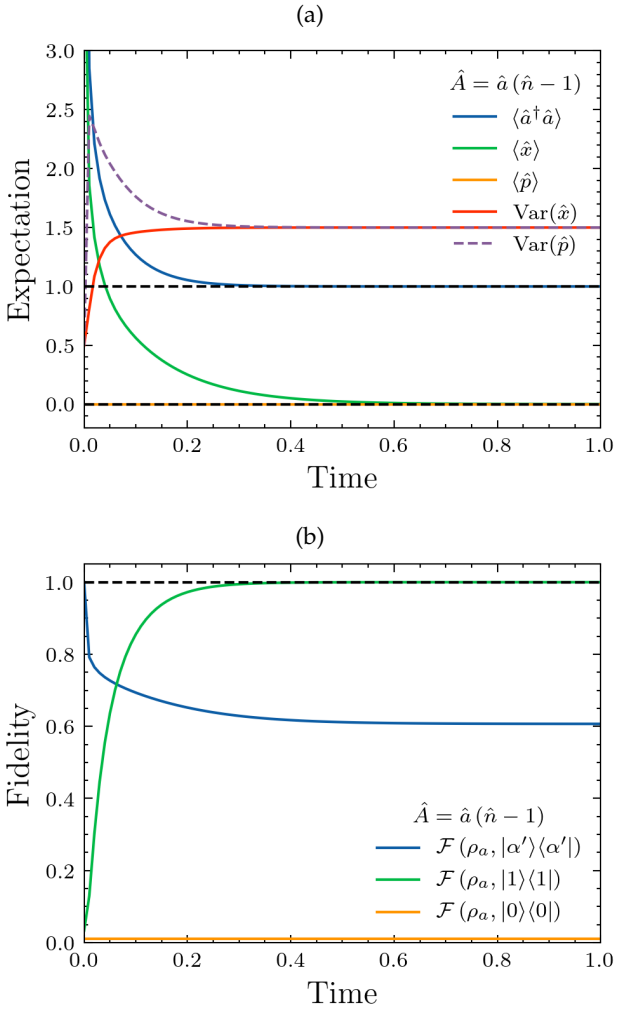


Figure 6.5: $\hat{A} = \hat{a}\left(\hat{a}^\dagger \hat{a} - 1\right)$ (a) Operator expectation values for state $\rho_a(t)$ as it evolves. An initially coherent state with $\alpha = 3.0$ decays to a state with $\langle \hat{n} \rangle = 1$, which we confirm as state $|1\rangle\langle 1|$ by considering the fidelity in (b). Horizontal gridlines are displayed in black, dashed. Numerical method: direct integration.

implying that these elements are constant in time. The single-photon state requires zero in each of these elements, and so we may predict that high fidelity between ρ_a and $|1\rangle\langle 1|$ may only be obtained when $\rho_{0,0}(t=0)$, $\rho_{0,1}(t=0)$, and $\rho_{1,0}(t=0) \ll 1$. This implies, in particular, that high fidelity with $|1\rangle\langle 1|$ is not obtainable for coherent states with small amplitude[4]. In Fig. 6.6 we show this explicitly.

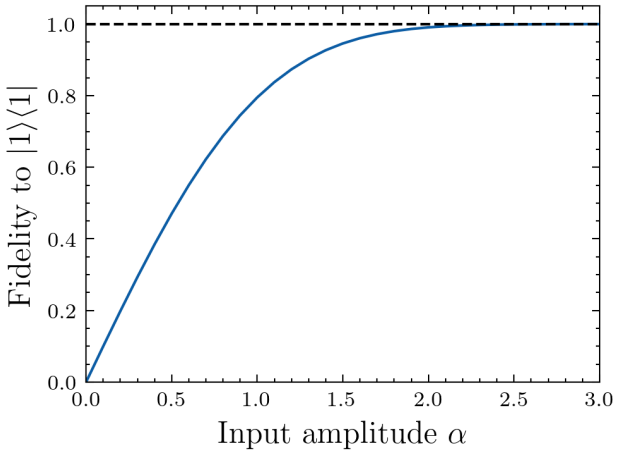


Figure 6.6: The fidelity of $\rho_a(t \to \infty)$ to single-photon state $|1\rangle\langle 1|$ depends on initial coherent state amplitude α since the density matrix elements $\rho_{0,0}, \rho_{0,1}$ and $\rho_{1,0}$ are constant in time.

Before we move on, let us quickly explore the related operator $\hat{a}\left(\hat{a}^\dagger\hat{a}-2\right)$. Based on the above discussion we might reasonably expect the steady-state to be $|2\rangle\langle 2|$, and this is indeed what we see in Fig. 6.7, where the fidelity to the two-photon state increases to 1.

We will refer to the decay described by Lindblad operator $\hat{A} = \hat{a}\left(\hat{a}^\dagger\hat{a}-1\right)$ as *nonlinear coherent loss* (NCL), since the eigenstates of the operator[5] $\hat{a}\left(\hat{a}^\dagger\hat{a}-1\right)$ are known as "nonlinear coherent states" [211], while the operator itself may be considered as the annihilation operator for a so-called f-deformed harmonic oscillator [212].

4 The requirement of large α for the input coherent state is not very restrictive, and as we shall see in the next section there are additional reasons to prefer $\alpha \gg 1$

5 The operator $\hat{a}\left(\hat{a}^\dagger\hat{a}-1\right)$ is a specific example of $\hat{a}\hat{f}(\hat{n})$ for operator-valued function $\hat{f}$. Glauber coherent states are obtained for the choice $\hat{f} = \hat{\mathbb{1}}$.

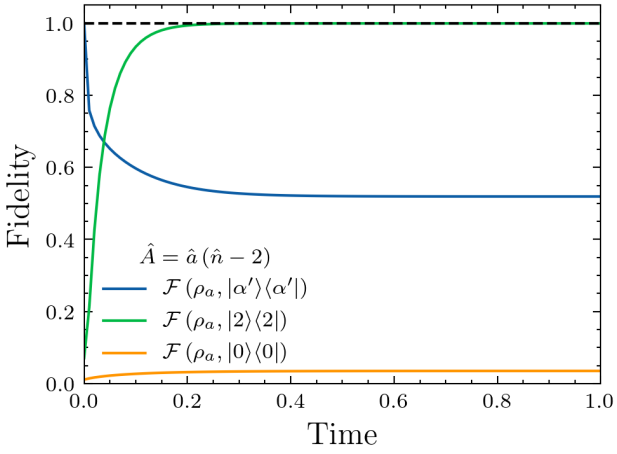


Figure 6.7: $\hat{A} = \hat{a}\left(\hat{a}^\dagger\hat{a} - 2\right)$. The steady-state of this loss operator is $|2\rangle\langle 2|$. The fidelity of ρ_a to this two-photon state increases to 1.

6.3 INCLUDING LOSS

We have seen that the nonlinear coherent loss (NCL) operator $\hat{a}\left(\hat{a}^\dagger\hat{a} - 1\right)$ is a good candidate for driving an initial coherent state towards a single photon state. Any system, therefore, which can implement the Lindblad equation 6.1 with decay operator $\hat{A} = \hat{a}\left(\hat{a}^\dagger\hat{a} - 1\right)$ will asymptotically and deterministically give rise to single-photon Fock states, although we have seen that fidelities close to 1 are obtainable even at finite time, Fig. 6.5b.

In a realistic situation however it is unlikely that a system can be designed to implement $\hat{a}\left(\hat{a}^\dagger\hat{a} - 1\right)$ only. We must consider how the system's output states are affected by additional loss mechanisms. In an optical system the single-photon (linear) loss can never be avoided, so we will explore its effect on the nonlinear coherent loss mechanism. To do this, we modify our original Lindblad equation to include several Lindbladian terms

$$\frac{d}{dt}\rho_a = \gamma_1 \mathcal{L}\left[\hat{a}\right]\rho_a + \gamma_{NCL}\mathcal{L}\left[\hat{a}\left(\hat{a}^\dagger\hat{a} - 1\right)\right]\rho_a \tag{6.21}$$

with γ_1 the decay rate via the single-photon loss channel $\hat{a}$, and γ_{NCL} the loss rate via NCL, $\hat{a}\left(\hat{a}^\dagger\hat{a} - 1\right)$. We can immediately see that $|1\rangle\langle 1|$ is only a steady-state of Eq. 6.21 when $\gamma_1 = 0$, in which case we revert to the analysis of Sec. 6.2.3. For all $\gamma_1 > 0$, the vacuum is the steady-state and the matrix elements $\rho_{0,0}, \rho_{0,1}, \rho_{1,0}$ are no longer constant in time.

Physically we see that the presence of linear loss leads to a degradation of the highly non-classical output states reached under NCL alone, as the additional linear loss mechanism pushes ρ_a towards the vacuum. We see this explicitly in Fig. 6.8b (c.f. Fig. 6.5), where an intially increasing fidelity with $|1\rangle\langle 1|$ eventually dies away, and fidelity to the vacuum state increases to 1. Additionally, photon number ex-

pectations decay to 0, and an initial increase in quadrature variances decays back to the vacuum state variance, Fig. 6.8a.

Figure 6.8b suggests an interesting phenomenon: over short timescales the system appears to be dominated by NCL $\hat{a}\left(\hat{a}^\dagger\hat{a}-1\right)$. Consider for example the fidelity between $\rho_a\,(t<0.05)$ and $|\alpha'\rangle\langle\alpha'|$ denoting a coherent state with equivalent photon-number expectation. By considering this alone, for short times the behaviour is indistinguishable from the case with $\gamma_1=0$. Similar reasoning applies also to the fidelities between $\rho_a\,(t<0.1)$ and $|1\rangle\langle 1|$, where the evolution is practically independent of γ_1 over short times.

From fidelity $\mathcal{F}\left(\rho_a\,(t<0.1)\,,|0\rangle\langle 0|\right)$, Fig. 6.8 even suggests that large γ_1 might help drive ρ_a towards the single-photon state faster than in the $\gamma_1=0$ case. However we infer that loss actually is not helpful here, since after about $t=0.05$ the fidelity to $|\alpha'\rangle\langle\alpha'|$ begins to increase again. This suggests that fidelity might not always be a useful measure of our desired behaviour when both nonlinear dissipation and linear loss are included.[6]

We examine the maximum attainable fidelity to $|1\rangle\langle 1|$ in Fig. 6.9. The maximum fidelity decreases with increasing γ_1, but increasing α appears to allow larger fidelities to be reached for the same γ_1 (c.f. Fig. 6.6). We will explore this phenomenon further in Sec. 6.3.3.

6.3.1 *Mandel parameter* Q

Although the fidelity has been a helpful measure for measuring the ability of our system to produce single-photons, we have observed in Fig. 6.3b a case where fidelity to the single-photon increases while ρ_a remains entirely coherent. It is therefore worth considering which other measures we might use to assess progress. One such measure is the Mandel Q parameter [6, 205, 206]:

$$Q=\frac{\left\langle\Delta\hat{n}^2\right\rangle}{\langle\hat{n}\rangle}-1, \tag{6.22}$$

which is written in terms of photon-number expectation $\langle\hat{n}\rangle$ and variance $\left\langle\Delta\hat{n}^2\right\rangle$. Equation 6.22 may equivalently be written in normal order as

$$Q=\frac{\left\langle\hat{a}^\dagger\hat{a}^\dagger\hat{a}\hat{a}\right\rangle}{\langle\hat{a}^\dagger\hat{a}\rangle}-\left\langle\hat{a}^\dagger\hat{a}\right\rangle. \tag{6.23}$$

Intuitively, the Mandel parameter is a measure of the amount of photon-number squeezing in ρ_a. Coherent states have Poissonian photon-number statistics, $\left\langle\Delta\hat{n}^2\right\rangle=\langle\hat{n}\rangle$, and so $Q=0$ in this case. States with $Q<0$ have reduced photon-number variance and are known as sub-Poissonian, while states with $Q>0$ are super-Poissonian.

6 Of course, we could have guessed this based on Fig. 6.3b as the fidelity to $|1\rangle\langle 1|$ increases until $t\approx 0.25$ while the state remains completely coherent.

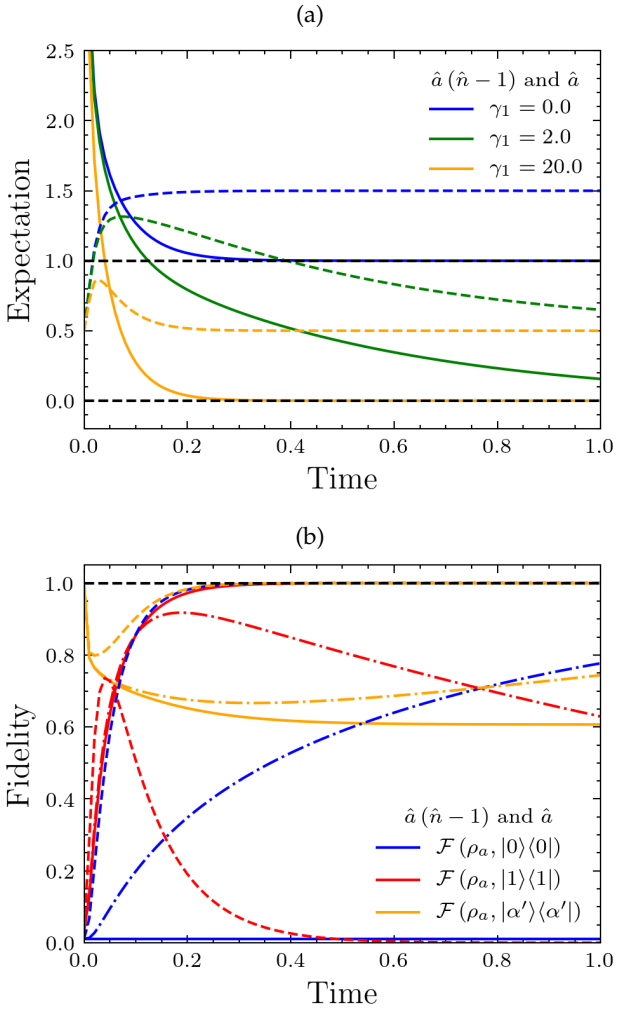


Figure 6.8: NCL $\hat{a}\left(\hat{a}^\dagger\hat{a}-1\right)$ and linear loss $\hat{a}$. Initial coherent state amplitude $\alpha = 3.0$, and $\gamma_{\mathrm{NCL}} = 8.0$. (a) Operator expectation values. Solid: $\langle\hat{a}^\dagger\hat{a}\rangle$. The presence of linear loss $\gamma_1 > 0$ ensures that the photon number decays to 0. Dashed: $\mathrm{Var}(\hat{x})$. Similarly, for $\gamma_1 > 0$ we see the variance in x return to its initial value, hinting that our state is being pushed towards vacuum. (b) Fidelities of $\rho_a(t)$ against vacuum (blue), single-photon state (red) and coherent state with equivalent photon-number expectation (orange). Solid: $\gamma_1 = 0$. Dot-dashed: $\gamma_1 = 2$. Dashed: $\gamma_1 = 20$. The presence of linear loss pushes ρ_a away from the single-photon state for $t > 0.1$. For $t < 0.1$ the system is dominated by NCL. Numerical method: direct integration.

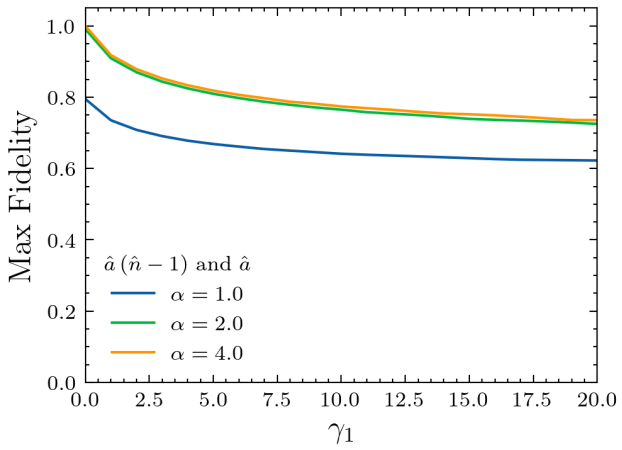


Figure 6.9: Maximum attainable fidelity between ρ_a and $|1\rangle\langle 1|$ at different linear loss levels γ_1. Linear loss drives ρ_a towards the vacuum and destroys the quantumness of our state, but over short times the fidelity to $|1\rangle\langle 1|$ appears independent of γ_1, Fig. 6.8. Here, we observe that after $\gamma_1 \approx 7.5$ the maximum attainable fidelity is practically independent of linear loss rate, while it does depend on α. We shall exploit this later. Numerical method: direct integration.

In the limit of zero uncertainty in photon-number, $\langle \Delta\hat{n} \rangle \to 0$ and so $Q \to -1$ and we reach the Fock states.

Clearly, both decay operators $\hat{a}\left(\hat{a}^\dagger\hat{a}-1\right)$ and $\hat{a}^2$ give steady-states with sub-Poissonian photon number statistics, while $\hat{a}$ gives rise to the vacuum, which is Poissonian. We will therefore seek to find parameter regimes for which the loss operators $\hat{a}\left(\hat{a}^\dagger\hat{a}-1\right)$ or $\hat{a}^2$ give $Q < 0$, even in the presence of linear loss.

The effect of NCL $\hat{a}\left(\hat{a}^\dagger\hat{a}-1\right)$ on Q is displayed in Fig. 6.10a under several different linear loss rates γ_1. We see that the effect of NCL is indeed to drive ρ_a towards a Fock state, and $Q \to -1$ for $\gamma_1 = 0$, only. For all $\gamma_1 \neq 0$ we see that Q eventually returns to 0 as the system tends towards the vacuum. However, even in this case large $|Q|$ are still obtained for finite t. In Fig. 6.10 we observe that the behaviour of Q over the initial evolution of ρ_a is independent of linear loss rate γ_1 (c.f. Fig. 6.8b, 6.9). This bodes well for implementation of $\hat{a}\left(\hat{a}^\dagger\hat{a}-1\right)$ as a deterministic generator of nonclassical states, since a restriction to small times t is always possible.

We therefore alter our goals. Since Fig. 6.10 predicts $Q(t) > -1$ whenever $\gamma_1 \neq 0$ we will unfortunately be unable to use NCL operator $\hat{a}\left(\hat{a}^\dagger\hat{a}-1\right)$ to generate single-photons. So, rather than finding a system which deterministically generates single-photon states in the long-time limit, we seek a system which will deterministically generate highly sub-Poissonian states after a specified evolution time. From now on we will take it as our goal to generate sub-Poissonian light over the initial stages of the system evolution.

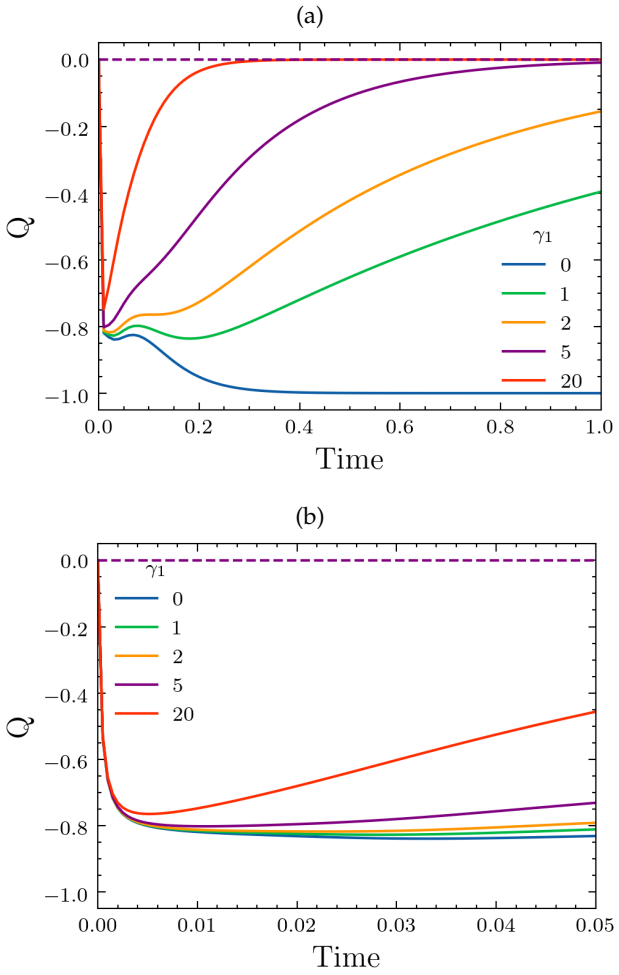


Figure 6.10: Mandel Q parameter under both NCL and linear loss. With $\gamma_1 = 0$, $Q \to -1$ as the system approaches $|1\rangle\langle 1|$. For any $\gamma_1 > 0$, $Q(t \to \infty) \to 0$, but significant $Q < 0$ are still obtained for finite t. Solid: $\gamma_{NCL} \neq 0$. Dashed: $\gamma_{NCL} = 0$, i.e. just linear loss. Numerical method: direct integration. (a) and (b) show the same evolution, but (b) is displayed over a shorter timescale.

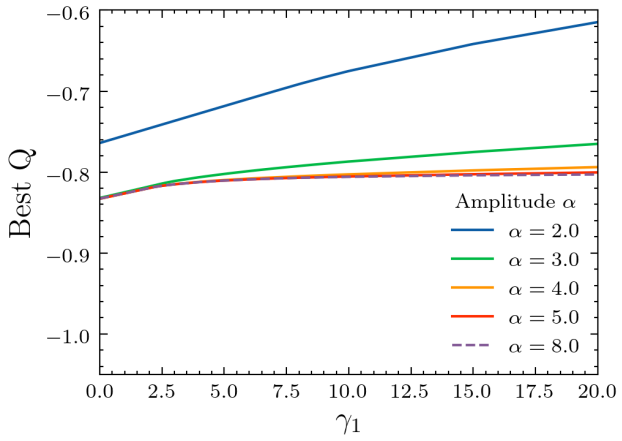


Figure 6.11: The best attainable value of Mandel parameter Q is approximately independent of γ_1 when the loss rate is nonzero. Larger α allows for better Q to be reached. Numerical method: direct integration ($\alpha = 2.0, 3.0, 4.0, 5.0$); quantum Monte Carlo ($\alpha = 8.0$).

We examine the best attainable $Q < 0$ for a given linear loss rate γ_1, and plot in Fig. 6.11. As we see, although the best attainable Q is no longer -1, it varies only slightly with increasing linear loss, and even for large $\gamma_1 = 15$ a Mandel parameter of $Q \approx -0.778$ is still attainable, while 3.2 photons remain in the state.

Figure 6.11 also appears to show that choosing larger initial α allows for smaller Q to be obtained, and we saw similar effects previously in Fig. 6.9 when considering the maximum attainable fidelity to the single-photon. While the large improvement in attainable Q between $\alpha = 2.0$ and $\alpha = 3.0$ is primarily due to reduction in the initial $\rho_{0,0}, \rho_{1,0}, \rho_{0,1}$, the improvement between $\alpha = 3.0$ and $\alpha = 4.0$ cannot be explained in the same way. We will explore this further using additional methods in the following sections, but for now let us briefly adopt an analytical approach. Consider the Lindblad equation describing both linear loss and NCL:

$$\frac{d}{dt}\rho_a = \left[\gamma_1 \mathcal{L}\left[\hat{a}\right] + \gamma_{NCL}\mathcal{L}\left[\hat{a}\left(\hat{a}^\dagger\hat{a} - 1\right)\right]\right]\rho_a, \tag{6.24}$$

and expand in Fock basis,

$$\begin{aligned}\frac{d}{dt}\rho_n = &-\left[\gamma_1 n + \gamma_{NCL} n\,(n-1)^2\right]\rho_n \\ &+\left[\gamma_1\,(n+1) + \gamma_{NCL}\,(n+1)\,n^2\right]\rho_{n+1},\end{aligned} \tag{6.25}$$

where $\rho_n = \langle n|\rho|n\rangle$. Terms in Eq. 6.25 involving γ_{NCL} are proportional to n^3, while terms involving γ_1 are proportional only to n. Therefore, for every nonzero choice of γ_1, γ_{NCL}, there exists an n for which the NCL dominates ($\gamma_{NCL} n^3 \gg \gamma_1 n$) and so Eq. 6.25 reduces to

$$\frac{d}{dt}\rho_n \approx -\gamma_{NCL} n\,(n-1)^2\,\rho_n + \gamma_{NCL}\,(n+1)\,n^2\rho_{n+1}, \tag{6.26}$$

which is independent of γ_1. Thus, a sufficient increase in the initial $\langle n \rangle$ will compensate for the effects of linear loss, which corroborates Fig. 6.11. We thus have an additional tool, the initial coherent state amplitude, to aid us toward generation of sub-Poissonian states via NCL.

To summarise, the inclusion of linear loss γ_1 causes our system to be driven toward the vacuum rather than a single-photon state. However, strong photon-number squeezing is obtained over the initial stages of system dynamics, Fig. 6.10, and is roughly independent of γ_1, Fig. 6.11. Linear loss may further be combatted [213, 214] by increasing the initial coherent state amplitude, thereby increasing $\langle n \rangle$, which causes NCL to dominate over the initial stages of dynamics. A strongly photon-number squeezed state is then obtained at the output by stopping the evolution at an appropriate time.

6.3.2 *Nonlinear decay*

Finally, let us examine behaviour of photon-number expectation $\langle \hat{n} \rangle$ when both NCL and linear loss are included. We have observed already, Fig. 6.8a, that linear loss causes ρ_α to decay to the vacuum rather than $|1\rangle\langle 1|$, and so in the long-time limit we have $\langle \hat{n} \rangle \to 0$. We have determined however that we are primarily interested in the early stages of dynamics over which NCL dominates, and so in our system we might expect to see a signature of NCL behaviour on the photon-number expectation.

As was remarked earlier, the NCL operator $\hat{a}\left(\hat{a}^\dagger \hat{a} - 1\right)$ may be interpreted as an intensity-dependent single-photon loss, with rate proportional to $\hat{n}$. This implies that a large coherent state amplitude should give rise to quick decay of photon-number, while smaller amplitude yields smaller decay. This is in contrast to linear loss in which the decay of $\langle n \rangle$ is exponential with constant rate.

We vary initial coherent state amplitude α and plot the initial stages of dynamics in Fig. 6.12, where we have initially set $\gamma_1 = 0$ in order to isolate the effects of NCL. Although each coherent state initially possesses different average photon number, after a short amount of time each state possesses the same average photon number since they have experienced different decay rates. This "nonlinear decay" is a key indicator of NCL [215, 216].

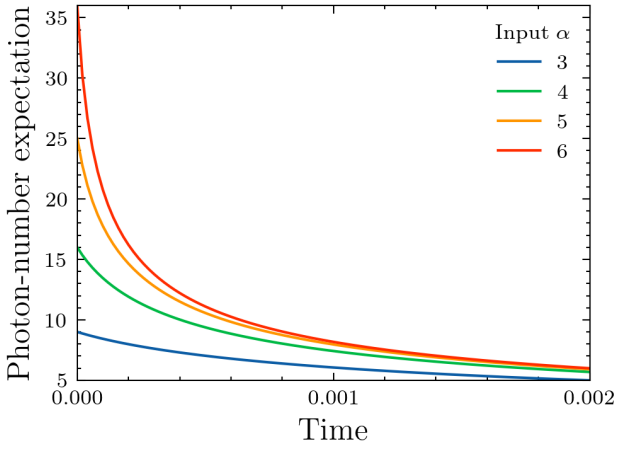


Figure 6.12: NCL induces intensity-dependent decay rates, and so states with initially different $\langle \hat{n} \rangle$ quickly decay to a level where they possess the same average photon number. This is a key demonstration of NCL. Linear loss rate $\gamma_1 = 0.0$. Numerical method: direct integration.

6.3.3 *Summary of NCL effects*

The two signature behaviours of NCL which we have observed are

- $Q < 0$ Fig. 6.13a, and
- Nonlinear decay of $\langle \hat{n} \rangle$ Fig. 6.13b.

These are good indicators that a system is undergoing NCL. Generating the condition $Q < 0$ is precisely our goal, while a system which undergoes the nonlinear decay we might reasonably expect will also generate $Q < 0$. Throughout the rest of the chapter we observe these two signature behaviours in increasingly complex models, Fig. 6.1.

Let us conclude by displaying the two signature behaviours for a system which has all three types of loss which were examined in Sec. 6.2, namely single-photon loss $\hat{a}$, two-photon loss $\hat{a}^2$ and nonlinear coherent loss $\hat{a}\left(\hat{a}^\dagger \hat{a} - 1\right)$. We will use parameters which we demonstrate to be realistic in Sec. 6.4.

Specifically, we solve

$$\frac{d}{dt}\rho_a = \left[\gamma_1 \mathcal{L}\left(\hat{a}\right) + \gamma_2 \mathcal{L}\left(\hat{a}^2\right) + \gamma_{NCL} \mathcal{L}\left(\hat{a}\left(\hat{a}^\dagger \hat{a} - 1\right)\right)\right] \rho_a \qquad (6.27)$$

with parameters $\gamma_2 = 0.0005$, and $\gamma_{NCL} = 0.002$. We allow linear loss rate γ_1 to vary, while (for $\gamma_1 > 0$) it remains the dominating loss channel for the system. For $\gamma_1 = 0$ in Fig. 6.13a we observe that $Q = -0.8$ is the limiting value, independent of initial α. However, larger input α enables the system to reach this limit faster. Figure 6.13b displays NL decay in this system.

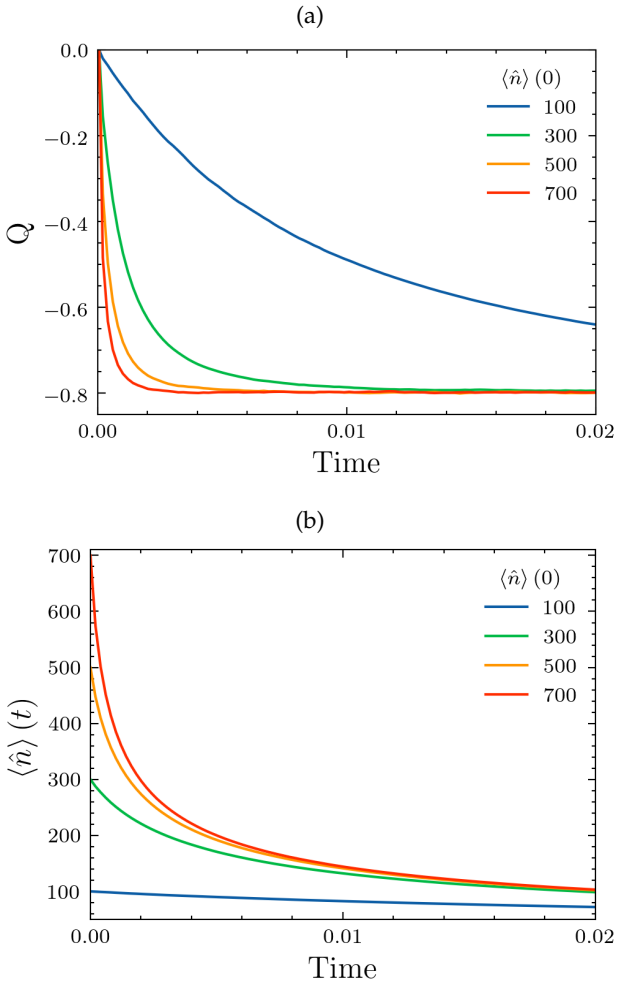


Figure 6.13: Signature behaviours of NCL in a system obeying Eq. 6.27 with $\gamma_2 = 0.0005$, $\gamma_{NCL} = 0.002$ and an initial coherent state with average photon number $\langle \hat{n} \rangle (0)$. (a) Generation of sub-Poissonian light, as evidenced by $Q < 0$. Linear loss $\gamma_1 = 0$ and so the maximum value of $|Q|$ is obtained for most choices of α, but the time taken to reach maximum Q decreases as initial α increases. (b) Nonlinear decay of photon-number expectation $\langle \hat{n} \rangle$. Intensity-dependent loss causes states with large photon numbers to decay very quickly, while states with similar photon numbers experience similar decay rate. Numerical method: quantum Monte Carlo.

Varying γ_1 and α, Fig. 6.14, we see that although linear loss γ_1 causes progressively worse values for Q, the dynamics are approximately independent of γ_1 over short timescales. However, for a given large γ_1, larger values of $|Q|$ can be reached by increasing the initial coherent state amplitude. Therefore, our recipe for generating non-classical states with highly sub-Poissonian photon-number statistics is to design a system which obeys Eq. 6.27, and then allow an initially bright coherent state to evolve for a very short amount of time. In the limit $\gamma_1 \to 0$ this can generate states with up to $Q = -0.8$ (or $Q = -1$ if $\gamma_2 \to 0$ also), while for all $\gamma_1 > 0$ we can force $Q \to -0.8$ by choosing $\alpha \gg 1$. The state is no longer close to a single-photon state, e.g. the best Q in Fig. 6.14b occurs when the state with initially $\langle \hat{n} \rangle = 700$ has reduced to $\langle \hat{n} \rangle = 285$, and so the output state is both bright and highly sub-Poissonian.

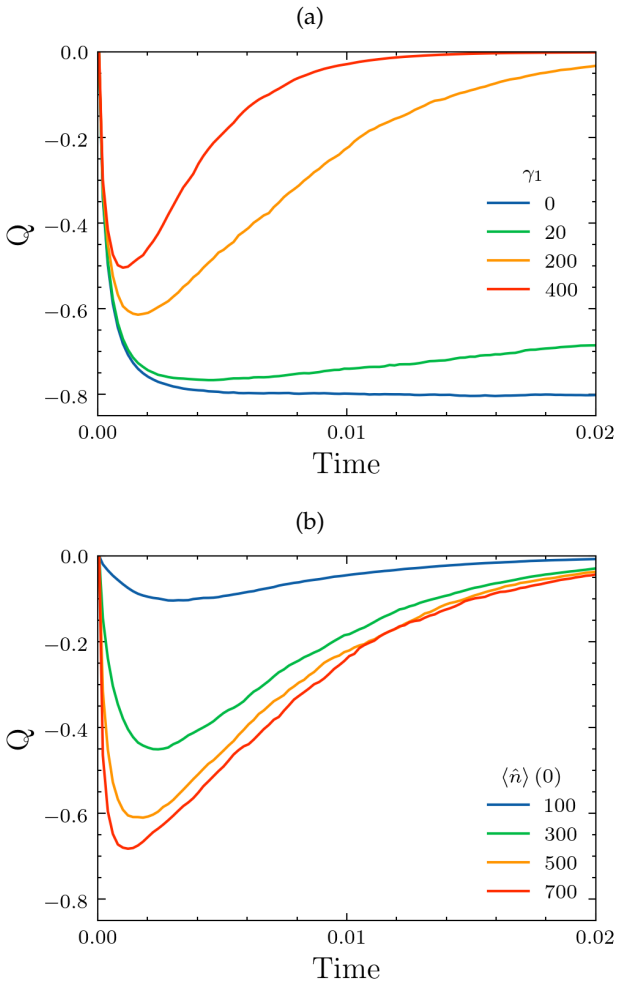


Figure 6.14: Evolution of the Mandel Q parameter as γ_1 and α are varied in a system obeying Eq. 6.27 with $\gamma_2 = 0.0005$, $\gamma_{\mathrm{NCL}} = 0.002$ and an initial coherent state with average photon number $\langle \hat{n} \rangle (0)$. (a) Constant $\langle \hat{n} \rangle (0) = 500$ photons and varying linear loss γ_1. Larger γ_1 causes progressively smaller values of $|Q|$ to be obtained, c.f. Fig. 6.11, although the dynamics are practically independent of γ_1 for small times. (b) Constant $\gamma_1 = 200$. Even with large linear loss, larger $|Q|$ may be obtained by starting with a brighter coherent state (larger $\langle \hat{n} \rangle (0)$). Numerical method: quantum Monte Carlo.

6.4 THREE-MODE MODEL

Having analysed the single-mode model in detail, and demonstrated that the NCL operator $\hat{a}\left(\hat{a}^\dagger\hat{a}-1\right)$ is a good candidate for deterministic generation of highly non-classical states even in the presence of two-photon loss and strong linear loss, we must turn to consider whether such an NCL operator can be effectively realised in practice. In this section we will demonstrate that $\hat{a}\left(\hat{a}^\dagger\hat{a}-1\right)$ may be effectively simulated in a three-mode system via a combination of strong linear loss, linear coupling between multiple modes, and the Kerr nonlinearity. Our starting point is the three-mode model, depicted in Fig. 6.15, in which two bosonic modes, a and b, are coupled to a third, c_0, which then decays into a Markovian reservoir R with decay rate γ_c.

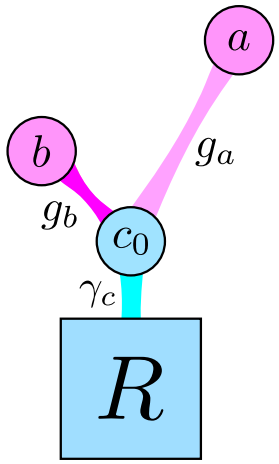


Figure 6.15: Three-mode model of PhoG device. Two bosonic modes, a and b, are each coupled to a third mode, c_0. Mode c_0 is then strongly coupled to Markovian reservoir R via linear loss $(\hat{A}=\hat{a})$ with decay rate γ_c.

The Lindblad equation describing this three-mode model is

$$\frac{d}{dt}\rho_3 = -i\left[\hat{H}_3,\rho_3\right] + \left[\gamma_1\mathcal{L}\left[\hat{a}\right]+\gamma_1\mathcal{L}\left[\hat{b}\right]+\gamma_c\mathcal{L}\left[\hat{c}_0\right]\right]\rho_3 \tag{6.28}$$

where the subscript 3 denotes that we are dealing with this three-mode model. We have additionally assumed that modes a and b to be coupled to independent Markovian reservoirs with rate γ_1 which models the conventional linear loss. The Hamiltonian is taken to be $\hat{H}_3 = \hat{H}_3^{\text{int}} + \hat{H}_3^{\text{Kerr}}$, where

$$\begin{aligned}\hat{H}_3^{\text{int}} &= g_a\hat{a}^\dagger\hat{c}_0 + g_b\hat{b}^\dagger\hat{c}_0 + \text{h. c.}\\ \hat{H}_3^{\text{Kerr}} &= \frac{U}{2}\sum_x \hat{x}^\dagger\hat{x}^\dagger\hat{x}\hat{x} \quad \text{with} \quad \hat{x}\in\left\{\hat{a},\hat{b},\hat{c}_0\right\}.\end{aligned} \tag{6.29}$$

The interaction Hamiltonian $\hat{H}_3^{\text{int}}$ describes linear coupling between modes, while the Kerr Hamiltonian $\hat{H}_3^{\text{Kerr}}$ describes the self-Kerr interaction (self-phase modulation) on each mode. This Hamiltonian may

be realised, for example, by evanescently coupled waveguides in a $\chi^{(3)}$ glass [217–219]. The constant U is the Kerr nonlinear interaction constant, and we will relate this to glass properties in Sec. 6.5, below.

The three-mode model Eq. 6.28, while a physically useful starting point for building a system which accurately simulates NCL, is currently too difficult to analyse, either analytically or using the numerical methods which proved useful for the single mode model in Secs. 6.2, 6.3 (see Appendix E).

We may reduce the complexity of Eq. 6.28 by assuming that the decay rate γ_c of mode c_0 into the reservoir R is large enough that mode c_0 completely decays on a much faster timescale than modes a, b. This will allow for adiabatic elimination of mode c_0 via the methods described in Appendix. D. We identify

$$\begin{aligned} H^{(0,0)} &= \frac{U}{2} \sum_{x\in\{a,b\}} x^{\dagger 2} x^2, \\ H^{(0,1)} &= g_a a^\dagger c_0 + g_b b^\dagger c_0, \\ H^{(0,2)} &= 0, \end{aligned} \tag{6.30}$$

and so, substituting into Eq. D.14, we arrive at

$$\begin{aligned} \frac{d}{dt}\rho_2 = -i\left[\frac{U}{2}\sum_{x\in\{a,b\}} x^{\dagger 2}x^2, \rho_2\right] + \frac{4G^2}{\gamma_c}\mathcal{L}\left[\frac{g_a a + g_b b}{G}\right]\rho_2 \\ + \gamma_1\left(\mathcal{L}[a] + \mathcal{L}[b]\right)\rho_2, \end{aligned} \tag{6.31}$$

where $G = \sqrt{g_a^2 + g_b^2}$. The three-mode model has been reduced to a two-mode system involving only modes a, b. Introducing the following collective symmetric and antisymmetric modes

$$\begin{aligned} \hat{s}_+ &= \frac{1}{G}\left(g_a \hat{a} + g_b \hat{b}\right) \quad \text{symmetric}, \\ \hat{s}_- &= \frac{1}{G}\left(g_a \hat{b} - g_b \hat{a}\right) \quad \text{antisymmetric}, \end{aligned} \tag{6.32}$$

and rewriting Eq. 6.31 in terms of these new modes we arrive at the final equation for our two-mode model

$$\frac{d}{dt}\rho_2 = -i\left[\hat{H}_2, \rho_2\right] + \left[\gamma_1 \mathcal{L}[\hat{s}_-] + (\Gamma + \gamma_1)\mathcal{L}[\hat{s}_+]\right].\rho_2 \tag{6.33}$$

The subscript 2 denotes that each quantity is for this two-mode model. We have defined the new decay rate as $\Gamma = 4G^2/\gamma_c$. The Hamiltonian $\hat{H}_2$ takes the form $\hat{H}_2 = \hat{H}_2^{\text{self}} + \hat{H}_2^{\text{int}}$, with

$$\begin{aligned} H_2^{\text{self}} &= \sigma_1\left(n_+^2 + n_-^2\right) + \sigma_2 n_+ n_- + \sigma_3\left(n_+ + n_-\right), \\ H_2^{\text{int}} &= \sigma_4\left(s_+^\dagger s_-\right)^2 + \sigma_5 s_+^\dagger s_-\left(n_- - n_+ - 1\right) + \text{h. c.}, \end{aligned} \tag{6.34}$$

where $n_\pm = s_\pm^\dagger s_\pm$. Our σ coefficients are

$$\sigma_1 = \frac{U}{2G^4}\left(g_a^4 + g_b^4\right),\ \sigma_2 = \frac{4U}{G^4}\left(g_a g_b\right)^2,$$
$$\sigma_3 = \frac{\sigma_2}{4} - \frac{U}{2},\ \sigma_4 = \frac{\sigma_2}{4},\ \sigma_5 = \frac{U}{G^4} g_a g_b \left(g_a^2 - g_b^2\right). \tag{6.35}$$

The two-mode model obeying Eq. 6.33 is depicted in Fig. 6.16. Mode s_+ decays into reservoir R with decay rate $\Gamma + \gamma_1$. In the absence of linear loss, $\gamma_1 = 0$, mode s_- will decay only vicariously through s_+, and the coupling between modes is proportional to nonlinearity parameter U. In a linear system, $U = 0$, the antisymmetric mode s_- will not decay and so in that case we may identify it as the dark mode of such linear system, which is considered further e.g. in Ref. [220].

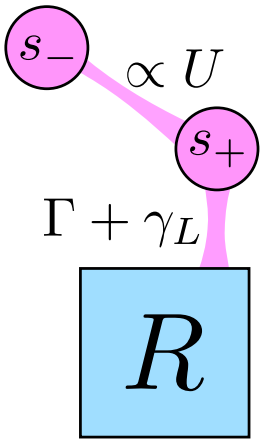


Figure 6.16: Two-mode model of the PhoG device. Having adiabatically eliminated mode c_0 from the three-mode model (Fig. 6.15) and rotated to collective basis s_-, s_+ using Eqs. 6.32 we see that mode s_- will only decay into R by first decaying into s_+. The linear coupling between s_- and s_+ is proportional to U, and so for a linear system $U = 0$ mode s_- cannot decay into R. Decay rate $\Gamma = 4G^2/\gamma_1$.

We have thus reduced the complexity of our system from three modes to two. However, even two bosonic modes are computationally very challenging to simulate when large photon numbers are required[7], although we shall encounter approximation methods in Sec. 6.6.2 which help us to deal with this.

We thus seek to adiabatically eliminate mode s_+ from the system, which will leave us with an equation for s_- only. Let us assume that the decay rate $\Gamma + \gamma_1$ is the dominating decay rate of the two-mode model, and that mode s_+ decays to its steady state much quicker

7 For example, we note in Appendix E that a coherent state may be accurately modelled on a Hilbert space size $2\lceil\alpha^2\rceil$ without adverse effects due to Hilbert space truncation. In practice, initial $\langle\hat{n}\rangle = 700$, required in Fig. 6.14b to give large negative Q, will require a Hilbert space size $|\mathcal{H}| > 794$ on each mode, and so a total Hilbert space size of $794 \times 794 = 630436$. This is challenging to implement.

than the typical timescale of the dynamics of s_-. Then applying the adiabatic elimination method described in Appendix D we identify

$$\begin{aligned} H^{(0,0)} &= \sigma_1 n_-^2 + \sigma_3 n_-, \\ H^{(0,1)} &= \sigma_5 s_-^\dagger n_-, \\ H^{(0,2)} &= \sigma_4 s_-^{\dagger 2}, \end{aligned} \tag{6.36}$$

and so

$$\frac{d}{dt}\rho_1 = -i\left[\hat{H}_1, \rho_1\right] + \left\{\gamma_1 \mathcal{L}\left[s_-\right] + \gamma_2 \mathcal{L}\left[s_-^2\right] + \gamma_{NCL}\mathcal{L}\left[\hat{a}\left(\hat{a}^\dagger \hat{a} - 1\right)\right]\right\}\rho_1. \tag{6.37}$$

We have used the commutator to write $n_- s_- \to \hat{a}\left(\hat{a}^\dagger \hat{a} - 1\right)$. The new decay rates are

$$\gamma_2 = \frac{4U^2\left(g_a g_b\right)^4}{G^8\left(\Gamma + \gamma_1\right)} \quad \text{and} \quad \gamma_{NCL} = \frac{4U^2\left(g_a g_b\right)^2}{G^8\left(\Gamma + \gamma_1\right)}\left(g_a^2 - g_b^2\right)^2. \tag{6.38}$$

We see that Eq. 6.37 matches Eq. 6.27 except for the addition of the Hamiltonian $\hat{H}_1 = H^{(0,0)}$, which does not affect the photon-number statistics.

The effective decay rates γ_2, γ_{NCL} in this single-mode model explicity depend on coupling constants g_a, g_b (Fig. 6.15, Eq. 6.29). We see for example that in the limit of symmetric coupling $g_a = g_b$, we have $\gamma_{NCL} = 0$ and there will be no NCL for mode s_-. Large γ_{NCL} can be obtained however for strong asymmetry $g_a \gg g_b$ or $g_b \gg g_a$.

Since it is NCL which drives ρ most effectively towards highly sub-Poissonian states we will seek to maximise γ_{NCL}. We fix $G = \sqrt{g_a^2 + g_b^2}$ and define $g_a = xG, g_b = \sqrt{1-x^2}G$ for $0 < x < 1$. Substituting these couplings into our equation for γ_{NCL} we see that

$$\gamma_{NCL} = \frac{-4Ux^2\left(1-2x^2\right)^2\left(-1+x^2\right)}{\Gamma + \gamma_1}. \tag{6.39}$$

We proceed by setting $\frac{d}{dx}\gamma_{NCL} = 0$, which yields

$$x = \frac{\sqrt{2+\sqrt{2}}}{2} \tag{6.40}$$

as the only solution[8] $0 < x < 1$ which will yield a nonzero γ_{NCL}. So, the optimum choice for g_a, g_b is

$$g_b = \left(\sqrt{2} - 1\right) g_a. \tag{6.41}$$

8 Note that $x = 1/\sqrt{2}$ is the only other solution with $0 < x < 1$. This choice of x will yield symmetric coupling $g_a = g_b$ and hence $\gamma_{NCL} = 0$. We will return to this scenario in Sec. 6.7.

Taking this optimal choice,

$$\gamma_2 = \frac{U^2}{16\,(\Gamma+\gamma_1)} \quad \text{and} \quad \gamma_{\text{NCL}} = \frac{U^2}{4\,(\gamma_1+\Gamma)}, \tag{6.42}$$

and we are finally able to give motivation for the choices of $\gamma_2 = 0.0005, \gamma_{\text{NCL}} = 0.002$ used in Sec. 6.3.3 as the decay rates given by Eq. 6.42 when $\Gamma = 432g$, $U = 2g$, $\gamma_1 = 0$. The g is a dimensionless scaling parameter which we here take to be 1. Altering g will only serve to re-scale the time axis of Figs. 6.13, 6.14 but the qualitative dynamics will remain unchanged.

To summarise, we have reduced the three-mode model (Eq. 6.28, Fig. 6.15) to a single-mode model (Eqs. 6.27 , 6.37, Fig. 6.2) via sequential adiabatic eliminations of modes c_0 and s_+, which each rapidly decayed into reservoir R. In essence, the behaviour of the antisymmetric collective mode s_- in the three-mode model simulates behaviour of a single mode undergoing nonlinear coherent loss, two-photon loss and single-photon loss, which were all considered in Secs. 6.2, 6.3. The combination of Kerr nonlinearity, linear coupling and single-photon loss allows for the effective NCL decay operator to be constructed.

We demonstrate in Figs. 6.17, 6.18 that both the three-mode model and the two-mode model do indeed give rise to the same behaviour as the single-mode model. Considering the two-mode model (Fig. 6.18a) we see that initially mode s_- does not have rapid decay. This is because mode s_+ is populated (Fig. 6.18b). However, once s_+ begins to decay, we observe good agreement between two-mode and single-mode model. The two-mode model exhibits behaviours signature to NCL.

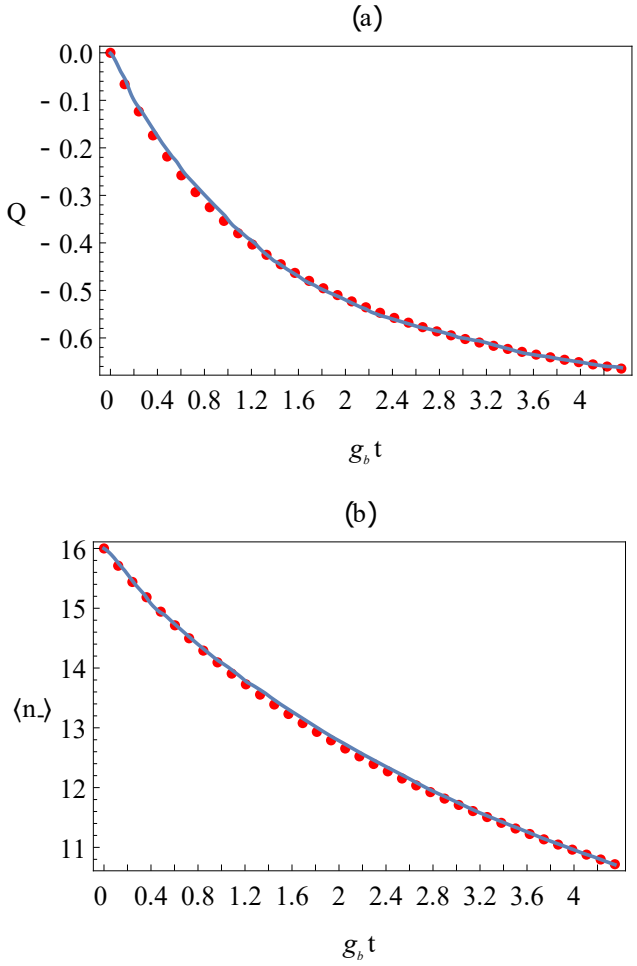


Figure 6.17: Evolution of Mandel parameter (a) and mean photon number (b) of the antisymmetric mode s_- computed via the three-mode model (solid lines) and the single-mode model (dots) for parameters: $g_b/g_a = \sqrt{2}-1$, $U = 0.012 g_b$, $\gamma_c = 6.04 g_b$, and $\gamma_1 = 0.0$. *Picture credit: Anton Sakovich in Ref. [221].* Numerical method: quantum Monte Carlo (three-mode model); direct integration of Eq. 6.25 (single-mode model)

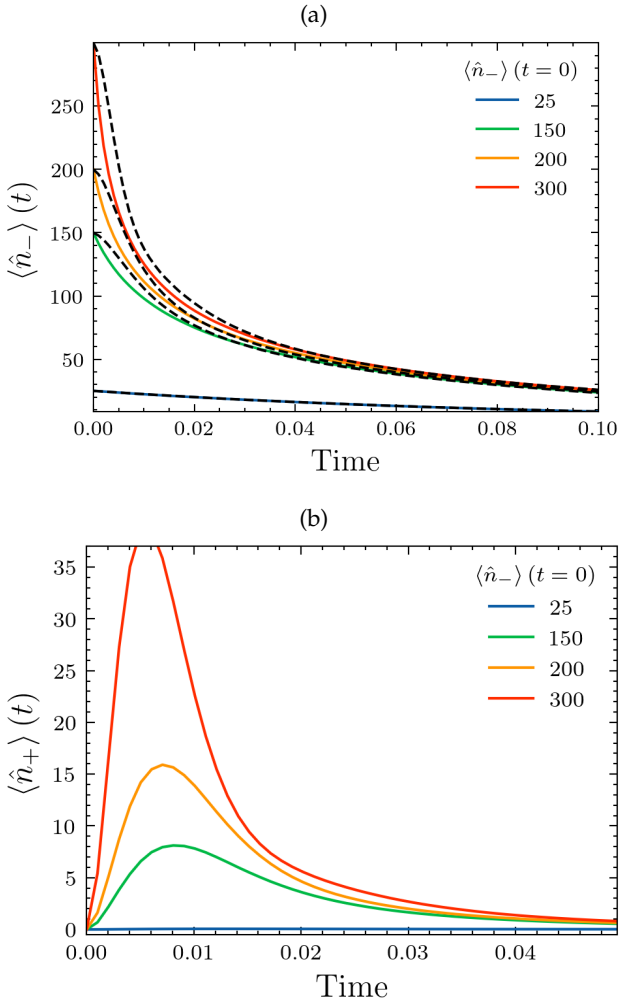


Figure 6.18: (a) Comparison of nonlinear decay for single-mode model (solid) and two-mode model (dashed) with varying input $\langle \hat{n}_- \rangle$. Input $\langle \hat{n}_+ \rangle = 0$, optimal couplings $g_a, g_b, \gamma_1 = 10.0$ and otherwise equivalent parameters to Fig. 6.13. Finite (nonzero) decay time (b) of mode s_+ means that the adiabatic elimination of s_+ is not yet valid for $t \approx 0$. Otherwise, there is good agreement between models once s_+ has begun to decay, and the two-mode model exhibits the same signature behaviours of NCL.

6.5 REALISTIC PARAMETERS

Let us consider how the analysis we have performed so far connects to real parameters of a physical system which is capable of implementing the PhoG device. We have in mind a network of waveguides laser-inscribed into highly nonlinear glass, e.g. IG2 [199], which will be created using methods similar to the recent work Ref [198]. Our envisioned system is depicted in Fig. 6.19.

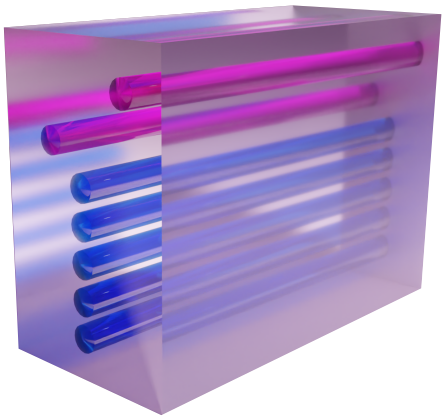


Figure 6.19: 3D representation of finished PhoG device. Waveguides are laser-inscribed into IG2 glass and allow for NCL to be simulated.

In order to proceed, we must consider two new things: (i) realistic glass parameters and how they influence constants which enter into our Lindblad equations 6.28, 6.33, 6.37; (ii) simulation of a Markovian reservoir R by a "tail" of additional bosonic modes. We consider (i) in this section, and (ii) in Sec. 6.6.

We will derive realistic parameters in this section, and they will be used in Sec. 6.6 to show that the desired signature behaviours are still observed. These order-of-magnitude calculations are intended to illustrate feasibility of our device in real glass, but ideally the parameters must be measured experimentally on the device itself [222].

The important quantity to estimate is the Kerr nonlinearity parameter U which is used in our Hamiltonians. To do so, we will follow the analyses put forth in Refs. [217–219], and assume that a pulse of finite length L_{eff} propagates through a waveguide with length L, such that $L \gg L_{\text{eff}}$. The waveguide in $\chi^{(3)}$ glass is assumed[9] to have no dispersion and the pulse shape does not change. We consider only the changes of the quantum state of the pulse caused by nonlinearity, linear loss and nonlinear phase changes.

The Kerr nonlinearity parameter may be written as

$$U = 2\hbar \frac{\omega^2}{V_{\text{eff}}} \frac{n_2}{n_{\text{eff}}}, \tag{6.43}$$

9 We will briefly discuss relaxation of these conditions in Sec. 6.8.

which is derived e.g. in Refs. [217–219] either in terms of nonlinear refractive index parameter n_2 or third-order susceptibility $\chi^{(3)}$. V_{eff} is the effective mode volume which we take to be $V_{\text{eff}} \sim A_{\text{eff}} L_{\text{eff}}$, with A_{eff} the transverse mode area. We take the effective refractive index of the waveguide mode to be $n_{\text{eff}} \approx 2.5$ which is typical for IG2 glass [199]. IG2 also has $n_2 \sim 3 \times 10^{-18} \text{W}^{-1}\text{m}^2$ [222, 223].

The effective mode area is yet uncertain and for implementation must be measured on the realistic device. For an upper bound we take A_{eff} to be the area of the waveguide which is on the order of 10^{-12}m^2 as in Ref. [198] for similar laser-inscribed waveguides capable of supporting large pulse energies. Taking for example $A_{\text{eff}} = 120 \times 10^{-12}\text{m}^2$, for a 100 fs pulse at 1064 nm we calculate $U \approx 8.5 \times 10^{-8}$. We may reasonably expect the final values of U to even increase in a finished device owing to reduction in A_{eff} (e.g. in Ref. [198] the waveguides are approximately $4\mu\text{m} \times 4\mu\text{m}$). Evolution under this $U = 8.5 \times 10^{-8}$ is modelled in Sec. 6.6. We should stress however that the specific value of U must be measured on a final physical device, and the values in this section are order-of-magnitude estimates only.

6.6 MULTI-MODE MODEL

In the previous sections we have demonstrated that the three-mode model considered in Sec. 6.4 accurately simulates NCL and allows for deterministic generation of sub-Poissonian light over the initial stages of the dynamics. A natural next question to ask is "how might we implement such a model?".

One approach which was successfully demonstrated in Ref. [198] is to replace the Markovian reservoir R with a "tail" of further bosonic modes. Here we adopt this replacement in order to implement the system in laser-inscribed waveguides. This replacement was recently considered in Ref. [195, 198]. We therefore wish to analyse the multi-mode model of the PhoG device, Fig. 6.20, in which two "signal" modes are linearly coupled to the "tail" of further modes. The intra-tail coupling g_c should be chosen to mimic the effect of reservoir R, and thus allow for the adiabatic elimination of modes c_0 and s_+. We will solve this model and compare it to the models used previously in order to demonstrate agreement between these approaches. The Lindblad master equation describing the multi-mode system is

$$\frac{d}{dt}\rho = -i\left[\hat{H}, \rho\right] + \gamma_1 \left[\mathcal{L}\left[\hat{a}\right] + \mathcal{L}\left[\hat{b}\right] + \sum_{j=0}^{N} \mathcal{L}\left[\hat{c}_j\right]\right] \rho, \tag{6.44}$$

with $\hat{H} = \hat{H}^{\text{int}} + \hat{H}^{\text{Kerr}}$, and

$$\hat{H}^{\text{int}} = g_a \hat{a}^\dagger \hat{c}_0 + g_b \hat{b}^\dagger \hat{c}_0 + \sum_{j=1}^{N} g_j \hat{c}_{j-1}^\dagger \hat{c}_j + \text{h. c.},$$
$$\hat{H}^{\text{Kerr}} = \frac{U}{2} \sum_{x \in \{a,b,c_j\}} \hat{x}^\dagger \hat{x}^\dagger \hat{x} \hat{x}, \qquad j = 0, 1, \ldots, N. \tag{6.45}$$

The Kerr nonlinearity constant is U, total number of tail modes is N, and coupling constants are g_a, g_b, g_c. We cannot hope to numerically simulate Eq. 6.44 over the necessary parameter regimes of large input α and large number of modes[10]. For the multi-mode model the only decay route into a Markovian reservoir is via linear loss γ_1 which we take to affect every mode independently. We require the tail to be long enough that state which has initially decayed into the tail cannot return to the signal modes over the timescales of interest. This traps us in the unfortunate scenario of having to make predictions of the behaviour of a large number of coupled modes, with strong nonlinearity and a necessarily large Hilbert space size of each mode.

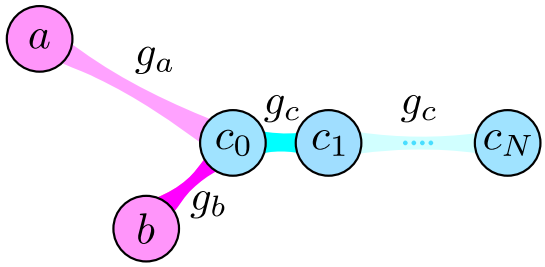


Figure 6.20: Multi-mode model of the PhoG device (c.f. Fig. 6.1 IV) in which the Markovian reservoir R from the three-mode model (Fig. 6.15) is replaced by a long "tail" of additional bosonic modes.

To proceed we will consider two related approaches to approximate the system Eq. 6.44: a meanfield approach (Sec. 6.6.1) and a quantum linearization approach (Sec. 6.6.2). Each of these techniques will give us a set of coupled differential equations for expectations of quantum operators. The number of equations scales only polynomially[11] in N and so is much more manageable than the numerical methods considered in Appendix E.1, E.2 and used in previous sections.

10 Even taking each mode as a qubit cannot help, as the total Hilbert space size is 2^N which remains intractable for N large.

11 Rather than the exponential scaling of the Lindblad master equation 6.44, see Appendix E.

6.6.1 *Meanfield approach*

To illustrate the first of these approaches, let us use our master equation 6.44 to find an equation for expectation $\langle \hat{a} \rangle$ of mode a. We see that

$$\frac{d}{dt} \langle \hat{a} \rangle (t) = \mathrm{Tr}\left(\hat{a} \frac{d}{dt} \rho \right), \tag{6.46}$$

and so

$$\frac{d}{dt} \langle \hat{a} \rangle (t) = -i g_a \langle \hat{c}_0 \rangle - i \frac{U}{2} \left\langle \hat{a}^\dagger \hat{a} \hat{a} \right\rangle - \frac{\Gamma}{2} \langle \hat{a} \rangle, \tag{6.47}$$

which is an exact differential equation for $\langle \hat{a} \rangle$ in terms of first- and third-order expectations. Analogously, equations for second-order terms such as $\langle \hat{a}\hat{a} \rangle$ or $\left\langle \hat{a}^\dagger \hat{a} \right\rangle$ will involve second- and fourth-order expectations. As we noted in the discussion around Eq. 6.8, this system of equations is not closed. In fact, when equations for expectations of third- or fourth- order operator products are derived, we see that they must be written in terms of fifth- and sixth- order operators, and so on. This yields an infinite hierarchy of coupled differential equations of progressively higher orders. We must seek a simplification.

If we write $\hat{a} \approx \langle \hat{a} \rangle$ and substitute in to Eq. 6.47 we see terms second-order or higher becoming much easier to handle. This allows us to simplify higher order terms, for example:

$$\langle \hat{a}^\dagger \hat{a} \hat{a} \rangle \approx \langle \hat{a}^\dagger \rangle \langle \hat{a} \rangle \langle \hat{a} \rangle, \tag{6.48}$$

and so Eq. 6.47 becomes

$$\frac{d}{dt} \langle \hat{a} \rangle (t) = -i g_a \langle \hat{c}_0 \rangle - i \frac{U}{2} \langle \hat{a}^\dagger \rangle \langle \hat{a} \rangle \langle \hat{a} \rangle - \frac{\Gamma}{2} \langle \hat{a} \rangle \tag{6.49}$$

solely in terms of first-order expectations[12]. The differential equations for second-order expectations like $\left\langle \hat{a}^\dagger \hat{a} \right\rangle$ are likewise reduced to first-order

$$\frac{d}{dt} \langle \hat{a}^\dagger \hat{a} \rangle = \frac{d}{dt} |\langle \hat{a} \rangle|^2 = -\Gamma \langle \hat{a}^\dagger \rangle \langle \hat{a} \rangle - i \langle \hat{a}^\dagger \rangle \langle \hat{c}_0 \rangle + i \langle \hat{a} \rangle \langle \hat{c}_0^\dagger \rangle \tag{6.50}$$

and so the system is completely specified by $N + 2$ differential equations[13], one for each mode $\langle \hat{a} \rangle, \langle \hat{b} \rangle, \langle \hat{c}_j \rangle \ldots$. We display this full system of equations in Appendix E.5.

The approximation $\hat{a} \approx \langle \hat{a} \rangle$ is known as the *mean-field* approximation, which treats our quantum system as a quasi-classical one. This system may be readily solved with any standard numerical package, and we display the evolution of photon-number expectation $\langle \hat{n}_- \rangle$ in Fig. 6.21 for the multi-mode model (dashed). We include also behaviour of the single-mode model (solid), for comparison. We see that even in the mean-field approximation, nonlinear decay due to NCL may be observed. The slight discrepancy between single- and multi-mode models for large initial amplitudes is due to finite (nonzero) decay time for mode s_+, and the impact of the tail.

12 Note that each expectation $\langle \hat{a} \rangle$ is just a c-number.

13 Rather than $2(N + 2)$, since $\langle \hat{a}^\dagger \rangle = \langle \hat{a} \rangle^*$.

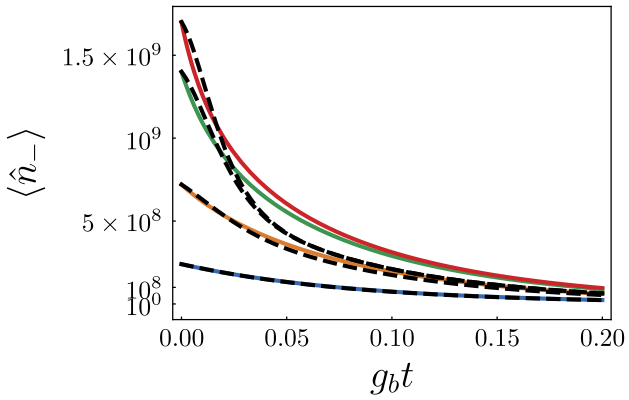


Figure 6.21: Nonlinear decay is observed even in mean-field approximation. Solid: single-mode model. Dashed: multi-mode model. Initial coherent states with $\langle \hat{n}_- \rangle (0) = 1.7 \times 10^9, 1.4 \times 10^9, 7.2 \times 10^8$ and 2.4×10^8 were initialised in mode s_-. Linear loss $\gamma_1 = 11.5$, g_a and g_b optimal and $g_c = 60 m^{-1}$. $U = 8.5 \times 10^{-8}$. Full systems of equations are shown in Sec. E.3 for single-mode, and Sec. E.5 for multi-mode models.

While the mean-field approach is useful for observing the effect of nonlinear decay, it cannot give any insight into the squeezing of photon-number statistics. The Q given by the mean-field approximation is:

$$Q = \frac{\langle \hat{a}^\dagger \hat{a} \hat{a}^\dagger \hat{a} \rangle}{\langle \hat{a}^\dagger \hat{a} \rangle} - 1 = \frac{\langle \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} \rangle - \langle \hat{a}^\dagger \hat{a} \rangle^2}{\langle \hat{a}^\dagger \hat{a} \rangle} = \frac{|\langle \hat{a} \rangle|^4 - |\langle \hat{a} \rangle|^4}{|\langle \hat{a} \rangle|^2}$$

which is identically 0. Note that in this equation we have implicitly used a subtle feature of the mean-field approximation. Since the mean-field approximation cannot capture phenomena arising from different ordering of operators, we must specify that the approximation only applies to expectations of normal-ordered operators.

6.6.2 *Higher-order linearization*

Since the mean-field approximation cannot capture the dynamics of Q we must consider a different approach in order to reduce the order of Eq. 6.47. We will adopt a linearization approach which is typical for consideration of non-linear waveguide systems [224–226]. This is essentially a linearization of the quantum correction to the previous mean-field approach. We will derive the approach and then provide useful formulae which can be substituted into Eq. 6.47 and any similar equation.

Consider arbitrary quantum operators A, B, C. We will explicitly demonstrate how $\langle ABC \rangle$ may be simplified, and then display the results for a generalization to expectations of fourth-order operator products.

Let us expand each operator A, B, C into a mean-field term and a quantum fluctuation term: $A = \langle A \rangle + \delta A$, and we take $\langle \delta A \rangle = 0$ to ensure that $\langle A \rangle$ is well-defined. It is important to note that the $\langle A \rangle$ derived here in general behave differently to those derived in the mean-field approach. Substituting these expansions into $\langle ABC \rangle$,

$$\begin{aligned}&\langle ABC \rangle = \\ &\langle A \rangle \langle B \rangle \langle C \rangle + \langle A \rangle \langle \delta B \delta C \rangle + \langle B \rangle \langle \delta A \delta C \rangle + \langle C \rangle \langle \delta A \delta B \rangle + \langle \delta A \delta B \delta C \rangle .\end{aligned} \tag{6.51}$$

A key tool which we require is the cumulant expansion [227] for a set of generic operators $\{O_1, \ldots, O_n\}$,

$$\mathcal{C}(O_1, \ldots, O_n) = \sum_{\mathcal{P} \in \mathbb{P}} (|\mathcal{P}| - 1)! \, (-1)^{|\mathcal{P}|-1} \prod_{p \in \mathcal{P}} \left\langle \prod_{i \in p} O_i \right\rangle \tag{6.52}$$

where $\mathbb{P}$ denotes all disjoint partitions of the set $\{O_1, \ldots, O_n\}$, $|\mathcal{P}|$ denotes the number of blocks in partition $\mathcal{P}$, and p iterates over each block in the partition. For example,

$$\mathcal{C}(X, Y, Z) = \langle XYZ \rangle + 2 \langle X \rangle \langle Y \rangle \langle Z \rangle - \langle X \rangle \langle YZ \rangle - \langle Y \rangle \langle XZ \rangle - \langle Z \rangle \langle XY \rangle . \tag{6.53}$$

We perform our linearization approximation on Eq. 6.51 by specifying that $\mathcal{C}(\delta A, \delta B, \delta C) = 0$, which implies additionally that $\langle \delta A \delta B \delta C \rangle = 0$, since $\langle \delta A \rangle = \langle \delta B \rangle = \langle \delta C \rangle = 0$ by definition. Finally, using $\delta A = A - \langle A \rangle$ we arrive at our final expression:

$$\langle ABC \rangle \approx \langle A \rangle \langle BC \rangle + \langle B \rangle \langle AC \rangle + \langle C \rangle \langle AB \rangle - 2 \langle A \rangle \langle B \rangle \langle C \rangle . \tag{6.54}$$

Expectations of higher-order operator products may be calculated in the same way, with the only requirements assumed about the fluctuations being the zero-mean condition $\langle \delta A \rangle = \cdots = \langle \delta Z \rangle = 0$ and the assumption on the cumulant of δ-operators[14].

The replacement for fourth-order operators is derived similarly,

$$\langle ABCD \rangle \approx \langle AB \rangle \langle CD \rangle + \langle AC \rangle \langle BD \rangle + \langle AD \rangle \langle BC \rangle - 2 \langle A \rangle \langle B \rangle \langle C \rangle \langle D \rangle \tag{6.55}$$

while the replacements for fifth- and sixth-order operators are not displayed[15]. Thus Eq. 6.47 reduces to (c.f. Eq. 6.49)

$$\frac{d}{dt} \langle \hat{a} \rangle = -\frac{\Gamma}{2} \langle \hat{a} \rangle - i g_a \langle \hat{c}_0 \rangle + 2iU \langle \hat{a}^\dagger \rangle \langle \hat{a} \rangle \langle \hat{a} \rangle - 2iU \langle \hat{a} \rangle \langle \hat{a}^\dagger \hat{a} \rangle - iU \langle \hat{a}^\dagger \rangle \langle \hat{a} \hat{a} \rangle , \tag{6.56}$$

and equations for the remaining expectations are calculated likewise. The full system of equations is shown in Sec. E.6.

14 e.g. for a truncation of the system of equations to third-order, one would instead set $\mathcal{C}(\delta A, \delta B, \delta C) \neq 0$ but $\mathcal{C}(\delta A, \delta B, \delta C, \delta D) = 0$, and so on.

15 Each expansion is derived identically to the third- and fourth-order expressions, but the fifth-order one contains 26 terms, while the sixth-order one contains 31 terms.

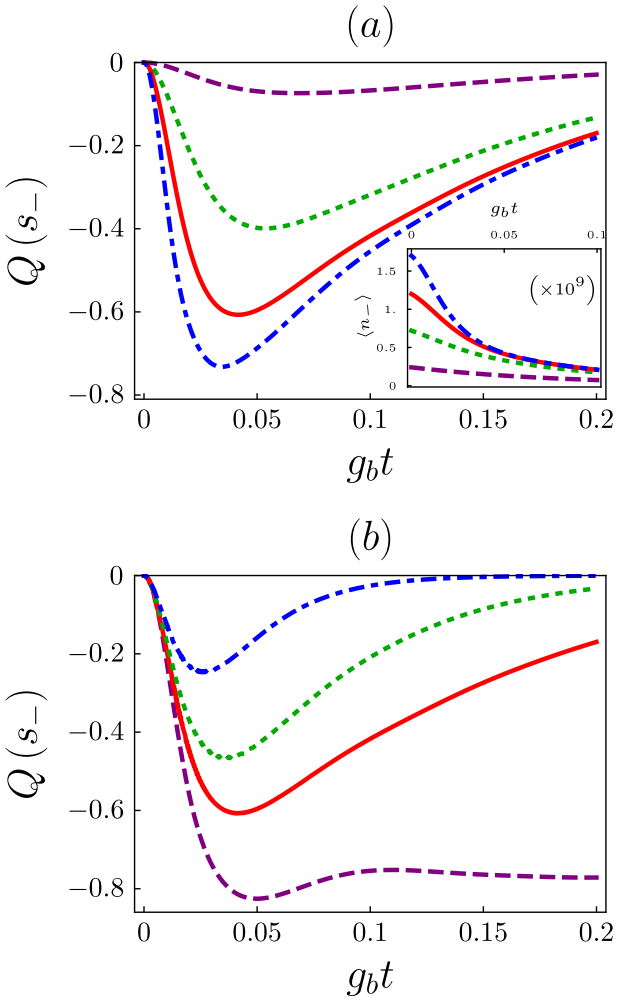


Figure 6.22: With the realistic parameters $U = 8.5 \times 10^{-8}$, $g_c = 60\text{m}^{-1}$, tail length $N = 28$ and optimal coupling ratio Eq. 6.41, the mode s_- quickly evolves to a strongly sub-Poissonian state. A coherent state with average photon number $\langle s_-^\dagger s_- \rangle$ is initialized in mode s_-, and all other modes are initialized into the vacuum. (a) The dot-dashed, solid, dotted, and dashed lines correspond to initial photon numbers 1.7×10^9, 1.2×10^9, 7.2×10^8 and 2.4×10^8, respectively. We take linear loss rate $\gamma_1 = 11.5\text{m}^{-1}$. Inset: the evolution of photon-number expectation, exhibiting the nonlinear decay behaviour of the NCL mechanism. (b) The Mandel Q parameter remains strongly negative even in the presence of realistic linear loss γ_1. The dashed, solid, dotted and dot-dashed lines correspond to $\gamma_1 = 0.0$, 11.5, 20.0, and 40m^{-1}, respectively, and $\langle s_-^\dagger s_- \rangle = 1.2 \times 10^9$.

We may rotate our output equations into the collective s_-, s_+ basis and write Q as

$$Q_{\text{Linearized}}[\hat{s_-}] = \frac{\langle \hat{s_-}^\dagger \hat{s_-}\rangle^2 + \langle \hat{s_-}^\dagger \hat{s_-}^\dagger\rangle \langle \hat{s_-}\hat{s_-}\rangle + \langle \hat{s_-}^\dagger \hat{s_-}\rangle - 2\langle \hat{s_-}^\dagger\rangle^2 \langle \hat{s_-}\rangle^2}{\langle \hat{s_-}^\dagger \hat{s_-}\rangle} - 1. \tag{6.57}$$

We plot the Mandel Q parameter of mode s_- in Fig. 6.22 and observe the characteristic $Q < 0$ behaviour we are aiming for. Even at realistic parameters of small U and large γ_1, desirable $Q \sim -0.8$ is attainable over short timescales for an initial bright coherent state containing 1.7×10^9 photons. This corresponds to an input pulse energy of approximately 320 pJ. The feasibility of these energy levels in the context of our setup is confirmed by the recent work Ref. [228] where waveguides were written using femtosecond pulses with energy greater than 10 nJ at comparable wavelengths.

In Fig. 6.22a we see that the linearized multi-mode model qualitatively obtains the same scaling behaviour of better Q with increasing input α, while γ_1 in Fig. 6.22b causes Q to decay to zero. In the inset of (a) we observe the nonlinear decay characteristic of NCL. The photon-number decay was reproducible in the mean-field approach, while our new linearization approximation allows Q to be captured.

6.6.3 *Comparison to single-mode model*

Finally, we return to the single-mode model, Eq. 6.37, in order to demonstrate the accuracy of our linearization approach. We have demonstrated already that both mean-field and linearization approaches are accurate at modelling the non-linear decay of photon number expectation, and so in Fig. 6.23 we make a comparison of Q under both the linearization approach derived in Sec. 6.6.2 and quantum Monte Carlo on Eq. 6.37. We refer to the reader to Appendix E.1 for more information about this numerical method.

The linearization approximation (dashed lines) accurately predicts the evolution of Q over the initial stages of evolution, and actually underestimates $|Q|$ in the later stages. Including realistic γ_1 allows the approximation to remain accurate as the nonclassical output state is pushed towards the vacuum. Since when $\gamma_1 = 0$ the linearization approximation remains accurate over the timescales of interest, and since the presence of realistic losses makes the approximation increasingly accurate, we may confidently apply the linearization approach over the parameter regimes of interest – short times and realistic loss – even in the case of a large number of modes. Indeed, we may even expect linearization to be more accurate in the multi-mode case than in the single-mode case, since the largest multi-mode expectation which is truncated is originally of fourth-order, as opposed to sixth-order for single-mode.

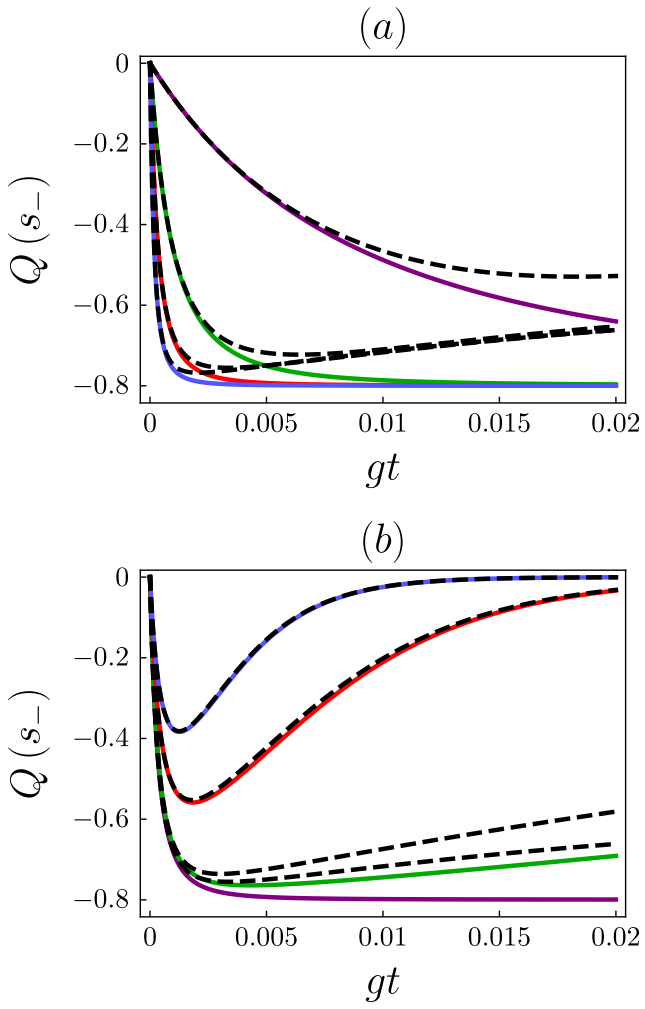


Figure 6.23: Evolution of the Mandel Q parameter is accurately predicted by the linearization method over the initial stages of evolution, while |Q| is underestimated at later stages. Dashed: linearized approximation. Solid: exact solution Eq. 6.37, via quantum Monte Carlo. $U = 2g$ and $\Gamma = 432g$. (a) Initial photon number $\langle \hat{n}_- \rangle = 100, 300, 500, 700$ (top to bottom), with $\gamma_1 = 0$. (b) Initial photon number $\langle \hat{n}_- \rangle = 500$, $\gamma_1 = 0, 20g, 200g, 400g$ (bottom to top). With realistic linear loss rates γ_1 our linearization approximation remains accurate even in the late stages of evolution. Both graphs use the same time scaling gt as Fig. 6.14 ($g = 1$), and solid lines are identical to Fig. 6.14.

We have observed that even the full multi-mode model of the PhoG device, with realistic $U = 8.5 \times 10^{-8}$ and large linear loss γ_1, is capable of producing highly sub-Poissonian light at the output. The main feature of our system which we have exploited is that NCL dominates (i) over short timescales, and (ii) for large photon number. By increasing the input coherent state amplitude we force ourselves into the regime of NCL. The amplitudes require pulse energies ~ 320 pJ which is feasible in similar glasses to IG2 [228].

6.7 MODAL ENTANGLEMENT

In the previous sections we have observed one of the remarkable features of our device: that strong linear loss on one mode of a multimode system, Kerr nonlinearity which is present in $\chi^{(3)}$ materials, and linear coupling, can be arranged and configured in order to simulate useful loss operators. When no linear loss is present in the signal modes of the system, we are able to deterministically generate a single-photon steady-state at the output, while bright strongly sub-Poissonian states are attainable even in the presence of linear loss. We have simulated loss operator $\hat{A} = \hat{a}\left(\hat{a}^\dagger \hat{a} - 1\right)$ in our system, which required very asymmetric coupling $g_a \gg g_b$ or $g_a \ll g_b$ (c.f. Eq. 6.38).

In this section, we will explore the quantum effects which occur when this asymmetry is not met. Let us return to the two-mode model of the PhoG device (Eq. 6.33, Fig. 6.16) and set $g_a = g_b$. This will mean that the rate γ_{NCL} of NCL simulated by this model is now zero, and so we cannot expect to reach strongly sub-Poissonian light, except in the limit[16] $\gamma_1 \to 0$.

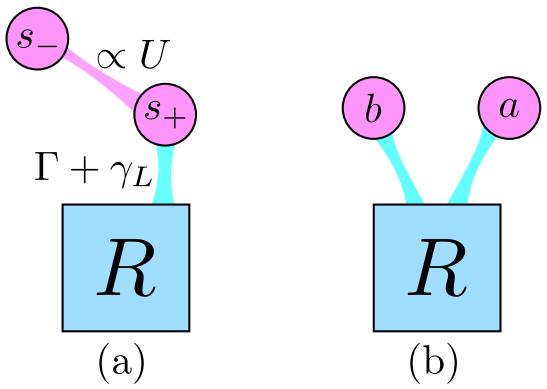


Figure 6.24: Two-mode model of PhoG device. (a) Collective basis s_-, s_+, Eq. 6.33. (b) Signal basis a, b, Eq. 6.31

However, even this symmetric system exhibiting two-photon absorption can be useful for generation of non-classical states. We will demonstrate that a symmetric PhoG device is capable to produce entanglement shared between signal modes a and b. The system we

16 The steady-state of $\hat{A} = \hat{a}^2$ has $Q = -0.5$

consider is displayed in Fig. 6.24. Because we wish to allow for large photon-numbers, we must resort to the linearized model described in Sec. 6.6.2. This leaves us in a perfect position to access first- and second-order expectations of creation and annihilation operators, and thus consider the Gaussian entanglement shared between modes a and b [13, 229, 230].

We proceed as follows. After using our linearization method to solve for expectations of the form $\langle \hat{a} \rangle$, $\langle \hat{a}^\dagger \hat{a} \rangle$, $\langle \hat{a} \hat{b} \rangle$, etc., we transform these quantities into expectations of quadrature operators, Eq. 1.21. So, for example, we form expectations as

$$\begin{aligned} \langle \hat{x}_a \rangle &= \frac{\langle \hat{a} \rangle + \langle \hat{a}^\dagger \rangle}{\sqrt{2}}, \\ \langle \hat{p}_a \rangle &= \frac{i \left(\langle \hat{a}^\dagger \rangle - \langle \hat{a} \rangle \right)}{\sqrt{2}}, \\ &\text{etc.} \end{aligned}$$

Crucially, we can access second-order expectations such as

$$\begin{aligned} \langle \hat{x}_a \hat{x}_a \rangle &= \frac{1}{2} \left[\left\langle \hat{a}^\dagger \hat{a}^\dagger \right\rangle + \langle \hat{a} \hat{a} \rangle + 2 \left\langle \hat{a}^\dagger \hat{a} \right\rangle + 1 \right], \\ \langle \hat{x}_a \hat{p}_b \rangle &= \frac{i}{2} \left[\left\langle \hat{a}^\dagger \hat{b}^\dagger \right\rangle + \left\langle \hat{b}^\dagger \hat{a} \right\rangle - \left\langle \hat{a}^\dagger \hat{b} \right\rangle - \langle \hat{a} \hat{b} \rangle \right], \\ &\text{etc.} \end{aligned}$$

Therefore, we can to construct a covariance matrix σ which describes the quadrature correlations between modes a and b [13]. The matrix element $\sigma_{j,k}$ is constructed as

$$\sigma_{j,k} = \frac{1}{2} \left[\langle d_j d_k \rangle + \langle d_k d_j \rangle \right] - \langle d_j \rangle \langle d_k \rangle \tag{6.58}$$

with vector $\overrightarrow{d} = [\hat{x}_a, \hat{p}_a, \hat{x}_b, \hat{p}_b]$.

The Gaussian entanglement between modes a and b may then be calculated in terms of $\sigma_{j,k}$ via the Gaussian logarithmic negativity, $\mathcal{N}_G$ [229, 230]. This entanglement measure $\mathcal{N}_G$ quantifies the extent to which the state ρ described by σ fails the positive partial transpose (PPT) criterion [230, 231]. Taking the positive partial transpose of mode b, $\rho \to \rho^{T_B}$, the covariance matrix transforms as [230]

$$\begin{aligned} \hat{x}_a &\to \hat{x}_a \\ \hat{p}_a &\to \hat{p}_a \\ \hat{x}_b &\to \hat{x}_b \\ \hat{p}_b &\to -\hat{p}_b \end{aligned}$$

and we write $\tilde{\sigma}$ as this transformed covariance matrix corresponding to ρ^{T_B}.

The measure $\mathcal{N}_G$ is then defined as[17]

$$\mathcal{N}_G = \max\left\{0, -\log\tilde{\lambda}\right\} \tag{6.59}$$

where $\tilde{\lambda}$ is the smallest symplectic eigenvalue of $\tilde{\sigma}$.

We calculate $\mathcal{N}_G$ and plot it in Fig. 6.25. For example, for $\left\langle \hat{a}^\dagger \hat{a} \right\rangle(0) = \left\langle \hat{b}^\dagger \hat{b} \right\rangle(0) = 2500$, $U = 2g$, $\gamma_c = 15g$, $\gamma_1 = 11.5g$ and symmetric coupling $g_a = g_b = 60g$ (we take $g = 1$), the system evolves to $\mathcal{N}_G \approx 1.25$ within $t \sim 0.01g$, while modes a and b each contain approximately 18 photons. The maximally entangled state (TMSV Eq. 1.51) requires squeezing parameter $\zeta = 0.62$ and thermal photon number $\bar{n} = 0.44$ to give the same $\mathcal{N}_G$, while a TMSV with $\bar{n} = 18$ gives $\mathcal{N}_G = 4.3$.

Thus, we see that the symmetric PhoG is able to generate entanglement between modes a and b over the intial stages of dynamics, even though it cannot produce photon-number squeezing.

17 Note the similarities between this and the logarithmic negativity [231] which is defined directly in terms of ρ^{T_B}.

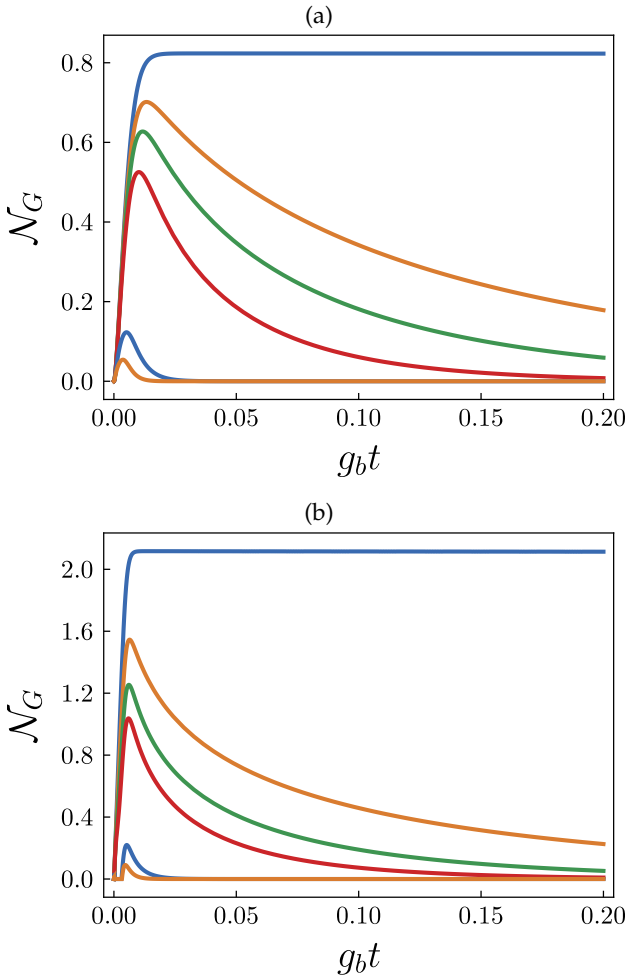


Figure 6.25: Attainable logarithmic negativities $\mathcal{N}_G$ in the symmetric two-mode PhoG device. (a) Modes a and b each initialized in coherent states with 200 photons. Symmetric coupling $g_a = g_b = 10$, $\Gamma = 432$ $U = 2.0$ for comparison with Fig. 6.13. $\gamma_1 = 0$, 5, 10, 20, 200, 400m^{-1}. (top to bottom). (b) Modes a and b each initialized in coherent states with 2500 photons. Symmetric coupling $g_a = g_b = 60$, $\Gamma = 1087$, $\gamma_1 = 0$, 5, 11.5, 20, 200, 400m^{-1}. $U = 2.0$.

6.8 OUTLOOK

In this Chapter we have introduced and analysed a device, which we name PhoG, which is capable to produce highly non-classical states at its output. The device requires just a coherent state at the input. Depending on whether the device is configured with asymmetric signal mode coupling (Secs. 6.2-6.6) or symmetric signal mode coupling (Sec. 6.7) the device produces either a strongly photon-number squeezed (sub-Poissonian) state, or an entangled state. In the limit of no linear loss, $\gamma_1 \to 0$, the sub-Poissonian output of the asymmetric PhoG tends towards a single-photon Fock state. However, even with realistic loss and realistic levels of nonlinearity, the device is predicted to create bright output states which are strongly sub-Poissonian, with feasible predicted Mandel parameter $Q \gtrsim -0.8$.

The device relies on realising an exotic form of dissipation, known as Nonlinear Coherent Loss (NCL), and which is simulated in our realistic multi-mode system via strong linear loss (realised by the waveguide "tail") and Kerr nonlinearity. Our hierarchy of models agree in their observation of the two key behaviours of NCL and so we are confident that $Q < 0$ should be observable in a full, finished device. Our design of the PhoG device with a system of waveguides laser-inscribed into bulk IG2 glass should serve as a practical design for such deterministic sources of non-classicality. Since the glass is comparatively inexpensive, since the device itself relatively easy to produce, and since coherent states are deemed a "cheap" quantum state to use, the PhoG device can find applications as a ready source of nonclassicality for different imaging, measurement and metrology tasks [232, 233].

In future work, we desire to undertake further modelling of the realistic multimode PhoG device described in Sec. 6.6, in order to relax several simplifying assumptions which we have made in this chapter. The assumption made in Sec. 6.5, that the pulse shape is unchanging over the course of evolution, seems unrealistic in a realistic system in which linear (evanescent) coupling, self-phase modulation and dispersion are all present. It should therefore be directly verified what impact the inclusion of these effects has in a system where the pulse shape is permitted to change. Furthermore, the pulse durations of approx 100 fs considered in this Chapter are on the threshold for when higher-order effects such as Raman scattering should be considered.

We have recently begun some preliminary work on this question. In particular, we have begun investigating the spectral and temporal properties of a pulse in a system identical to the multi-mode one, Sec. 6.6, including chromatic dispersion, self-phase modulation and self-steepening. We solve the so-called nonlinear Schrödinger equation (NLSE):

$$\frac{\partial A_j}{\partial z} + i\beta_1 \frac{\partial A_j}{\partial \tau}_i \frac{\beta_2}{2}\frac{\partial^2 A_j}{\partial \tau^2} - \frac{\beta_3}{6}\frac{\partial^3 A_j}{\partial \tau^3} + \frac{\gamma_1}{2} = i\gamma_{NL}\left(1 + \frac{i}{\omega_0}\frac{\partial}{\partial \tau}\right)|A_j|^2 A_j - ig_{j,k}A_k \tag{6.60}$$

where $A_j(z,\tau)$ is the pulse envelope in the j^{th} waveguide, γ_1 is the linear loss parameter, γ_{NL} is the nonlinearity parameter given by

$$\gamma_{NL} = \frac{n_2\omega_0}{cA_{eff}}, \tag{6.61}$$

ω_0 is the carrier frequency of the pulse, $g_{j,k}$ describes coupling between waveguide j and waveguide k, and the β are the first-, second-, and third-order dispersion terms. The propagation direction is z and this equation is valid in a frame co-moving with the pulse, with intra-pulse coordinate τ. This equation may be solved via the split-step Fourier method [197].

One should note that Eq. 6.60 is an entirely classical equation describing the evolution of the pulse's envelope A, and so cannot give us direct information about quantum effects such as the photon-number statistics or entanglement properties. However we have begun to observe NL decay of the pulse energies contained within the signal modes [221], and this provides a hopeful signature that NCL may indeed be present.

There are several methods which may be used to quantize Eq. 6.60, such as the back-propagation method [234–236] or a coarse-grained approach [224, 226, 237–239]. An immediate next step will be to employ either of these methods and check whether we indeed observe a Mandel parameter $Q < 0$. The coarse-grained approach has been successfully applied to similar systems and it has been observed [226] that a similar setup can induce spectral entanglement within the pulse. If this can be observed for our PhoG device it will be another proof of its versatility to generate a broad array of nonclassical behaviours, deterministically from a quasi-classical input.

Part III

APPENDICES

A

CRYPTOGRAPHY: THERMAL NOISE CHANNEL

In this Appendix we will demonstrate how channel thermal noise affects honest players' measurement outcomes. This will allow us to give an expression for the excess noise ξ, as it is modelled in this Thesis.

In Appendix B we introduce an expansion of the coherent state in Fock basis, and use it to demonstrate that enacting a beamsplitter on a coherent state gives a product of coherent states at output. It turns out to be analytically tricky to perform similar operations in the presence of thermal noise (though it is entirely numerically feasible).

Our main tool will be the Wigner function representation of the quantum states. We will introduce various quantities and relations as we need them, but the reader is referred to Refs. [1, 14, 36] for a more thorough discussion of where such quantities come from. Our strategy is to mix a coherent state with a thermal state on a beamsplitter, which will model the channel. We will then heterodyne on the output in order to give a final expression for the measurement outcomes.

MODELLING THE CHANNEL A coherent state $|\alpha\rangle$ with complex amplitude $\alpha = (q_0 + ip_0)/\sqrt{2}$ has Wigner function

$$W_{\text{coh}}(q,p) = \frac{1}{\pi}\exp\left[-(q-q_0)^2-(p-p_0)^2\right], \tag{A.1}$$

while a thermal state ρ_{thermal} with thermal photon number $\bar{n}$ has Wigner function

$$W_{\text{thermal}}(q,p) = \frac{1}{\pi(2\bar{n}+1)}\exp\left[-\frac{q^2+p^2}{2\bar{n}+1}\right]. \tag{A.2}$$

The total input Wigner function to the beamsplitter is therefore

$$W_{\text{input}}(q_1,p_1;q_2,p_2) = W_{\text{coh}}(q_1,p_1)\,W_{\text{thermal}}(q_2,p_2). \tag{A.3}$$

The output Wigner function from the beamsplitter is [1]

$$W_{\text{output}}(q_1,p_1;q_2,p_2) = W_{\text{input}}(q_1',p_1';q_2',p_2') \tag{A.4}$$

where the primed quantities are

$$\begin{pmatrix} q_1' \\ q_2' \end{pmatrix} = \begin{pmatrix} \tau & \rho \\ -\rho & \tau \end{pmatrix}\begin{pmatrix} q_1 \\ q_2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} p_1' \\ p_2' \end{pmatrix} = \begin{pmatrix} \tau & \rho \\ -\rho & \tau \end{pmatrix}\begin{pmatrix} p_1 \\ p_2 \end{pmatrix}. \tag{A.5}$$

In other words, the beamsplitter simply enacts a rotation on the quadrature variables, and the output Wigner function takes the same form as the input Wigner function in the rotated quadratures. We have $\tau = \sqrt{T}$ and $\rho = \sqrt{1-T}$ where T is the channel transmission.

Our output Wigner function is

$$W_{\text{output}}(q_1, p_1; q_2, p_2) = \frac{1}{\pi^2 (2\bar{n}+1)} \exp\left[\left(-1 + T - \frac{T}{2\bar{n}+1}\right)(q_2 - \delta)^2\right] \times \exp[B_{q_2}] \times \quad \text{terms in } p, \tag{A.6}$$

where δ takes a complicated form (not shown) in terms of T, q_0, q_1 and $\bar{n}$, and

$$B_{q_2} = -\frac{\left(q_1 - q_0\sqrt{T}\right)^2}{1 + 2\bar{n}(1-T)}. \tag{A.7}$$

In the protocols discussed in the main Thesis body, the transmitted state is given to the honest player, while the dishonest player receives the reflected state. Tracing out the reflected state (mode 2) we arrive at

$$W_{\text{honest}}(q, p) = \frac{1}{\pi[1 + 2\bar{n}(1-T)]} \exp\left[-\frac{\left(q - q_0\sqrt{T}\right)^2}{1 + 2\bar{n}(1-T)} - \frac{\left(p - p_0\sqrt{T}\right)^2}{1 + 2\bar{n}(1-T)}\right], \tag{A.8}$$

as the state held by the honest player after the thermal channel.

HETERODYNE MEASUREMENT The honest player performs heterodyne measurement on their state. As we saw in Sec. 1.4.2, heterodyne measurement corresponds to projection onto a coherent state [13, 14]. It will be illustrative to show that this is equivalent to a "double-homodyne" setup.

To perform the double-homodyne measurement, the state will be split at on a balanced beamsplitter. Homodyne detection in q is performed on one output arm, while homodyne detection in p is performed on the other output arm.

The calculation proceeds identically to the previous section: rotation of quadrature variables then tracing out the unwanted mode. The first output mode from the balanced beamsplitter is then given by

$$W_1(q, p) = \frac{1}{\pi[1 + \bar{n}(1-T)]} \exp\left[-\frac{\left(q - q_0\sqrt{\frac{T}{2}}\right)^2}{1 + \bar{n}(1-T)} - \frac{\left(p - p_0\sqrt{\frac{T}{2}}\right)^2}{1 + \bar{n}(1-T)}\right], \tag{A.9}$$

and the second output mode is identical.

Ideal homodyne measurement corresponds to projection onto a quadrature eigenstate, i.e. $\langle q|\rho|q\rangle$ [13, 14]. It can be shown [1] that in

terms of Wigner functions, the overlap between two operators is given by

$$\mathrm{tr}\left[\hat{F}_1\hat{F}_2\right] = 2\pi\iint_{-\infty}^{\infty} dq\, dp\, W_1(q,p)\, W_2(q,p), \tag{A.10}$$

where the $\hat{F}_1, \hat{F}_2$ are arbitrary operators, and their corresponding Wigner functions are W_1, W_2.

The Wigner function corresponding to quadrature eigenstate $|q_1\rangle$ is

$$W_{|q_1\rangle}(q,p) = \frac{1}{2\pi} e^{2ip(q_1-q)}\delta(q_1-q) \tag{A.11}$$

where $\delta(q_1-q)$ is the Dirac delta function, and the overall Wigner function is derived by substituting $\rho = |q_1\rangle\langle q_1|$ into Wigner's formula Eq. 1.28 and using $\langle q|q'\rangle = \delta(q-q')$.

The probability to receive homodyne outcome $q_{out} = x$ on W_1 is then

$$P(x) = \mathrm{tr}\left[|x\rangle\langle x|\,\rho\right] = \frac{1}{\sqrt{\pi\left[1+\bar{n}(1-T)\right]}} \exp\left[-\frac{\left(x - q_0\sqrt{\frac{T}{2}}\right)^2}{1+\bar{n}(1-T)}\right]. \tag{A.12}$$

Similarly, the probability to measure y on the other output mode is

$$P(y) = \mathrm{tr}\left[|y\rangle\langle y|\,\rho\right] = \frac{1}{\sqrt{\pi\left[1+\bar{n}(1-T)\right]}} \exp\left[-\frac{\left(y - p_0\sqrt{\frac{T}{2}}\right)^2}{1+\bar{n}(1-T)}\right]. \tag{A.13}$$

Defining the complex variable $z = x + iy$, and noting that $P(z) = P(x)\,P(y)$, we arrive at

$$P(z) = \frac{1}{\pi\left[1+\bar{n}(1-T)\right]} \exp\left[-\frac{\left|z - \sqrt{T}\alpha\right|^2}{1+\bar{n}(1-T)}\right], \tag{A.14}$$

where we have used $\alpha = (q_0 + ip_0)/\sqrt{2}$.

The equation A.14 is the probability of heterodyne measurement giving z, when an input coherent state α is distributed through a thermal noise channel, transmission T and thermal photon number $\bar{n}$. Setting $\bar{n} = 0$, Eq. A.14 reduces to the noiseless case which is used already in the Thesis body.

For a QDS protocol the probability p_{err} may be calculated via Eq. A.14 identically to the Thesis body.

Excess noise

We define the excess noise ξ as the measured variance of a state above the vacuum level. In Ch. 5 we defined it as

$$\xi = \mathrm{Var}(x) - \frac{1}{2}, \tag{A.15}$$

where clearly from Eq. A.12 (setting $\bar{n} = 0$) the vacuum variance is $1/2$. The variance in position homodyne measurement outcome is

$$\frac{1 + \bar{n}(1-T)}{2}, \tag{A.16}$$

and so excess noise in q is

$$\xi_q = \frac{\bar{n}(1-T)}{2}, \tag{A.17}$$

with an equivalent expression for ξ_p. In Chs. 3, 4 we assume that $\xi_q = \xi_p$ and simply call the excess noise ξ,

$$\xi = \frac{\bar{n}(1-T)}{2}. \tag{A.18}$$

Finally, we note that ξ depends both on $\bar{n}$ and T. For a given ξ the corresponding $\bar{n}$ varies with T, and fixing $\bar{n}$ will give drastically different behaviour from fixing ξ. Thus, we are careful to distinguish between channels for which $\bar{n}$ is fixed and those for which ξ is fixed.

B

CRYPTOGRAPHY: NUMERICAL METHODS

B.1 TRUNCATION

In this Appendix we display the full form of the quantum states which are used in Chapter. 3 to analyse eavesdropping attacks. Each state is calculated as described in Sec. 3.6, and is conditioned on the honest player possessing $c = q_{out} + ip_{out} \in \mathbb{C}$, for heterodyne outcomes q_{out}, p_{out}.

We denote each state as $\tilde{\rho}_{\mathbb{B}\,|\,c}$, where $\mathbb{B}$ denotes that the state belongs to dishonest Bob, while $\mathbb{B}\,|\,c$ makes explicit that this state depends on c. Since each state $\tilde{\rho}_{\mathbb{B}\,|\,c}$ is a conditional quantum state [16], they have norm $\mathrm{tr}\left[\tilde{\rho}_{\mathbb{B}\,|\,c}\right] \leqslant 1$. The $\mathrm{tr}\left[\tilde{\rho}_{\mathbb{B}\,|\,c}\right] = P(c)$ is the probability that Charlie measures c. The tilde denotes that the state is sub-normalized, and we will define the normalized state as

$$\rho_{\mathbb{B}\,|\,c} := \frac{\tilde{\rho}_{\mathbb{B}\,|\,c}}{P(c)}. \tag{B.1}$$

It is the normalized forms $\rho_{\mathbb{B}\,|\,c}$ which are used in the main body of this Thesis.

Each of the states required to calculate Holevo information χ involves sums of the form

$$\sum_{n=0}^{\infty}, \tag{B.2}$$

since each state lives in a Hilbert space $\mathcal{H}$ with a countably infinite dimensionality $|\mathcal{H}|$. It is impossible to exactly encode such a state numerically, and so we must resort to a truncation of the Hilbert space size to some large but finite $|\mathcal{H}| = N$, i.e.

$$\sum_{n=0}^{\infty} \to \sum_{n=0}^{N}. \tag{B.3}$$

We will briefly discuss such truncation again in Appendix E in the context of the PhoG chapter. It is still an open question [141] as to whether this will afford an eavesdropper additional powers. In lieu of an answer to this, whenever we numerically encode any of the following states we will choose $|\mathcal{H}|$ large enough such that the state living on the truncated space is normalized. Additionally, in each of the calculations in the main body of this Thesis, we gradually increased the Hilbert space size $|\mathcal{H}|$ until we converged to a a constant output χ which does not further vary with $|\mathcal{H}|$. For a coherent state amplitude $\alpha \leqslant 2$ we typically chose $|\mathcal{H}| \lesssim 10$, though we note that often much smaller $|\mathcal{H}|$ were often possible (Tab. E.1). We note that this

strategy is the same one as was adopted in the recent state-of-the-art work Ref. [141].

Each of the following expressions for output states $\tilde{\rho}_{\mathbb{B}\,|\,c}$ were encoded in the displayed Fock basis in a custom script[1] in Mathematica 11.3. The overall state is then a matrix in $\mathcal{M}_{|\mathcal{H}|\times|\mathcal{H}|}(\mathbb{C})$. The Von Neumann entropy $S(\bullet)$ of the state is found by taking eigenvalues and using Eq. 1.83.

B.2 ATTACK BS0

Beamsplitter attack BS0 is described in Sec. 3.6.1. The total input state into the channel is

$$\rho_{\text{input}} = \frac{1}{4}\sum_{k} |\alpha_k\rangle\langle\alpha_k|_A \otimes |0\rangle\langle 0|_B \tag{B.4}$$

where

$$|\alpha_k\rangle_A = e^{-\frac{|\alpha_k|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha_k^n}{\sqrt{n!}} |n\rangle_A \tag{B.5}$$

is Alice's input coherent state, with α_k chosen from the QPSK alphabet.

Enacting beamsplitter relation Eq. 1.57 on ρ_{input} and performing heterodyne detection on Charlie's mode, we arrive at

$$\begin{aligned}\tilde{\rho}_{\mathbb{B}\,|\,c} = \sum_{k} \frac{1}{\pi} e^{-|\alpha_k|^2} e^{-|c|^2} \sum_{n,m=0}^{\infty} \sum_{k,l=0}^{n,m} \frac{\alpha^n \alpha^{*m}}{\sqrt{k!\,(n-k)!}} \frac{c^k c^{*l}}{\sqrt{k!l!}} \\ \times \frac{\left(\sqrt{T}\right)^{k+l} \left(\sqrt{1-T}\right)^{n+m-k-l}}{\sqrt{l!\,(m-l)!}} |n-l\rangle\langle m-l|.\end{aligned} \tag{B.6}$$

Rearranging[2] the summation indices we arrive at Eq. 3.41 from the main body.

B.3 ATTACK BS1

Beamsplitter attack BS1 is described in Sec. 3.6.1. The total input state into the channel is

$$\rho_{\text{input}} = \frac{1}{4}\sum_{k} |\alpha_k\rangle\langle\alpha_k|_A \otimes \rho_{\text{thermal}}. \tag{B.7}$$

with

1 Making extensive use of the `SparseArray[]` function for speed.
2 See e.g. page 142 of Ref. [3]

$$|\alpha_k\rangle_A = e^{-\frac{|\alpha_k|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha_k^n}{\sqrt{n!}} |n\rangle_A \quad \text{and}$$
$$\rho_{\text{thermal}} = \left(1 - e^{-\tilde{\beta}}\right) \sum_{p=0}^{\infty} e^{-p\tilde{\beta}} |p\rangle\langle p|_B \quad \text{with} \quad \tilde{\beta} = \log_e\left(\frac{1}{\bar{n}} + 1\right) \tag{B.8}$$

Enacting beamsplitter relation Eq. 1.57 on ρ_{input} and heterodyning on Charlie's mode we arrive at

$$\begin{aligned}\tilde{\rho}_{B|c} &= \sum_k \frac{e^{-|\alpha_k|^2}}{\pi} e^{-|c|^2} \left(1 - e^{-\tilde{\beta}}\right) \sum_{n,m,p=0}^{\infty} \frac{\alpha^n \alpha^{*m}}{\sqrt{n!m!}} e^{-p\tilde{\beta}} \\ &\times \sum_{k_1,k_2,l_1,l_2=0}^{n,p,m,p} c^{k_1+k_2} (c^*)^{l_1+l_2} \binom{n}{k_1} \binom{p}{k_2} \binom{m}{l_1} \binom{p}{l_2} \left(\sqrt{T}\right)^{k_1+l_1} \\ &\times \left(\sqrt{1-T}\right)^{n+m-k_1-l_1} \left(-\sqrt{1-T}\right)^{k_2+l_2} \left(\sqrt{T}\right)^{2p-k_2-l_2} \sqrt{(n+p-k_1-k_2)!} \\ &\times \sqrt{(m+p-l_1-l_2)!}\, |n+p-k_1-k_2\rangle\langle m+p-l_1-l_2| \,. \end{aligned} \tag{B.9}$$

B.4 ATTACK EC

Entangling cloner attack EC is described in Sec. 3.6.2. The total input state into the channel is

$$\rho_{\text{input}} = \frac{1}{4} \sum_k |\alpha_k\rangle\langle\alpha_k|_A \otimes |\text{TMSV}\rangle\langle\text{TMSV}|_B \,, \tag{B.10}$$

with Alice's coherent state

$$|\alpha_k\rangle_A = e^{-\frac{|\alpha_k|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha_k^n}{\sqrt{n!}} |n\rangle_A \tag{B.11}$$

and Bob's two-mode squeezed vacuum state

$$|\text{TMSV}\rangle = \frac{1}{\cosh\zeta} \sum_{n=0}^{\infty} (\tanh\zeta)^n |n,n\rangle_B \,. \tag{B.12}$$

Enacting beamsplitter relation Eq. 1.55 on ρ_{input} and heterodyning on Charlie's mode, we arrive at

$$\begin{aligned}\tilde{\rho}_{B|c} &= \sum_k \frac{e^{-|\alpha_k|^2}}{\cosh^2\zeta} \frac{e^{-|c|^2}}{\pi} \sum_{n_1,m_1,n_2,m_2=0}^{\infty} \sum_{k_1,k_2=0}^{n_1,n_2} \sum_{l_1,l_2=0}^{m_1,m_2} \alpha^{n_1} \alpha^{*m_1} (\tanh\zeta)^{n_2+m_2} \\ &\times c^{k_1+k_2} (c^*)^{l_1+l_2} \sqrt{n_2!m_2!} \left(\sqrt{T}\right)^{k_1+l_1} \left(\sqrt{1-T}\right)^{n_1+m_1-k_1-l_1} \left(-\sqrt{1-T}\right)^{k_2+l_2} \\ &\times \left(\sqrt{T}\right)^{n_2+m_2-k_2-l_2} \frac{\sqrt{(n_1+n_2-k_1-k_2)!}\sqrt{(m_1+m_2-l_1-l_2)!}}{k_1!k_2!l_1!l_2!\,(n_1-k_1)!\,(n_2-k_2)!\,(m_1-l_1)!\,(m_2-l_2)!} \\ &\times |n_1+n_2-k_1-k_2\rangle\langle m_1+m_2-l_1-l_2| \otimes |n_2\rangle\langle m_2| \,. \end{aligned} \tag{B.13}$$

C

CRYPTOGRAPHY: LARGER QDS ALPHABETS

In this appendix we will demonstrate how the QDS protocol discussed in Chapter 3 may be modified to allow for a general NPSK alphabet of N coherent states equally distributed around the origin of phase space. We display an example of an NPSK alphabet in Fig. 1.4. For reasons which will become clear, we are forced to take $N = 2k, k \in \mathbb{N}$. The QPSK alphabet used throughout this Thesis is simply an NPSK alphabet with $N = 4$.

During the protocol with NPSK alphabet, Bob and Charlie eliminate precisely $N/2$ coherent states to form their eliminated signature, using the same strategy as in Fig. 3.4. This means for example that the integration limits used for a particular eliminated signature element should vary. Besides this, the running of the protocol remains identical.

As before, our starting point is the entropy $H\left(\mathcal{E}_j, y_1^j, \ldots, y_{N/2}^j \,\middle|\, \phi_j\right)$ (c.f. Eq. 3.29). We use the chain rule for conditional entropies twice, giving

$$H\left(y_1^j, \ldots, y_{N/2}^j \,\middle|\, \phi_j\right) = H\left(y_1^j, \ldots, y_{N/2}^j \,\middle|\, \mathcal{E}_j, \phi_j\right) + H\left(\mathcal{E}_j \mid \phi_j\right) \tag{C.1}$$

once we have taken into account that $H\left(\mathcal{E}_j \,\middle|\, y_1^j, \ldots, y_{N/2}^j, \phi_j\right) = 0$. Using $H\left(\mathcal{E}_j \mid \phi_j\right) \leqslant h\left(p_e\right)$ and the fact that Bob and Charlie eliminate exactly $N/2$ out of N possible alphabet states, we arrive at

$$H\left(y_1^j, \ldots, y_{N/2}^j \,\middle|\, \phi_j\right) \leqslant H\left(y_1^j, \ldots, y_{N/2}^j \,\middle|\, \mathcal{E}_j = 0, \phi_j\right) + h\left(p_e\right), \tag{C.2}$$

and therefore

$$\begin{aligned} &H\left(y_1^j, \ldots, y_{N/2}^j\right) - \chi\left(y_1^j, \ldots, y_{N/2}^j : \phi_j\right) \\ &\quad \leqslant H\left(y_1^j, \ldots, y_{N/2}^j \,\middle|\, \mathcal{E}_j, \phi_j\right) + h\left(p_e\right). \end{aligned} \tag{C.3}$$

To complete our proof we simply observe

$$\begin{aligned} H\left(y_1^j, \ldots, y_{N/2}^j\right) &= \log 2\left(N \times \frac{N}{2}!\right), \\ H\left(y_1^j, \ldots, y_{N/2}^j \,\middle|\, \mathcal{E}_j, \phi_j\right) &= \log 2\left(\frac{N}{2} \times \frac{N}{2}!\right) \end{aligned} \tag{C.4}$$

where we have taken into account the ability to relabel elements y_n^j of the eliminated signature. The equation

$$h\left(p_e\right) \geqslant 1 - \chi\left(y_1^j, \ldots, y_{N/2}^j : \phi_j\right) \tag{C.5}$$

follows immediately (c.f. Eq. 3.40).

The quantities used to calculate the Holevo information $\chi\left(y_1^j, \ldots, y_{N/2}^j : \phi_j\right)$ must also be altered to reflect the NPSK alphabet. Alice's input state into the channel becomes

$$\frac{1}{N}\sum_{k=0}^{N-1} |\alpha_k\rangle\langle\alpha_k|_A\,, \tag{C.6}$$

from which all other quantities may be calculated.

We display the signature length L under several different NPSK alphabets in Fig. C.1. At each channel transmission T the signature length has been optimized over α. Choosing an alphabet size larger than $N = 4$ decreases the optimal α_{opt} while slightly increasing the required signature length L. As the alphabet size increases it becomes closer to a Gaussian distribution, and so the beamsplitter and entangling-cloner attacks become increasingly optimal. The largest jump in protocol efficiency occurs from $N = 2$ to $N = 4$.

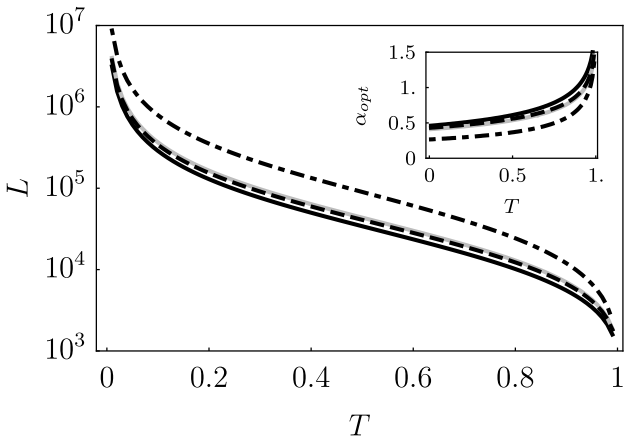


Figure C.1: Signature length L under QDS protocol discussed in Chapter 3 under BS0 attack. At each T, length L has been optimized over amplitude $|\alpha|$ of the alphabet. We have considered NPSK alphabets with $N = 2, 4, 6, 8$. Dot-dashed: $N = 2$. Black, solid: $N = 4$. Dashed: $N = 6$. Gray, solid: $N = 8$. Inset: the corresponding optimal α_{opt}.

D

PHOG: ADIABATIC ELIMINATION

In this appendix we will derive Eq. D.14 which is used in Sec. 6.4 to simplify the analytical description of a multi-mode bosonic system when one of the modes takes its steady-state. Our analysis will use notation following Ref. [216].

Consider a system involving a highly lossy bosonic mode, c. We assume that c decays into a Markovian reservoir with decay rate γ, and that the system contains additional modes with possible losses, couplings and nonlinearities.

After $t \gg 1/\gamma$ the mode c is empty, and it is assumed that this timescale is much faster than all other timescales in the system. Then, for $t \gg 1/\gamma$ the mode c can be assumed to be in its steady-state and so, for example, $\frac{d}{dt}\hat{c} = 0$. This will be used in order to simplify the description of our original system.

The Lindblad master equation for our entire system is

$$\frac{d}{dt}\rho = -i\left[\hat{H}, \rho\right] + \gamma\mathcal{L}\left[\hat{c}\right]\rho + \Gamma_j\mathcal{L}\left[f\left(\hat{a}_j\right)\right]\rho, \tag{D.1}$$

where ρ is the density matrix describing the entire system and $\hat{H}$ is the system's Hamiltonian, on which we will later derive some restrictions. The term proportional to γ denotes strong loss of mode c into the reservoir, and the term in Γ denotes potential other sources of loss which do not affect c. We shall ignore terms in Γ_j until the very last step, since they do not affect our analysis and will always be present.

It is easiest to proceed in Heisenberg picture, and so we transform to the adjoint master equation [15] which describes the evolution of an arbitrary operator $\hat{A}$

$$\frac{d}{dt}\hat{A} = i\left[\hat{H}, \hat{A}\right] + \gamma\mathcal{L}\left[\hat{c}^\dagger\right]\hat{A} + \Gamma_j\mathcal{L}\left[f\left(\hat{a}_j\right)^\dagger\right]\hat{A}, \tag{D.2}$$

and expand $\hat{H}$ and $\hat{A}$ in terms of normal-ordered powers of creation and annihilation operators of the lossy mode

$$\hat{H} = \sum_{p,q=0}^{\infty} \hat{H}^{(p,q)}\left(\hat{c}^\dagger\right)^p \hat{c}^q, \tag{D.3}$$

$$\hat{A} = \sum_{p,q=0}^{\infty} \hat{A}^{(p,q)}(t)\left(\hat{c}^\dagger\right)^p \hat{c}^q. \tag{D.4}$$

Operators $\hat{H}^{(p,q)}, \hat{A}^{(p,q)}$ are, in general, operators acting on the remaining modes of the system. Let us take Eqs. D.3, D.4 and substitute into Eq. D.2. Grouping terms in $\hat{c}^\dagger, \hat{c}$ we see that

$$\frac{d}{dt}A^{(m,n)}(t)\,c^{\dagger m}c^{n} = i\sum_{p,q,k,l}\Big(H^{(k,l)}A^{(p,q)}(t)\,c^{\dagger k}c^{l}c^{\dagger p}c^{q} - A^{(p,q)}(t)\,H^{(k,l)}c^{\dagger p}c^{q}c^{\dagger k}c^{l}\Big) + \quad \text{terms in } \gamma, \Gamma. \tag{D.5}$$

We have dropped hats from operators for ease of notation. Relabelling dummy indices,

$$\frac{d}{dt}A^{(p,q)}(t)\,c^{\dagger p}c^{q} = i\sum_{p,q,k,l}F(p,q,k,l;t)\,c^{\dagger p}c^{q}c^{\dagger k}c^{l} + \quad \text{terms in } \gamma, \Gamma \quad , \tag{D.6}$$

where

$$F(p,q,k,l;t) = H^{(k,l)}A^{(p,q)}(t) - A^{(p,q)}(t)\,H^{(k,l)}.$$

The differential equation for $A^{(0,0)}$ is such that there are no operators in mode c remaining on the right hand side of Eq. D.6. Clearly this occurs when $p = q = k = l = 0$. It can also occur for other values of p, q, k, l, owing to constant terms appearing via the commutators of $\hat{c}$ operators. Additionally, since the Lindblad operator $\mathcal{L}$ is second-order in $\hat{c}$ we can see immediately that there will be no terms proportional to γ in the equation for $A^{(0,0)}$.

Writing Eq. D.6 in normal order using the commutator,

$$\frac{d}{dt}A^{(p,q)}(t)\,c^{p,\dagger}c^{q} = i\sum_{p,q,k,l}\Big(F(p,q,k,l;t)\,c^{\dagger p}c^{\dagger k}c^{q}c^{l} + F(p,q,k,l;t)\left[c^{q},c^{\dagger k}\right]c^{\dagger p}c^{l}\Big), \tag{D.7}$$

we observe that additional contributions to $A^{(0,0)}$ are possible when $p = 0, l = 0$ but $q, k \neq 0$ provided that the commutator $\left[c^{q}, c^{\dagger k}\right]$ contains a constant term. We observe

$$\begin{aligned}\left[c, c^{\dagger}\right] &= 1,\\ \left[c^{2}, c^{\dagger 2}\right] &= 4c^{\dagger}c + 2,\\ \left[c^{3}, c^{\dagger 3}\right] &= 9c^{\dagger}c^{\dagger}cc + 18c^{\dagger}c + 6,\\ &\vdots\end{aligned} \tag{D.8}$$

while commutators with $q \neq k$ cannot give a constant term.

For ease, and because the largest terms considered in Ch. 6 are of the form $c^{\dagger}c^{\dagger}cc$ we will restrict ourselves to $0 \leqslant q, k \leqslant 2$. This gives

$$\frac{d}{dt}A^{(0,0)}(t) = i\left(\left[H^{(0,0)}, A^{(0,0)}\right] + F(0,1,1,0) + 2F(0,2,2,0)\right),$$

and so

$$\frac{d}{dt}A^{(0,0)}(t) = i\left(\left[H^{(0,0)}, A^{(0,0)}\right] + H^{(0,1)}A^{(1,0)} - A^{(0,1)}H^{(1,0)} + 2H^{(0,2)}A^{(2,0)} - 2A^{(0,2)}H^{(2,0)}\right). \tag{D.9}$$

Let us return to Eq. D.2 and substitute Eq. D.4 into the γ term. By rearranging into normal order we arrive at

$$\gamma\mathcal{L}\left[\hat{c}^\dagger\right]\hat{A} \to -\gamma\sum_{p,q}\frac{(p+q)}{2}\hat{A}^{(p,q)}\hat{c}^{\dagger p}\hat{c}^q, \tag{D.10}$$

and so for $t \gg 1/\gamma$ we may approximate the evolution of $\hat{A}^{(p,q)}$ by

$$\frac{d}{dt}A^{(p,q)} \approx i\left[H^{(p,q)}, A^{(0,0)}\right] - \frac{\gamma(p+q)}{2}A^{(p,q)}, \tag{D.11}$$

since $A^{(p,q)}$ is dominated by the decay. Assuming that t is such that $A^{(p,q)}$ has reached its steady-state we set $\frac{d}{dt}A^{(p,q)} = 0$ and so

$$A^{(p,q)}(t) \approx \frac{2i}{\gamma(p+q)}\left[H^{(p,q)}, A^{(0,0)}(t)\right], \tag{D.12}$$

provided that $p \neq 0$ or $q \neq 0$. By substituting this equation for $A^{(p,q)}$ into Eq. D.9, we finally arrive at

$$\frac{d}{dt}A^{(0,0)} = i\left[H^{(0,0)}, A^{(0,0)}\right] + \frac{4}{\gamma}\sum_{p=1,2}\mathcal{L}\left[H^{(0,p)}\right]A^{(0,0)} + \Gamma_j\mathcal{L}\left[a_j\right]\rho. \tag{D.13}$$

Transforming back to our master equation in Lindblad form,

$$\frac{d}{dt}\rho = -i\left[H^{(0,0)}, \rho\right] + \frac{4}{\gamma}\sum_{p=1,2}\mathcal{L}\left[H^{(0,p)\dagger}\right]\rho + \Gamma_j\mathcal{L}\left[a_j\right]\rho. \tag{D.14}$$

This Eq. D.14 is our key equation for performing the adiabatic elimination of the highly lossy mode[1]. The recipe to apply it to a general system is to identify the $H^{(0,0)}$ and $H^{(0,p)}$ terms, which can take arbitrary form, and then substitute them into Eq. D.14. The only requirement for the use of Eq. D.14 is that $\hat{H}$ must have its largest term in lossy mode c of the form $\hat{c}^\dagger\hat{c}^\dagger\hat{c}\hat{c}$, i.e. two creation and two annihilation operators. More general forms of Eq. D.14 may be considered by continuing our analysis to higher-order commutators $\left[\hat{c}^n, \hat{c}^{\dagger n}\right]$ which has constant term $n!$, allowing for different maximum combinations of $\hat{c}$ operators

1 Mode $\hat{c}$ in Chapter 6.

E

PHOG: NUMERICAL METHODS

In this appendix we will briefly overview the numerical methods which are used in Chapter 6. The first two methods, direct integration in Sec. E.1, and quantum Monte Carlo in Sec. E.2, are standard methods for handling the Lindblad master equation. The final two methods, mean-field and linearization, Secs. E.3, E.4, E.5, E.6, are discussed at length in the main body of the Thesis, Sec. 6.6, and so we will just reproduce the final systems of equations in this Appendix.

E.1 DIRECT INTEGRATION

The dynamics of a quantum system coupled to a reservoir is governed by the Lindblad equation

$$\frac{d}{dt}\rho = -i\left[\hat{H},\rho\right] + \sum_n \left(\hat{C}_n\rho\hat{C}_n^\dagger - \frac{1}{2}\hat{C}_n^\dagger\hat{C}_n\rho - \frac{1}{2}\rho\hat{C}_n^\dagger\hat{C}_n\right), \tag{E.1}$$

where $\hat{H}$ acts only on ρ and $\hat{C}_n$ are the collapse operators governing decay into the reservoir. Here we take $\hat{C}_n = \sqrt{\gamma_n}\hat{A}_n$ where $\hat{A}_n$ is an operator acting on ρ. This is the operator through which ρ couples to the reservoir in the original system-reservoir Schrödinger equation. The derivation of this Lindblad equation including requisite approximations is discussed extensively in many canonical texts such as Refs. [6, 15].

There are many routes which one can take to solve Eq. E.1. One such approach is to interpret ρ, $\hat{H}$ and $\hat{C}_n$ as matrices. Let our underlying Hilbert-space be denoted $\mathcal{H}$ and have dimension $|\mathcal{H}|$. Then ρ, $\hat{H}$ and $\hat{C}_n$ each have dimension $|\mathcal{H}|^2$ and may be interpreted as a matrices in $M_{|\mathcal{H}|\times|\mathcal{H}|}(\mathbb{C})$. In this approach, the Lindblad equation E.1 can be interpreted as a coupled system of $|\mathcal{H}|^2$ first-order ODEs, which can then be solved via an appropriate numerical method [240], the efficiency and power of which will depend strongly on the choices of $\hat{H}$, $\hat{C}_n$ and initial condition $\rho(0)$.

It should be noted that such an approach will only ever give an approximation to the true systems which we study in this Thesis. The key reason for this is that the quantum states we begin with are coherent states which take the form

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

where $|n\rangle$ is the n-photon Fock state. The sum in Eq. E.2 runs from zero to infinity and so the required Hilbert space size is countably

infinite. However, for any given α, is is possible to find N such that the state

$$|\psi\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{N} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{E.3}$$

has both $|\langle\psi|\psi\rangle|^2 \approx 1$ and $\langle\alpha|\psi\rangle \approx 1$. Thus, truncating the countable Hilbert space to a large but finite one should be possible. In this Thesis we use truncation values such that all states are appropriately normalized and that no ill effects are introduced from the truncation to a finite $|\mathcal{H}|$. A good rule-of-thumb is to pick

$$|\mathcal{H}| \geqslant \lceil 2\alpha^2 \rceil \tag{E.4}$$

which ensures that the coherent state Eq. E.3 is correctly normalized and a good approximation of the full Eq. E.2. For all simulations N was then increased until there was no change in the resulting dynamics.

In this Thesis we make use of open-source QuTiP package[1] [241] in Python to perform such numerical solutions. The coherent state must be defined in QuTiP specifying the "analytic" option to `qutip.coherent_dm`, which ensures that $|\alpha\rangle\langle\alpha|$ uses the expression Eq. E.3. The default option, "operator," instead finds the eigenstate of annihilation operator $\hat{a}$. As $|\mathcal{H}| \to \infty$ these two forms of coherent state become equivalent, but for small $|\mathcal{H}|$ they can differ significantly. We have found that the analytic form gives much more accurate behaviour in the parameter ranges considered and requires smaller $|\mathcal{H}|$ to give an accurate representation of the resulting dynamics.

Direct integration of the ODE system is performed using the `qutip.mesolve` command, which itself calls `scipy.integrate.ode`. On a standard home-use laptop[2] a single-mode system with $|\mathcal{H}| = 35$, initial $\rho(0)$ a coherent state with $\alpha = 3.0$, decay rate $\gamma = 1.0$, collapse operator $\hat{a}$ and free Hamiltonian $\hat{H} = \omega\hat{a}^\dagger\hat{a}$ with $\omega = 1.0$ can be solved in[3] 41.7 ms $\pm$11.7 ms. Setting $|\mathcal{H}| = 50$ takes 92.6 ± 3 ms, $|\mathcal{H}| = 200$ takes 829 ms $\pm$191 ms.

However, using collapse operator $\hat{a}\,(\hat{a}^\dagger\hat{a} - 1)$ increases the computational power required, and $|\mathcal{H}| = 35$ takes 11.3 s $\pm$1.64 s, and $|\mathcal{H}| = 100$ takes 110 s. We see then that this approach is highly dependent on both the form of $\hat{H}$, $\hat{C}_n$ and the Hilbert-space size. Indeed, a Hilbert space size $|\mathcal{H}|$ yields $|\mathcal{H}|^2$ coupled ODEs[4] to solve. We compare timings between direct integration and quantum Monte Carlo methods in Tab. E.1.

1 QuTiP version 4.4.1; Numpy version 1.16.4; Scipy version 1.3.1; Cython version 0.29.13; Matplotlib version 3.1.0; Python version 3.7.4.

2 Intel(R) Core(TM) i5 – 3230M CPU @2.60 GHz; 8.00 GB RAM.

3 Timed via iPython `%timeit` magic command.

4 Including more modes in our model means the number of equations increases even faster. For two modes, living on Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$, the total system size is $|\mathcal{H}_A \otimes \mathcal{H}_B| = |\mathcal{H}_A| \times |\mathcal{H}_B|$.

E.2 QUANTUM MONTE CARLO

We have seen that direct integration of Eq. E.1 requires a system of $|\mathcal{H}|^2$ coupled ODEs to be simultaneously solved. This is possible in the limit of small $|\mathcal{H}|$, but quickly becomes difficult as $|\mathcal{H}|$ increases. An alternative approach does not solve a matrix differential equation, rather a vector one, and so instead scales as $|\mathcal{H}|$.

We will outline the quantum Monte Carlo (QMC) approach and then discuss its implementation and use in this Thesis. The key principle of the QMC approach is to solve the Schrödinger equation,

$$i\frac{d}{dt}|\psi\rangle = \hat{H}|\psi\rangle, \tag{E.5}$$

instead of the Lindblad equation. The Schrödinger equation is an equation for ket vector $|\psi\rangle$ rather than density matrix $|\psi\rangle\langle\psi|$, and so requires fewer computational resources. The Hamiltonian $\hat{H} = \hat{H}_{\text{eff}}$ should be chosen as

$$\hat{H}_{\text{eff}} = \hat{H}_{\text{sys}} + \hat{H}_{\text{non-Hermitian}} \tag{E.6}$$

where $\hat{H}_{\text{sys}}$ is the system Hamiltonian, identical to the $\hat{H}$ used in the Lindblad equation E.1, while

$$\hat{H}_{\text{non-Hermitian}} = -\frac{i}{2}\sum_n \hat{C}_n^\dagger \hat{C}_n \tag{E.7}$$

is a non-Hermitian Hamiltonian which causes dissipation to the state $|\psi\rangle$ via collapse operators $\hat{C}_n$. The non-Hermitian Hamiltonian does not conserve the norm of $|\psi\rangle$. QuTiP leverages this behaviour into the following algorithm which models a single trajectory of evolution of $|\psi\rangle$ [242–245].

Choose a number $r \in (0,1)$ uniformly at random. This number is related to the collapse probability of $|\psi\rangle$ caused by the $\hat{C}_n$. The Schrödinger equation Eq. E.5 is numerically integrated[5] and the norm $\langle\psi(t)|\psi(t)\rangle$ is monitored.

At time τ such that $\langle\psi(\tau)|\psi(\tau)\rangle = r$, project $|\psi(\tau)\rangle$ onto $\hat{C}_n|\psi(\tau)\rangle$ and re-normalize. This is referred to as a "jump". So

$$|\psi(\tau)\rangle \to \frac{\hat{C}_n|\psi(\tau)\rangle}{\sqrt{\langle\psi(\tau)|\hat{C}_n^\dagger\hat{C}_n|\psi(\tau)\rangle}}. \tag{E.8}$$

Draw another $r \in (0,1)$ and continue the evolution using the new $|\psi\rangle$ as the starting point. This process is repeated until the entire temporal range is covered. This gives us a single trajectory of the evolution of $|\psi\rangle$.

The above procedure is repeated many times, and observables should be averaged[6] over many trajectories. It can be shown that this

5 QuTiP calls `scipy.integrate.ode`

6 Simply using `numpy.mean` at each timestep

procedure implements the corresponding Lindblad master equation [1, 242] by noticing that the evolution from $|\psi(t)\rangle\langle\psi(t)|$ to $|\psi(t+\Delta t)\rangle\langle\psi(t+\Delta t)|$ is effectively a mixture over whether a jump occurred or not:

$$|\psi\rangle\langle\psi|(t+\Delta t) = \Delta P \left|\psi_{\text{Jump}}\right\rangle\left\langle\psi_{\text{Jump}}\right| + (1-\Delta P)\left|\psi_{\text{No Jump}}\right\rangle\left\langle\psi_{\text{No Jump}}\right| \tag{E.9}$$

The state $|\psi_{\text{Jump}}\rangle$ is given by Eq. E.8, while $|\psi_{\text{No Jump}}\rangle$ is found by explicitly enacting the non-Hermitian effective Hamiltonian on $|\psi\rangle$ for Δt. By substituting in our expressions and allowing $\Delta t \to 0$, this reduces to a Lindblad equation of our original form.

Let us consider the performance of the QMC method and compare it to direct integration. QMC may be implemented by using `qutip.mcsolve` and specifying $\hat{H}_{\text{sys}}$, $|\psi(0)\rangle$, $\hat{C}_n$ and the operators $\hat{E}_n$ whose expectations should be measured. Let us solve an identical system to the one discussed in Eq. E.1: a single-mode system consisting of an initial coherent state with $\alpha = 3.0$, decay rate $\gamma = 8.0$ with collapse operator $\hat{a}$, and let us measure the photon-number expectation $\langle \hat{a}^\dagger \hat{a} \rangle$.

For $|\mathcal{H}| = 35$, the QMC method takes 12.40 s to model 500 trajectories. This performance is worse than for direct-integration, owing to the high overhead to average a large number of trajectories. Function `qutip.mcsolve` also naturally uses parallel-processing functionality[7] which has high overhead. $|\mathcal{H}| = 50$ takes 11.61 s and $|\mathcal{H}| = 200$ takes 19.08 s.

We compare the speed of the direct integration and QMC approaches to solve Eq. 6.37 with $\gamma = 1.0$, varying initial coherent state amplitude and decay operator $\hat{a}$ $\left(\hat{a}^\dagger \hat{a} - 1\right)$ in Tab. E.1. All states were correctly normalized, which implies that the earlier condition Eq. E.4 is only a rule-of-thumb. We compare the QMC and direct integration methods for accuracy in Fig. E.1.

7 Provided by `multiprocessing.Pool`

Run parameters		Timings	
$\|\mathcal{H}\|$	α	DI [s]	QMC [s]
35	3.0	0.048	10.33
50	5.0	0.145	11.05
100	8.0	0.319	14.84
200	12.0	4.04	29.68
500	20.0	332.32	143.84
750	25.0	-	224.00
1500	37.0	-	753.05
1950	38.0	-	1361.72

Table E.1: Run-times to solve Eq. 6.37 with $\gamma_L = 10.0$, $\gamma_2 = 0.0005$, $\gamma_{NCL} = 0.002$, input coherent state amplitude α and 500 QMC trajectories. Missing direct integration entries returned memory errors.

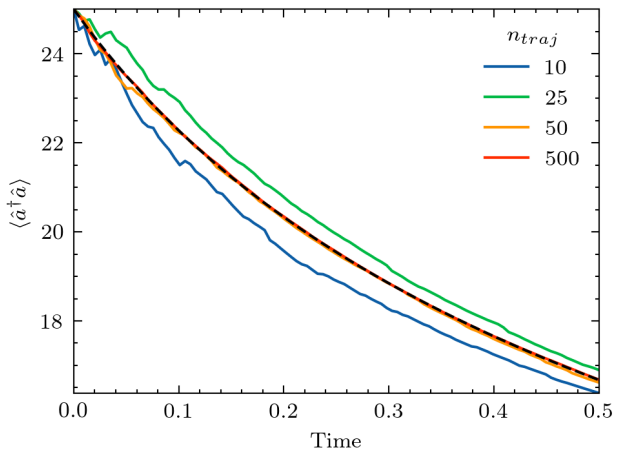


Figure E.1: Comparison of accuracy between direct integration and quantum monte carlo methods with varying number of monte carlo trajectories n_{traj}. Solving Eq. 6.37 with $\gamma_L = 0.0$, $\gamma_2 = 0.0005$, $\gamma_3 = 0.002$, $|\mathcal{H}| = 100$, $\alpha = 5.0$. Dashed: direct integration. Solid: quantum monte carlo. For n_{traj} small the behaviour is qualitatively similar to the full solution, but we must choose large n_{traj} in order to make accurate quantitative predictions. For this thesis we take $n_{traj} = 500$ unless otherwise stated.

E.3 MEAN-FIELD SINGLE-MODE MODEL

Applying the mean-field approximation discussed in Sec. 6.6.1 to the single-mode PhoG model Eq. 6.37, we arrive at the following equation for first-order expectation $\langle s_- \rangle$:

$$\frac{d}{dt}\langle s_-\rangle = -\frac{\gamma_1}{2}\langle s_-\rangle - i\sigma_1\langle s_-\rangle - i\sigma_3\langle s_-\rangle - 2i\sigma_1\langle s_-^\dagger\rangle\langle s_-\rangle\langle s_-\rangle$$
$$-\gamma_2\langle s_-^\dagger\rangle\langle s_-\rangle\langle s_-\rangle - \gamma_3\langle s_-^\dagger\rangle\langle s_-\rangle\langle s_-\rangle - \frac{\gamma_3}{2}\langle s_-^\dagger\rangle\langle s_-^\dagger\rangle\langle s_-\rangle\langle s_-\rangle\langle s_-\rangle \tag{E.10}$$

with $\langle s_-^\dagger\rangle = \langle s_-\rangle^*$. The system may be readily solved for $\langle s_-\rangle(t)$.

E.4 LINEARIZED SINGLE-MODE MODEL

By applying the linearization approximations derived in Sec. 6.6.2 to the system of coupled ODEs derived from single-mode Lindblad equation 6.37 we arrive at the following closed system of ODEs:

$$\begin{aligned}\partial_t\langle s_-\rangle &= c_1\langle s_-\rangle + c_2\left(\langle s_-^\dagger\rangle\langle s_-^2\rangle + 2\langle s_-\rangle\langle n_-\rangle - 2\langle s_-^\dagger\rangle\langle s_-\rangle^2\right)\\ &\quad -\frac{\gamma_3}{2}\Big(6\langle s_-^\dagger\rangle\langle n_-\rangle\langle s_-^2\rangle + 3\langle s_-\rangle\langle s_-^{\dagger 2}\rangle\langle s_-^2\rangle\\ &\quad +6\langle s_-\rangle\langle n_-\rangle^2 - 2\langle s_-^{\dagger 2}\rangle\langle s_-\rangle^3 - 12\langle n_-\rangle\langle s_-^\dagger\rangle\langle s_-\rangle^2\\ &\quad -6\langle s_-^2\rangle\langle s_-^\dagger\rangle^2\langle s_-\rangle + 6\langle s_-^\dagger\rangle^2\langle s_-\rangle^3\Big),\end{aligned}$$

$$\begin{aligned}\partial_t\langle s_-^\dagger\rangle &= c_1^*\langle s_-^\dagger\rangle + c_2^*\left(\langle s_-\rangle\langle s_-^{\dagger 2}\rangle + 2\langle s_-^\dagger\rangle\langle n_-\rangle - 2\langle s_-^\dagger\rangle^2\langle s_-\rangle\right)\\ &\quad -\frac{\gamma_3}{2}\Big(6\langle s_-\rangle\langle n_-\rangle\langle s_-^{\dagger 2}\rangle + 3\langle s_-^\dagger\rangle\langle s_-^2\rangle\langle s_-^{\dagger 2}\rangle\\ &\quad +6\langle s_-^\dagger\rangle\langle n_-\rangle^2 - 2\langle s_-^2\rangle\langle n_-^3\rangle - 12\langle n_-\rangle\langle s_-\rangle\langle s_-\rangle^2\\ &\quad -6\langle s_-^{\dagger 2}\rangle\langle s_-\rangle^2\langle s_-^\dagger\rangle + 6\langle s_-^{\dagger 3}\rangle\langle s_-\rangle^2\Big),\end{aligned}$$

$$\begin{aligned}\partial_t\langle s_-^2\rangle &= c_3\langle s_-s_-\rangle + c_4\left(3\langle n_-\rangle\langle s_-^2\rangle - 2\langle s_-^\dagger\rangle\langle s_-\rangle^3\right)\\ &\quad -\gamma_3\Big(3\langle s_-^{\dagger 2}\rangle\langle s_-^2\rangle^2 + 12\langle n_-\rangle^2\langle s_-^2\rangle - 2\langle s_-^{\dagger 2}\rangle\langle s_-\rangle^4\\ &\quad -12\langle s_-^2\rangle\langle s_-^\dagger\rangle^2\langle s_-\rangle^2 - 16\langle n_-\rangle\langle s_-^\dagger\rangle\langle s_-\rangle^3\\ &\quad +16\langle s_-^\dagger\rangle^2\langle s_-\rangle^4\Big),\end{aligned}$$

$$\begin{aligned}\partial_t\langle s_-^{\dagger 2}\rangle &= c_3^*\langle s_-^{\dagger 2}\rangle + c_4^*\left(3\langle s_-^{\dagger 2}\rangle\langle n_-\rangle - 2\langle s_-^\dagger\rangle^3\langle s_-\rangle\right)\\ &\quad -\gamma_3\Big(3\langle s_-^{\dagger 2}\rangle^2\langle s_-^2\rangle + 12\langle s_-^{\dagger 2}\rangle\langle n_-\rangle^2 - 2\langle s_-^2\rangle\langle s_-^\dagger\rangle^4\\ &\quad -21\langle s_-^{\dagger 2}\rangle\langle s_-^\dagger\rangle^2\langle s_-\rangle^2 - 16\langle n_-\rangle\langle s_-^\dagger\rangle^3\langle s_-\rangle\\ &\quad +16\langle s_-^\dagger\rangle^4\langle s_-\rangle^2\Big),\end{aligned}$$

$$\begin{aligned}\partial_t\langle n_-\rangle = &-\gamma_1\langle n_-\rangle + c_5\left(\langle s_-^{\dagger 2}\rangle\langle s_-^2\rangle + 2\langle n_-\rangle^2 - 2\langle s_-^\dagger\rangle^2\langle s_-\rangle^2\right)\\ &-\gamma_3\left(9\langle s_-^{\dagger 2}\rangle\langle n_-\rangle\langle s_-^2\rangle + 6\langle n_-\rangle^3 - 6\langle s_-^{\dagger 2}\rangle\langle s_-^\dagger\rangle\langle s_-\rangle^3\right.\\ &-18\langle n_-\rangle\langle s_-^\dagger\rangle^2\langle s_-\rangle^2 - 6\langle s_-^2\rangle\langle s_-^\dagger\rangle^3\langle s_-\rangle\\ &\left.+16\langle s_-^\dagger\rangle^3\langle s_-\rangle^3\right),\end{aligned} \tag{E.11}$$

with $n_- = s_-^\dagger s_-$. This system is solved numerically for $\langle s_-\rangle$, $\langle s_-^\dagger\rangle$, $\langle s_-^2\rangle$, $\langle s_-^{\dagger 2}\rangle$, $\langle n_-\rangle$ and the results are shown as dashed lines in Fig. 6.23 of the main Thesis.

E.5 MEAN-FIELD MULTI-MODE MODEL

Applying the mean-field approximation outlined in Sec. 6.6.1 to the multi-mode PhoG model Eq. 6.44, we arrive at the following system of equations for first-order expectations.

$$\begin{aligned}
&\frac{d}{dt}\langle a\rangle = -ig_a\langle c_0\rangle + iU\langle a^\dagger\rangle\langle a\rangle\langle a\rangle - \frac{\gamma}{2}\langle a\rangle,\\
&\frac{d}{dt}\langle b\rangle = -ig_b\langle c_0\rangle + iU\langle b^\dagger\rangle\langle b\rangle\langle b\rangle - \frac{\gamma}{2}\langle b\rangle,\\
&\frac{d}{dt}\langle c_0\rangle = -ig_a\langle a\rangle - ig_b\langle b\rangle - ig_c\langle c_1\rangle + iU\langle c_0^\dagger\rangle\langle c_0\rangle\langle c_0\rangle - \frac{\gamma}{2}\langle c_0\rangle,\\
&\frac{d}{dt}\langle c_j\rangle = -ig_c\langle c_{j-1}\rangle - ig_c\langle c_{j+1}\rangle + iU\langle c_j^\dagger\rangle\langle c_j\rangle\langle c_j\rangle - \frac{\gamma}{2}\langle c_j\rangle \quad \text{for} \quad 0 < j < N,\\
&\frac{d}{dt}\langle c_N\rangle = -ig_c\langle c_{N-1}\rangle + iU\langle c_N^\dagger\rangle\langle c_N\rangle\langle c_N\rangle - \frac{\gamma}{2}\langle c_N\rangle.
\end{aligned} \tag{E.12}$$

The system may be readily solved.

E.6 LINEARIZED MULTI-MODE MODEL

We will derive a linearized and closed system of coupled differential equations capable of modelling the multi-mode PhoG device. In fact, our equations will be capable of modelling any collection of coupled modes with on-site Kerr nonlinearity and Markovian reservoirs. Our starting Lindblad equation is (c.f. Eq. 6.44):

$$\frac{d}{dt}\rho = -i\left[\hat{H},\rho\right] + \gamma_1\left[\mathcal{L}\left(\hat{a}_1\right) + \mathcal{L}\left(\hat{a}_2\right) + \sum_{j=3}^{N+2}\mathcal{L}\left(\hat{a}_j\right)\right]\rho \tag{E.13}$$

where we here take $\hat{H} = \hat{H}^{\text{Coupling}} + \hat{H}^{\text{Kerr}}$. In this Appendix we label all modes as $\hat{a}_k$, with the subscript denoting which mode in the PhoG

device is meant. In particular, $a_1 \leftrightarrow a$, $a_2 \leftrightarrow b$, and $a_{k\geqslant 3} \leftrightarrow c_{k-3}$ in the main body. The Hamtiltonian is

$$\hat{H}^{\text{Kerr}} = \frac{U}{2} \sum_x \hat{x}^\dagger \hat{x}^\dagger \hat{x}\hat{x} \qquad x \in \{a, b, c_j\} \qquad 0 \leqslant j \leqslant N,$$
$$\hat{H}^{\text{Coupling}} = \sum_{k,l} \mathcal{G}_{k,l} \left(\hat{a}_k^\dagger \hat{a}_l + \hat{a}_l^\dagger \hat{a}_k \right). \tag{E.14}$$

We have introduced a "coupling matrix" $\mathcal{G}$ which contains all information relating to the linear coupling between modes of our system. Coupling matrix element $\mathcal{G}_{j,p}$ denotes the coupling strength between modes j and p, and $\mathcal{G}_{j,p} = 0$ if the modes are not coupled to each other, which is the case for most pairs (j, p). We display some examples of coupling matrices below.

E.6.1 *Example coupling matrices $\mathcal{G}$*

$$\mathcal{G} = \begin{bmatrix} 0 & g & 0 & 0 & \dots & 0 & 0 & 0 \\ g & 0 & g & 0 & \dots & 0 & 0 & 0 \\ 0 & g & 0 & g & \dots & 0 & 0 & 0 \\ 0 & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & g & 0 \\ 0 & 0 & 0 & 0 & \dots & g & 0 & g \\ 0 & 0 & 0 & 0 & \dots & 0 & g & 0 \end{bmatrix}$$

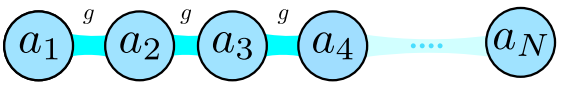


Figure E.2: Example coupling matrix $\mathcal{G}$ for a straight line of bosonic modes.

$$\mathcal{G} = \begin{bmatrix} 0 & 0 & g1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & g2 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ g1 & g2 & 0 & g3 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & g3 & 0 & g3 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & g3 & 0 & g3 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & g3 & 0 & \dots & 0 & 0 & 0 \\ 0 & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & g3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & g3 & 0 & g3 \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & g3 & 0 \end{bmatrix}$$

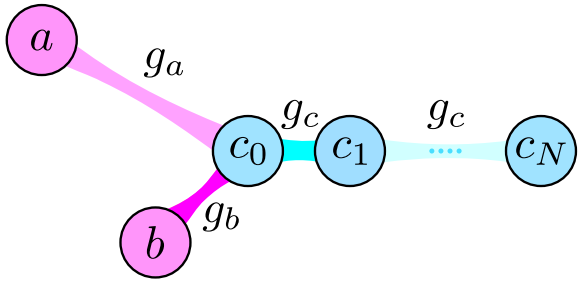


Figure E.3: Example coupling matrix $\mathcal{G}$ for the PhoG system.

E.6.2 *Linearized equations*

Letting $n, m \in [1, N+2]$, $n \neq m$, we derive a closed system of coupled differential equations for first- and second-order expectations

$$\begin{aligned}\partial_t\langle\hat{a}_n\rangle = &\left(-i\omega_n - \frac{\Gamma_n}{2}\right)\langle\hat{a}_n\rangle - 2iU\langle\hat{a}_n\rangle\langle\hat{a}_n^\dagger\hat{a}_n\rangle - iU\langle\hat{a}_n^\dagger\rangle\langle\hat{a}_n\hat{a}_n\rangle + 2iU\langle\hat{a}_n^\dagger\rangle\langle\hat{a}_n\rangle\langle\hat{a}_n\rangle \\ &- \sum_{j=1}^{N} iG_{n,j}\langle\hat{a}_j\rangle,\end{aligned}$$

$$\begin{aligned}\partial_t\langle\hat{a}_n^\dagger\rangle = &\left(+i\omega_n - \frac{\Gamma_n}{2}\right)\langle\hat{a}_n^\dagger\rangle + 2iU\langle\hat{a}_n^\dagger\rangle\langle\hat{a}_n^\dagger\hat{a}_n\rangle + iU\langle\hat{a}_n\rangle\langle\hat{a}_n^\dagger\hat{a}_n^\dagger\rangle - 2iU\langle\hat{a}_n^\dagger\rangle\langle\hat{a}_n^\dagger\rangle\langle\hat{a}_n\rangle \\ &+ \sum_{j=1}^{N} iG_{n,j}\langle\hat{a}_j^\dagger\rangle,\end{aligned}$$

$$\begin{aligned}\partial_t\langle\hat{a}_n\hat{a}_n\rangle = &\left(-2i\omega_n - \Gamma_n\right)\langle\hat{a}_n\hat{a}_n\rangle - 6iU\langle\hat{a}_n^\dagger\hat{a}_n\rangle\langle\hat{a}_n\hat{a}_n\rangle + 4iU\langle\hat{a}_n^\dagger\rangle\langle\hat{a}_n\rangle\langle\hat{a}_n\rangle\langle\hat{a}_n\rangle - iU\langle\hat{a}_n\hat{a}_n\rangle \\ &- \sum_{j=1}^{N} 2iG_{n,j}\langle\hat{a}_n\hat{a}_j\rangle,\end{aligned}$$

$$\partial_t\langle\hat{a}_n^\dagger\hat{a}_n\rangle = -\Gamma_n\langle\hat{a}_n^\dagger\hat{a}_n\rangle + \Gamma_n\bar{n}_{th}^{(n)} + \sum_{j=1}^{N} iG_{n,j}\left(\langle\hat{a}_j^\dagger\hat{a}_n\rangle - \langle\hat{a}_n^\dagger\hat{a}_j\rangle\right),$$

$$\begin{aligned}\partial_t\langle\hat{a}_n^\dagger\hat{a}_n^\dagger\rangle = &\left(2i\omega_n - \Gamma_n\right)\langle\hat{a}_n^\dagger\hat{a}_n^\dagger\rangle + 6iU\langle\hat{a}_n^\dagger\hat{a}_n^\dagger\rangle\langle\hat{a}_n^\dagger\hat{a}_n\rangle - 4iU\langle\hat{a}_n^\dagger\rangle\langle\hat{a}_n^\dagger\rangle\langle\hat{a}_n^\dagger\rangle\langle\hat{a}_n\rangle + iU\langle\hat{a}_n\hat{a}_n^\dagger\rangle \\ &+ \sum_{j=1}^{N} 2iG_{n,j}\langle\hat{a}_n^\dagger\hat{a}_j^\dagger\rangle,\end{aligned}$$

$$\begin{aligned}\partial_t\langle\hat{a}_n\hat{a}_m\rangle = &\left(i\left(\omega_n + \omega_m\right) - \frac{\Gamma_n + \Gamma_m}{2}\right)\langle\hat{a}_n\hat{a}_m\rangle - 2iU\langle\hat{a}_n^\dagger\hat{a}_n\rangle\langle\hat{a}_n\hat{a}_m\rangle - iU\langle\hat{a}_n^\dagger\hat{a}_m\rangle\langle\hat{a}_n\hat{a}_n\rangle \\ &- 2iU\langle\hat{a}_m^\dagger\hat{a}_m\rangle\langle\hat{a}_n\hat{a}_m\rangle - iU\langle\hat{a}_m^\dagger\hat{a}_n\rangle\langle\hat{a}_m\hat{a}_m\rangle + 2iU\langle\hat{a}_n^\dagger\rangle\langle\hat{a}_n\rangle\langle\hat{a}_n\rangle\langle\hat{a}_m\rangle \\ &+ 2iU\langle\hat{a}_n\rangle\langle\hat{a}_m^\dagger\rangle\langle\hat{a}_m\rangle\langle\hat{a}_m\rangle - \sum_{j=1}^{N} iG_{n,j}\langle\hat{a}_j\hat{a}_m\rangle - \sum_{q=1}^{N} iG_{m,q}\langle\hat{a}_n\hat{a}_q\rangle,\end{aligned}$$

$$\begin{aligned}\partial_t\langle\hat{a}_n^\dagger\hat{a}_m\rangle = &\left(i\left(\omega_n - \omega_m\right) - \frac{\Gamma_n + \Gamma_m}{2}\right)\langle\hat{a}_n^\dagger\hat{a}_m\rangle + 2iU\langle\hat{a}_n^\dagger\hat{a}_m\rangle\langle\hat{a}_n^\dagger\hat{a}_n\rangle + iU\langle\hat{a}_n^\dagger\hat{a}_n^\dagger\rangle\langle\hat{a}_n\hat{a}_m\rangle \\ &- 2iU\langle\hat{a}_n^\dagger\hat{a}_m\rangle\langle\hat{a}_m^\dagger\hat{a}_m\rangle - iU\langle\hat{a}_n^\dagger\hat{a}_m^\dagger\rangle\langle\hat{a}_m\hat{a}_m\rangle - 2iU\langle\hat{a}_n^\dagger\rangle\langle\hat{a}_n^\dagger\rangle\langle\hat{a}_n\rangle\langle\hat{a}_m\rangle \\ &+ 2iU\langle\hat{a}_n^\dagger\rangle\langle\hat{a}_m^\dagger\rangle\langle\hat{a}_m\rangle\langle\hat{a}_m\rangle + \sum_{j=1}^{N} iG_{n,j}\langle\hat{a}_j^\dagger\hat{a}_m\rangle - \sum_{q=1}^{N} iG_{m,q}\langle\hat{a}_n^\dagger\hat{a}_q\rangle,\end{aligned}$$

$$\begin{aligned}\partial_t\langle\hat{a}_n^\dagger\hat{a}_m^\dagger\rangle = &\left(i(\omega_n+\omega_m)-\frac{\Gamma_n+\Gamma_m}{2}\right)\langle\hat{a}_n^\dagger\hat{a}_m^\dagger\rangle + 2iU\langle\hat{a}_n^\dagger\hat{a}_m^\dagger\rangle\langle\hat{a}_n^\dagger\hat{a}_n\rangle + iU\langle\hat{a}_n^\dagger\hat{a}_n^\dagger\rangle\langle\hat{a}_m^\dagger\hat{a}_n\rangle \\ &+ 2iU\langle\hat{a}_n^\dagger\hat{a}_m^\dagger\rangle\langle\hat{a}_m^\dagger\hat{a}_m\rangle + iU\langle\hat{a}_n^\dagger\hat{a}_m\rangle\langle\hat{a}_m^\dagger\hat{a}_m^\dagger\rangle - 2iU\langle\hat{a}_n^\dagger\rangle\langle\hat{a}_n^\dagger\rangle\langle\hat{a}_n\rangle\langle\hat{a}_m^\dagger\rangle \\ &- 2iU\langle\hat{a}_n^\dagger\rangle\langle\hat{a}_m^\dagger\rangle\langle\hat{a}_m^\dagger\rangle\langle\hat{a}_m\rangle + \sum_{j=1}^{N} iG_{n,j}\langle\hat{a}_j^\dagger\hat{a}_m^\dagger\rangle + \sum_{q=1}^{N} iG_{m,q}\langle\hat{a}_n^\dagger\hat{a}_q^\dagger\rangle.\end{aligned} \tag{E.15}$$

BIBLIOGRAPHY

[1] U. Leonhardt, *Essential quantum optics* (Cambridge University Press, Cambridge, 2010).

[2] D. F. Walls and G. J. Millburn, *Quantum Optics* (Springer-Verlag, Berlin, Heidelberg, 1994).

[3] C. C. Gerry and P. L. Knight, *Introductory Quantum Optics* (Cambridge University Press, Cambridge, 2006).

[4] K Husimi, "Some formal properties of the density matrix", Proc. Phys. Math. Soc. Jpn. **22**, 264 (1940).

[5] R. J. Glauber, "Coherent and Incoherent States of the Radiation Field", Phys. Rev. **131**, 2766 (1963).

[6] H. J. Carmichael, *Statistical methods in quantum optics 1* (Springer-Verlag Berlin Heidelberg, 1999).

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing", Theor. Comput. Sci. **560**, 7 (2014).

[8] C Adami and N. J. Cerf, "Quantum Computation with Linear Optics", in Quantum Computing and Quantum Communications QCQC 1998. Lecture Notes in Computer Science, vol 1509. Edited by C. P. Williams (1999), p. 391.

[9] R. Boyd, *Nonlinear Optics* (Elsevier, Amsterdam, 2008).

[10] S. M. Barnett and P. M. Radmore, *Methods in Theoretical Quantum Optics* (Oxford University Press, Oxford, 2005).

[11] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement", Rev. Mod. Phys. **81**, 865 (2009).

[12] J. Eisert and M. B. Plenio, "Introduction to the basics of entanglement theory in continuous-variable systems", Int. J. Quant. Inf. **1**, 479 (2003).

[13] 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 (2012).

[14] A. Serafini, *Quantum Continuous Variables: A primer of theoretical methods* (Taylor & Francis, London, 2017).

[15] H. P. Breuer and F. Petruccione, *The Theory of Open Quantum Systems* (Oxford University Press, Oxford, 2007).

[16] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010).

[17] U. Leonhardt, "Measuring the Quantum State of Light", Prog. Quant. Electr. **19**, 89 (1995).

[18]M. Tomamichel, *Quantum Information Processing with Finite Resources - Mathematical Foundations* (Springer International Publishing, 2016).

[19]M. M. Wilde, "From Classical to Quantum Shannon Theory", (2013), arXiv:1106.1445 [quant-ph].

[20]J. Watrous, *The theory of quantum information* (Cambridge University Press, Cambridge, 2018).

[21]W. Hoeffding, "Probability inequalities for sums of bounded random variables", J. Am. Stat. Assoc. **58**, 13 (1963).

[22]S. Singh, *The Code Book* (HarperCollins, London, 2000).

[23]W. Diffie and M. Hellman, "New directions in cryptography", IEEE Trans. Inf. Theory **22**, 644 (1976).

[24]B. Schneier, *Applied cryptography: Protocols, algorithm, and source code in C* (John Wiley & Sons, Verlag, 1996).

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

[26]P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM Review **41**, 303 (1997).

[27]R. Amiri and E. Andersson, "Unconditionally Secure Quantum Signatures", Entropy **17**, 5635 (2015).

[28]D. J. Bernstein, N. Heninger, P. Lou, and L. Valenta, "Post-quantum RSA", in Post-Quantum Cryptogrography. PQCrypto 2017. Lecture Notes in Computer Science, vol 10346, edited by T. Lange and T. Takagi (2017), p. 311.

[29]L Chen, S Jordan, Y. K. Liu, D Moody, R Peralta, R Perlner, and D Smith-Tone, *Report on Post-Quantum Cryptography: NISTIR 8105, National Institute for Standards and Technology*, tech. rep. (2016).

[30]T. Gagliardoni, "Quantum Security of Cryptographic Primitives", PhD Thesis (Technical University of Darmstadt, Germany, 2017).

[31]D. J. Bernstein, "Introduction to post-quantum cryptography", in Post-Quantum Cryptogrography, edited by D. J. Bernstein, J. Buchmann, and E. Dahmen, 1978 (2009), p. 1.

[32]G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, and D. Smith-Tone, *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process: NISTIR 8105, National Institute for Standards and Technology*, tech. rep. (2019).

[33]M. Braithwaite, *Experimenting with post-quantum cryptography*, (2016) https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html (visited on 12/03/2020).

[34]A. Shamir, "How to Share a Secret", Communications of the ACM **22**, 612 (1979).

[35]G. R. Blakley, "Safeguarding cryptographic keys", in AFIPS 1979 (1979), p. 313.

[36]P. Kok and B. W. Lovett, *Introduction to optical quantum information processing* (Cambridge University Press, Cambridge, 2010).

[37]G. J. Simmons, "How to insure that data acquired to verify treaty compliance are trustworthy", Proceedings of the IEEE **76**, 621 (1988).

[38]L. Lamport, *Constructing digital signatures from a one-way function: Technical Report SRI-CSL-98, SRI International Computer Science Laboratory*, tech. rep. (1979).

[39]D. Gottesman and I. Chuang, "Quantum Digital Signatures", (2001), arXiv:quant-ph/0105032.

[40]Y. Wang, J. Li, S. Zhang, K. Su, Y. Zhou, K. Liao, S. Du, H. Yan, and S.-L. Zhu, "Efficient quantum memory for single-photon polarization qubits", Nat. Photonics **13**, 346 (2019).

[41]E. Andersson, M. Curty, and I. Jex, "Experimentally realizable quantum comparison of coherent states and its applications", Phys. Rev. A **74**, 022304 (2006).

[42]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 (2012).

[43]V. Dunjko, P. Wallden, and E. Andersson, "Quantum Digital Signatures without quantum memory", Phys. Rev. Lett. **112**, 040502 (2014).

[44]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", Phys. Rev. Lett. **113**, 040502 (2014).

[45]P. Wallden, V. Dunjko, A. Kent, and E. Andersson, "Quantum digital signatures with quantum-key-distribution components", Phys. Rev. A **91**, 042304 (2015).

[46]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 (2016).

[47]R. Amiri, P. Wallden, A. Kent, and E. Andersson, "Secure quantum signatures using insecure quantum channels", Phys. Rev. A. **93**, 032325 (2016).

[48]H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution", Phys. Rev. Lett. **94**, 230504 (2005).

[49]G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography", Phys. Rev. Lett. **85**, 1330 (2000).

[50]N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution", Phys. Rev. A **61**, 052304 (2000).

[51]R. König, R. Renner, and C. Schaffner, "The operational meaning of min-and max-entropy", IEEE Trans. Inf. Theory **55**, 4337 (2009).

[52]M. Tomamichel, "A Framework for Non-Asymptotic Quantum Information Theory", PhD Thesis (ETH Zurich, 2012).

[53]R. Renner, "Security of Quantum Key Distribution", PhD Thesis (Swiss Federal Institute of Technology, 2005).

[54]H.-L. Yin, Y. Fu, H. Liu, Q.-J. J. Tang, J. Wang, L.-X. X. You, W.-J. J. Zhang, S.-J. J. Chen, Z. Wang, Q. Zhang, T.-Y. Y. Chen, Z.-B. B. Chen, and J.-W. W. Pan, "Experimental quantum digital signature over 102 km", Phys. Rev. A **95**, 032334 (2017).

[55]H.-L. L. Yin, Y. Fu, and Z.-B. Chen, "Practical quantum digital signature", Phys. Rev. A **93**, 032316 (2016).

[56]X.-B. An, H. Zhang, C.-M. Zhang, W. Chen, S. Wang, Z.-Q. Yin, Q. Wang, D.-Y. He, P.-L. Hao, S.-F. Liu, X.-Y. Zhou, G.-C. Guo, and Z.-F. Han, "Practical quantum digital signature with a gigahertz BB84 quantum key distribution system", Opt. Lett. **44**, 1133 (2019).

[57]N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Trojan-horse attacks threaten the security of practical quantum cryptography", New J. Phys. **16**, 123030 (2014).

[58]C.-H. Zhang, X.-Y. Zhou, H.-J. Ding, C.-M. Zhang, G.-C. Guo, and Q. Wang, "Proof-of-Principle Demonstration of Passive Decoy-State Quantum Digital Signatures over 200 km", Phys. Rev. Appl. **10**, 034033 (2018).

[59]S. Sajeed, S. Kaiser, P. Chaiwongkhot, M. Gagné, J.-P. Bourgoin, C. Minshull, M. Legre, T. Jennewein, R. Kashyap, and V. Makarov, "Laser damage creates backdoors in quantum communications", in QCrypt 2016 (2016).

[60]U. Vazirani and T. Vidick, "Fully device-independent quantum key distribution", Phys. Rev. Lett. **113**, 140501 (2014).

[61]S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, "Device-independent quantum key distribution secure against collective attacks", New J. Phys. **11**, 045021 (2009).

[62]R. Colbeck, "Quantum And Relativistic Protocols For Secure Multi-Party Computation", PhD Thesis (University of Cambridge, 2009).

[63]H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution", Phys. Rev. Lett. **108**, 130503 (2012).

[64]I. V. Puthoor, R. Amiri, P. Wallden, M. Curty, and E. Andersson, "Measurement-device-independent quantum digital signatures", Phys. Rev. A **94**, 022328 (2016).

[65]G. L. Roberts, M. Lucamarini, Z. L. Yuan, J. F. Dynes, L. C. Comandar, A. W. Sharpe, A. J. Shields, M. Curty, I. V. Puthoor, and E. Andersson, "Experimental measurement-device-independent quantum digital signatures", Nat. Commun. **8**, 1098 (2017).

[66]R. J. Collins, R. Amiri, M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, M. Takeoka, E. Andersson, G. S. Buller, and M. Sasaki, "Experimental transmission of quantum digital signatures over 90-km of installed optical fiber using a differential phase shift quantum key distribution system", Opt. Lett. **41**, 4883 (2016).

[67]K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution", Phys. Rev. Lett. **89**, 379021 (2002).

[68]K. Inoue, "Differential phase-shift quantum key distribution systems", IEEE J. Sel. Top. Quantum Electron. **21**, 6600207 (2015).

[69]H.-l. Yin, W.-l. Wang, Y.-l. Tang, Q. Zhao, H. Liu, X.-x. Sun, H. Li, I. V. Puthoor, L.-X. You, E. Andersson, Z. Wang, Y. Liu, X. Jiang, X. Ma, Q. Zhang, M. Curty, T.-y. Chen, and J.-W. Pan, "Experimental measurement-device-independent quantum digital signatures over a metropolitan network", Phys. Rev. A **95**, 042338 (2017).

[70]S. L. Braunstein and H. J. Kimble, "Teleportation of Continuous Quantum Variables", Phys. Rev. Lett. **80**, 869 (1998).

[71]K. S. Ranade, "Functional analysis and quantum mechanics: an introduction for physicists", Fortschritte der Phys. **63**, 644 (2015).

[72]P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, "Numerical approach for unstructured quantum key distribution", Nat. Commun. **7**, 11712 (2016).

[73]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", Phys. Rev. Lett. **117**, 100503 (2016).

[74]R. J. Collins, R. J. Donaldson, and G. S. Buller, "Progress in experimental quantum digital signatures", in Proc. SPIE 10771, Quantum Commun. Quantum Imaging XVI, 107710F, edited by R. E. Meyers, Y. Shih, and K. S. Deacon (2018).

[75]M. Thornton, H. Scott, C. Croal, and N. Korolkova, "Continuous-variable quantum digital signatures over insecure channels", Phys. Rev. A **99**, 032341 (2019).

[76]S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, "Reply to 'Discrete and continuous variables for measurement-device-independent quantum cryptography'", Nat. Photonics **9**, 773 (2015).

[77]R. Amiri, A. Abidin, P. Wallden, and E. Andersson, "Unconditionally Secure Signatures", (2016), Cryptology ePrint Archive: Report2016/739.

[78]G. Hanaoka, J. Shikata, Y. Zheng, and H. Imai, "Unconditionally Secure Digital Signature Schemes Admitting Transferability", in ASIACRYPT '00: Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology (2000), p. 130.

[79]S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications", Nature Communications **8**, 15043 (2017).

[80]M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Sheilds, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters", Nature **557**, 400 (2018).

[81]S. M Barnett, T. Brougham, S. Croke, and S. J. D Phoenix, "Optimized attacks on twin-field quantum key distribution", Journal of the Optical Society of America B **36**, B122 (2019).

[82]M. Curty, K. Azuma, and H.-K. Lo, "Simple security proof of twin-field type quantum key distribution protocol", npj Quantum Inf. **5**, 64 (2019).

[83]C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, "Twin-field quantum key distribution without phase postselection", Physical Review Applied **11**, 034053 (2019).

[84]J. M. Arrazola, P. Wallden, and E. Andersson, "Multiparty Quantum Signature Schemes", Quantum Inf. Comput **6**, 0435 (2016).

[85]T.-Y. Wang, X.-Q. Cai, Y.-L. Ren, and R.-L. Zhang, "Security of quantum digital signatures for classical messages", Sci. Rep. **5**, 9231 (2015).

[86]T.-Y. Wang, J.-F. Ma, and X.-Q. Cai, "The postprocessing of quantum digital signatures", Quantum Inf. Process. **16**, 19 (2017).

[87]C. C. W. Lim, B. Korzh, A. Martin, F. Bussières, R. Thew, and H. Zbinden, "Detector-device-independent quantum key distribution", Appl. Phys. Lett. **105**, 221112 (2014).

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

[89]C.-H. Zhang, Y.-T. Fan, C.-M. Zhang, G.-C. Guo, and Q. Wang, "Twin-field quantum digital signatures", (2020), arXiv:2003.11262 [quant-ph].

[90]T. G. Noh, "Counterfactual quantum cryptography", Phys. Rev. Lett. **103**, 230501 (2009).

[91]H. Salih, Z. H. Li, M. Al-Amri, and M. S. Zubairy, "Protocol for direct counterfactual quantum communication", Phys. Rev. Lett. **110**, 170502 (2013).

[92]J. R. Hance, "How Quantum is 'Quantum Counterfactual Communication'?", (2019), arXiv:1909.07530 [quant-ph].

[93]L. Vaidman, "Analysis of counterfactuality of counterfactual communication protocols", Phys. Rev. A **99**, 052127 (2019).

[94]A. Leverrier, "Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction", Phys. Rev. Lett. **118**, 200501 (2017).

[95]F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-Variable Quantum Key Distribution with Gaussian Modulation – The Theory of Practical Implementations", Adv. Quantum Technol., 1800011 (2018).

[96]S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, "Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation", Phys. Rev. X **9**, 021059 (2019).

[97]M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing", Phys. Rev. A. **59**, 1829 (1999).

[98]D. Markham and B. C. Sanders, "Graph states for quantum secret sharing", Phys. Rev. A **78**, 042309 (2008).

[99]F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, "Virtual Entanglement and Reconciliation Protocols for Quantum Cryptography with Continuous Variables", Quantum Inf. Comput. **3** (2003).

[100]A. Karlsson, M. Koashi, and N. Imoto, "Quantum entanglement for secret sharing and secret splitting", Phys. Rev. A **59**, 162 (1999).

[101]W. Tittel, H. Zbinden, and N. Gisin, "Experimental demonstration of quantum secret sharing", Phys. Rev. A **63**, 042301 (2001).

[102]Z.-J. Zhang and Z.-X. Man, "Multiparty quantum secret sharing of classical messages based on entanglement swapping", Phys. Rev. A **72**, 022303 (2005).

[103]B. P. Williams, J. M. Lukens, N. A. Peters, B. Qi, and W. P. Grice, "Quantum secret sharing with polarization-entangled photon pairs", Phys. Rev. A **99**, 062311 (2019).

[104]K. Chen and H. K. Lo, "Conference key agreement and quantum sharing of classical secrets with noisy GHZ states", in Proceedings. International Symposium on Information Theory, 2005. ISIT 2005. Adelaide, SA, 2005. (2005), p. 1607.

[105]A. Keet, B. Fortescue, D. Markham, and B. C. Sanders, "Quantum secret sharing with qudit graph states", Phys. Rev. A **82**, 062315 (2010).

[106]H. K. Lau and C. Weedbrook, "Quantum secret sharing with continuous-variable cluster states", Phys. Rev. A **88**, 042313 (2013).

[107]Y. Wu, J. Zhou, X. Gong, Y. Guo, Z. M. Zhang, and G. He, "Continuous-variable measurement-device-independent multipartite quantum communication", Phys. Rev. A **93**, 022325 (2016).

[108]I. Kogias, Y. Xiang, Q. He, and G. Adesso, "Unconditional security of entanglement-based continuous-variable quantum secret sharing", Phys. Rev. A **95**, 012315 (2017).

[109]S. Armstrong, M. Wang, R. Y. Teh, Q. Gong, Q. He, J. Janousek, H.-A. Bachor, M. D. Reid, and P. K. Lam, "Multipartite Einstein–Podolsky–Rosen steering and genuine tripartite entanglement with optical networks", Nat. Phys. **11**, 167 (2015).

[110]Y. Xiang, I. Kogias, G. Adesso, and Q. He, "Multipartite Gaussian steering: Monogamy constraints and quantum cryptography applications", Phys. Rev. A **95**, 010101(R) (2017).

[111]C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, "High-rate secure quantum conferencing", (2017), arXiv:1709.06988 [quant-ph].

[112]Z.-J. Zhang, Y. Li, and Z.-X. Man, "Multiparty quantum secret sharing", Phys. Rev. A **71**, 044301 (2005).

[113]C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, "Experimental single qubit quantum secret sharing", Phys. Rev. Lett. **95**, 230505 (2005).

[114]F. G. Deng, X. H. Li, H. Y. Zhou, and Z. J. Zhang, "Improving the security of multiparty quantum secret sharing against Trojan horse attack", Phys. Rev. A **72**, 044302 (2005).

[115]S. J. Qin, F. Gao, Q. Y. Wen, and F. C. Zhu, "Improving the security of multiparty quantum secret sharing against an attack with a fake signal", Phys. Lett. A **357**, 101 (2006).

[116]G. P. He, "Comment on "Experimental single qubit quantum secret sharing"", Phys. Rev. Lett. **98**, 028901 (2007).

[117]C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, "Schmid et al. Reply", Phys. Rev. Lett. **98**, 028902 (2007).

[118]W. P. Grice and B. Qi, "Quantum secret sharing using weak coherent states", Phys. Rev. A **100**, 022339 (2019).

[119]M. Hai-Qiang, W. Ke-Jin, and Y. Jian-Hui, "Experimental single qubit quantum secret sharing in a fiber network configuration", Opt. Lett. **38**, 4494 (2013).

[120]J. Bogdanski, J. Ahrens, and M. Bourennane, "Sagnac secret sharing over telecom fiber networks", Opt. Express **17**, 1055 (2009).

[121]S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, "Experimental demonstration of four-party quantum secret sharing", Phys. Rev. Lett. **98**, 020503 (2007).

[122]B. A. Bell, D. Markham, D. A. Herrera-Martí, A. Marin, W. J. Wadsworth, J. G. Rarity, and M. S. Tame, "Experimental demonstration of graph-state quantum secret sharing", Nat. Commun. **5**, 5480 (2014).

[123]Y. A. Chen, A. N. Zhang, Z. Zhao, X. Q. Zhou, C. Y. Lu, C. Z. Peng, T. Yang, and J. W. Pan, "Experimental quantum secret sharing and third-man quantum cryptography", Phys. Rev. Lett. **95**, 200502 (2005).

[124]A. Broadbent and C. Schaffner, "Quantum Cryptography Beyond Quantum Key Distribution", Des. Codes Cryptogr. **78**, 351 (2015).

[125]M. Dušek, N. Lütkenhaus, and M. Hendrych, "Quantum Cryptography", Prog. Opt. **49**, 381 (2006).

[126]C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).

[127]M. Ban, K. Kurokawa, R. Momose, and O. Hirota, "Optimum measurements for discrimination among symmetric quantum states and parameter estimation", International Journal of Theoretical Physics **36**, 1269 (1997).

[128]S. M. Barnett, "Minimum-error discrimination between multiply symmetric states", Physical Review A **64**, 030303 (R) (2001).

[129]P. Wallden, V. Dunjko, and E. Andersson, "Minimum-cost quantum measurements for quantum information", J. Phys. A: Math. Theor **47**, 125303 (2014).

[130]S. M. Barnett and S. Croke, "Quantum state discrimination", Advances in optics and photonics **1**, 238.

[131]J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, "Quantum key distribution over 25 km with an all-fiber continuous-variable system", Phys. Rev. A **76**, 042305 (2007).

[132]A. Leverrier and P. Grangier, "Simple proof that Gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a Gaussian modulation", Phys. Rev. A **81**, 062314 (2010).

[133]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 (2008).

[134]A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states", Phys. Rev. Lett. **114**, 070501 (2015).

[135]F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, "Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks", Phys. Rev. Lett. **109**, 100502 (2012).

[136]A. Leverrier and P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation", Phys. Rev. Lett. **102**, 180504 (2009).

[137]P. Papanastasiou, C. Lupo, C. Weedbrook, and S. Pirandola, "Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal-loss channels", Phys. Rev. A **98**, 012340 (2018).

[138]F. Grosshans and P. Grangier, "Reverse reconciliation protocols for quantum cryptography with continuous variables", in Proceedings of the 6th International Conference on Quantum Communications, Measurement and Computing (2002).

[139]E. W. Weisstein, *Gamma Function*, `http://mathworld.wolfram.com/GammaFunction.html` (visited on 07/02/2020).

[140]C. Silberhorn, T. C. Ralph, N Lütkenhaus, and G Leuchs, "Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit", Phys. Rev. Lett. **89**, 167901 (2002).

[141]J. Lin, T. Upadhyaya, and N. Lütkenhaus, "Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution", Phys. Rev. X **9**, 041064 (2019).

[142]E. W. Weisstein, *Incomplete Gamma Function*, `http://mathworld.wolfram.com/IncompleteGammaFunction.html` (visited on 07/02/2020).

[143]A. Leverrier and P. Grangier, "Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation", Phys. Rev. A **83**, 042312 (2011).

[144]M. Navascués, F. Grosshans, and A. Acín, "Optimality of Gaussian attacks in continuous-variable quantum cryptography", Phys. Rev. Lett. **97**, 190502 (2006).

[145]R. García-Patrón and N. J. Cerf, "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution", Phys. Rev. Lett. **97**, 190503 (2006).

[146]Y. B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus, "Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks", Phys. Rev. A **79**, 012307 (2009).

[147]K. Brádler and C. Weedbrook, "A security proof of continuous-variable QKD using three coherent states", Phys. Rev. A **97**, 022310 (2018).

[148]K. P. Seshadreesan, L. Lami, and M. M. Wilde, "Rényi relative entropies of quantum Gaussian states", J. Math. Phys. **59**, 072204 (2018).

[149]A. Winick, N. Lütkenhaus, and P. J. Coles, "Reliable numerical key rates for quantum key distribution", Quantum **2**, 77 (2018).

[150]G. J. Simmons, "Prepositioned shared secret and/or shared control schemes", in Advances in Cryptology - Eurocrypt '89 LNCS 434 (1990), p. 436.

[151]D. Gottesman, "Theory of Quantum Secret Sharing", Phys. Rev. A **61**, 042311 (2000).

[152]E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: Principle, security and implementations", Entropy **17**, 6072 (2015).

[153]I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states", Proc. R. Soc. A **461**, 207 (2005).

[154]F. Furrer, T. Gehring, C. Schaffner, C. Pacher, R. Schnabel, and S. Wehner, "Continuous-Variable Protocol for Oblivious Transfer in the Noisy-Storage Model", Nat. Commun. **8**, 1450 (2018).

[155]G. De Palma, "Uncertainty relations with quantum memory for the Wehrl entropy", Lett. Math. Phys. **108**, 2139 (2018).

[156]G. De Palma, "The Wehrl entropy has Gaussian optimizers", Lett. Math. Phys. **108**, 97 (2018).

[157]K. Wei, X. Yang, C. Zhu, and Z. Q. Yin, "Quantum secret sharing without monitoring signal disturbance", Quantum Inf. Process. **17** (2018).

[158]T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance", Nature **509**, 475 (2014).

[159]W. P. Grice, P. G. Evans, B. Lawrie, M. Legré, P. Lougovski, W. Ray, B. P. Williams, B. Qi, and A. M. Smith, "Two-Party secret key distribution via a modified quantum secret sharing protocol", Opt. Express **23**, 7300 (2015).

[160]B. Sullivan, "Security Briefs - Cryptographic Agility", MSDN Mag. **24** (2009).

[161]B. Schneier, *Real-world security and the internet of things*, https://www.schneier.com/blog/archives/2016/07/real-world_secu.html.

[162]B. Schneier, *Security and the internet of things*, https://www.schneier.com/blog/archives/2017/02/security_and_th.html.

[163] S. Richter, M. Thornton, I. Khan, H. Scott, K. Jaksch, U. Vogl, B. Stiller, G. Leuchs, C. Marquardt, and N. Korolkova, "Agile quantum communication: signatures and secrets", (2020), arXiv:2001.10089 [quant-ph].

[164] "Quantum Key Distribution (QKD); Application Interface", ETSI Industry Specification Group Quantum Key Distribution; ETSI Group Specification (2010).

[165] "Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API", ETSI Industry Specification Group Quantum Key Distribution; ETSI Group Specification (2019).

[166] N. Killoran, J. Izaac, N. Quesada, V. Bergholm, M. Amy, and C. Weedbrook, "Strawberry Fields: A Software Platform for Photonic Quantum Computing", Quantum **3**, 129 (2019).

[167] *Qiskit API Documentation*, (2019) https://qiskit.org/documentation/index.html.

[168] P. Murali, J. M. Baker, A. J. Abhari, F. T. Chong, and M. Martonosi, "Noise-Adaptive Compiler Mappings for Noisy Intermediate-Scale Quantum Computers", in ASPLOS '19: Proceedings of the Twenty-Fourth International conference on Architectural Support for Programming Languages and Operating Systems (2019), p. 1015.

[169] G. Agrawal, *Applications of Nonlinear Fiber Optics* (Elsevier, Amsterdam, 2008).

[170] I. Khan, B. Stiller, K. Jaksch, N. Jain, C. Peuntinger, K. Günthner, T. Röthlingshöfer, D. Elser, C. Marquardt, and G. Leuchs, "Towards continuous-variable quantum key distribution at GHz rates", Poster QCrypt Conference Tokyo, Japan (2015).

[171] I. Khan, B. Stiller, K. Jaksch, K. Günthner, C. Peuntinger, J. Geyer-Ramsteck, D. Elser, C. Pacher, C. Marquardt, and G. Leuchs, "Continuous-variable quantum communication at 10 GHz and compatible with telecom networks", Poster QCrypt Conference Washington, USA (2016).

[172] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution", Rev. Mod. Phys. **81**, 1301 (2009).

[173] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, "Modular network for high-rate quantum conferencing", Commun. Phys. **2**, 118 (2019).

[174] S. Ren, R. Kumar, A. Wonfor, X. Tang, R. Penty, and I. White, "Reference pulse attack on continuous variable quantum key distribution with local local oscillator under trusted phase noise", J. Opt. Soc. Am. B **36**, B7 (2019).

[175]D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, "High-speed continuous-variable quantum key distribution without sending a local oscillator", Opt. Lett. **40**, 3695 (2015).

[176]T. Ozawa, H. M. Price, A. Amo, N. Goldman, M. Hafezi, L. Lu, M. Rechtsman, D. Schuster, J. Simon, O. Zilberberg, and I. Carusotto, "Topological Photonics", Rev. Mod. Phys. **91**, 015006 (2019).

[177]S. Lieu, "Topological phases in the non-Hermitian Su-Schrieffer-Heeger model", Phys. Rev. B **97**, 045106 (2018).

[178]M. Wolinsky and H. J. Carmichael, "Quantum noise in the parametric oscillator: From squeezed states to coherent-state superpositions", Phys. Rev. Lett. **60**, 1836 (1988).

[179]D. Braun, "Creation of entanglement by interaction with a common heat bath", Phys. Rev. Lett. **89** (2002).

[180]S. Clark, A. Peng, M. Gu, and S. Parkins, "Unconditional preparation of entanglement between atoms in cascaded optical cavities", Phys. Rev. Lett. **91**, 177901 (2003).

[181]M. Roghani and H. Weimer, "Dissipative preparation of entangled many-body states with Rydberg atoms", Quantum Sci. Technol. **3**, 035002 (2018).

[182]P. Zanardi and M. Rasetti, "Noiseless quantum codes", Phys. Rev. Lett. **79**, 3306 (1997).

[183]M. E. Kimchi-Schwartz, L. Martin, E. Flurin, C. Aron, M. Kulkarni, H. E. Tureci, and I. Siddiqi, "Stabilizing Entanglement via Symmetry-Selective Bath Engineering in Superconducting Qubits", Phys. Rev. Lett. **116**, 240503 (2016).

[184]H. M. Cammack, P. Kirton, T. M. Stace, P. R. Eastham, J. Keeling, and B. W. Lovett, "Coherence protection in coupled quantum systems", Phys. Rev. A **97**, 022103 (2018).

[185]Z. Leghtas, S. Touzard, I. M. Pop, A. Kou, B. Vlastakis, A. Petrenko, K. M. Sliwa, A. Narla, S. Shankar, M. J. Hatridge, M. Reagor, L. Frunzio, R. J. Schoelkopf, M. Mirrahimi, and M. H. Devoret, "Confining the state of light to a quantum manifold by engineered two-photon loss", Science **347**, 853 (2015).

[186]F. Verstraete, M. M. Wolf, and J. Ignacio Cirac, "Quantum computation and quantum-state engineering driven by dissipation", Nat. Phys. **5**, 633 (2009).

[187]A. Metelmann and A. A. Clerk, "Nonreciprocal photon transmission and amplification via reservoir engineering", Phys. Rev. X **5**, 021025 (2015).

[188]D. Porras and S. Fernández-Lorenzo, "Topological amplification in photonic lattices", Phys. Rev. Lett. **122**, 143901 (2019).

[189] D. N. Biggerstaff, R. Heilmann, A. A. Zecevik, M. Gräfe, M. A. Broome, A. Fedrizzi, S. Nolte, A. Szameit, A. G. White, and I. Kassal, "Enhancing coherent transport in a photonic network using controllable decoherence", Nat. Commun. **7**, 11282 (2016).

[190] D. Mogilevtsev, G. Y. Slepyan, E. Garusov, S. Y. Kilin, and N. Korolkova, "Quantum tight-binding chains with dissipative coupling", New J. Phys. **17**, 043065 (2015).

[191] A. Xuereb, S. Barzanjeh, and M. Aquilina, "Routing thermal noise through quantum networks", in Proc. SPIE 10672, 10672N (2018).

[192] J. T. Barreiro, M. Müller, P. Schindler, D. Nigg, T. Monz, M. Chwalla, M. Hennrich, C. F. Roos, P. Zoller, and R. Blatt, "An open-system quantum simulator with trapped ions", Nature **470**, 486 (2011).

[193] J. F. Poyatos, J. I. Cirac, and P Zoller, "Quantum Reservoir Engineering with Laser Cooled Trapped Ions", Phys. Rev. Lett. **77**, 4728 (1996).

[194] E. Kapit, "The upside of noise: Engineered dissipation as a resource in superconducting circuits", Quantum Sci. Technol. **2**, 033002 (2017).

[195] S. Mukherjee, A. Spracklen, D. Choudhury, N. Goldman, P. Öhberg, E. Andersson, and R. R. Thomson, "Observation of a Localized Flat-Band State in a Photonic Lieb Lattice", Phys. Rev. Lett. **114**, 245504 (2015).

[196] R. A. Vicencio, C. Cantillano, L. Morales-Inostroza, B. Real, C. Mejía-Cortés, S. Weimann, A. Szameit, and M. I. Molina, "Observation of Localized States in Lieb Photonic Lattices", Phys. Rev. Lett. **114**, 245503 (2015).

[197] G. Agrawal, *Nonlinear Fiber Optics* (Academic, Oxford, 2012).

[198] S. Mukherjee, D. Mogilevtsev, G. Y. Slepyan, T. H. Doherty, R. R. Thomson, and N. Korolkova, "Dissipatively coupled waveguide networks for coherent diffusive photonics", Nat. Commun. **8**, 1909 (2017).

[199] Vitron, *Vitron IG-2 Datasheet*, (2014) https://refractiveindex.info/download/data/2014/VITRONIG-2DatenblattJuni2014.pdf.

[200] H. J. Carmichael, *Statistical methods in quantum optics* 2 (Springer-Verlag Berlin Heidelberg, 1999).

[201] Y. R. Shen, "Quantum statistics of nonlinear optics", Physical Review **155**, 923 (1967).

[202] R. Loudon, "Non-classical effects in the statistical properties of light", Reports on Progress in Physics **43**, 913 (1980).

[203] H. D. Simaan and R. Loudon, "Quantum statistics of single-beam two-photon absorption", J. Phys. A: Math. Gen. **8**, 539 (1975).

[204]H. D. Simaan and R. Loudon, "Off-diagonal density matrix for single-beam two-photon absorbed light", J. Phys. A: Math. Gen. **11**, 435 (1978).

[205]L. Mandel, "Sub-poissonian photon statistics in resonance fluorescence", Opt. Lett. **4**, 205 (1979).

[206]L. Davidovich, "Sub-Poissonian processes in quantum optics", Rev. Mod. Phys. **68**, 127 (1996).

[207]H Ezaki, E Hanamura, and Y Yamamoto, "Generation of phase states by two-photon absorption", Phys. Rev. Lett. **83**, 3558 (1999).

[208]M Alexanian and S. Bose, "Comment on "Generation of phase states by two-photon Absorption"", Phys. Rev. Lett. **85**, 1136 (2000).

[209]H. Ezaki, E. Hanamura, and Y. Yamamoto, "Ezaki et al. reply", Phys. Rev. Lett. **85**, 1137 (2000).

[210]E. W. Weisstein, *Modified Bessel Function of the First Kind*, `https://mathworld.wolfram.com/ModifiedBesselFunctionoftheFirstKind.html` (visited on 02/10/2020).

[211]V. I. Man'ko, G. Marmo, E. C. Sudarshan, and F. Zaccaria, "F-Oscillators and Nonlinear Coherent States", Phys. Scr. **55**, 528 (1997).

[212]R. L. D. M. Filho and W Vogel, "Nonlinear coherent states", Phys. Rev. A **54**, 4560 (1996).

[213]A. Mikhalychev, D. Mogilevtsev, and S. Kilin, "Nonlinear coherent loss for generating non-classical states", J. Phys. A Math. Theor. **44**, 325307 (2011).

[214]D. Mogilevtsev, A. Mikhalychev, V. S. Shchesnovich, and N. Korolkova, "Nonlinear dissipation can combat linear loss", Phys. Rev. A **87**, 063847 (2013).

[215]D Mogilevtsev and V. S. Shchesnovich, "Single-photon generation by correlated loss in a three-core optical fiber", Opt. Lett. **35**, 3375 (2010).

[216]V. S. Shchesnovich and D. Mogilevtsev, "Generators of nonclassical states by a combination of linear coupling of boson modes, Kerr nonlinearity, and strong linear losses", Phys. Rev. A **84**, 013805 (2011).

[217]N. Imoto, H. H. A. Haus, and Y. Yamamoto, "Quantum nondemolition measurement of the photon number via the optical Kerr effect", Phys. Rev. A **32**, 2287 (1985).

[218]M. Kitagawa and Y. Yamamoto, "Number-phase minimum-uncertainty state with reduced number uncertainty in a Kerr nonlinear interferometer", Phys. Rev. A **34**, 3974 (1986).

[219]P. D. Drummond and D. F. Walls, "Quantum theory of optical bistability. I. Nonlinear polarisability model", J. Phys. A. Math. Gen. **13**, 725 (1980).

[220]M. Delanty, S. Rebić, J. Twamley, and S Rebi, "Novel collective effects in integrated photonics", Eur. Phys. J. D **66**, 93 (2012).

[221]M. Thornton, A. Sakovich, A. Mikhalychev, J. D. Ferrer, P. De La Hoz, N. Korolkova, and D. Mogilevtsev, "Coherent Diffusive Photon Gun for Generating Nonclassical States", Phys. Rev. Appl. **12**, 064051 (2019).

[222]T. Wang, X. Gai, W. Wei, R. Wang, Z. Yang, X. Shen, S. Madden, and B. Luther-Davies, "Systematic z-scan measurements of the third order nonlinearity of chalcogenide glasses", Opt. Mater. Express **4**, 1011 (2014).

[223]G. Demetriou, D. W. Hewak, A. Ravagli, C. Craig, and A. Kar, "Nonlinear refractive index of ultrafast laser inscribed waveguides in gallium lanthanum sulphide", Appl. Opt. **56**, 5407 (2017).

[224]C. R. Doerr, M. Shirasaki, and F. I. Khatri, "Simulation of pulsed squeezing in optical fiber with chromatic dispersion", J. Opt. Soc. Am. B **94**, 143 (1994).

[225]H. A. Haus and Y Lai, "Quantum theory of soliton squeezing : a linearized approach", J. Opt. Soc. Am. B **7**, 386 (1990).

[226]H. Ju, "Intrapulse quantum spectral correlation of femtosecond optical pulses in optical fiber", Phys. Rev. A **85**, 033810 (2012).

[227]E. W. Weisstein, *Cumulant*, `https://mathworld.wolfram.com/Cumulant.html`.

[228]H. L. Butcher, D. G. MacLachlan, D. Lee, R. R. Thomson, and D. Weidmann, "Demonstration and characterization of ultrafast laser-inscribed mid-infrared waveguides in chalcogenide glass IG2", Opt. Express **26**, 10930 (2018).

[229]G. Adesso, "Entanglement of Gaussian states", PhD thesis (Facoltà di Scienze Matematiche Fisiche e Naturali, 2007).

[230]R. Simon, "Peres-Horodecki Separability criterion for continuous variable systems", Phys. Rev. Lett. **84**, 2726 (2000).

[231]M. B. Plenio, "Logarithmic negativity: A full entanglement monotone that is not convex", Phys. Rev. Lett. **95**, 090503 (2005).

[232]M. A. Taylor, J. Janousek, V. Daria, J. Knittel, B. Hage, H. A. Bachor, and W. P. Bowen, "Biological measurement beyond the quantum limit", Nat. Photonics **7**, 229 (2013).

[233]I. R. Berchera and I. P. Degiovanni, "Quantum imaging with sub-Poissonian light : challenges and perspectives in optical metrology", Metrologia **56**, 024001 (2019).

[234]Y. Lai and S. S. Yu, "General quantum theory of nonlinear optical-pulse propagation", Phys. Rev. A **51**, 817 (1995).

[235]A. Hosaka, K. Hirosawa, R. Sawada, and F. Kannari, "Generation of photon-number squeezed states with a fiber-optic symmetric interferometer", Opt. Express **23**, 235350 (2015).

[236] A. Mecozzi and P. Kumar, "Linearized quantum-fluctuation theory of spectrally filtered optical solitons", Opt. Lett. **22**, 1232 (1997).

[237] A. Hosaka, T. Kawamori, and F. Kannari, "Multimode quantum theory of nonlinear propagation in optical fibers", Phys. Rev. A **94**, 053833 (2016).

[238] N. Nishizawa, T. Horio, M. Mori, T. Goto, and K. Yamane, "Effect of group-velocity dispersion on photon-number squeezing of optical pulses using optical fibers and spectral filter", Jpn. J. Appl. Phys. **38**, 1961 (1999).

[239] M. Fiorentino, J. Sharping, P. Kumar, and A. Porzio, "Amplitude squeezing in a Mach-Zehnder fiber interferometer: Numerical analysis of experiments with microstructure fiber", Opt. Express **10**, 128 (2002).

[240] R. M. Corless and F. Nicolas, *A graduate introduction to numerical methods* (Springer, New York, 2013).

[241] J. R. Johansson, P. D. Nation, and F Nori, "QuTiP 2: A Python framework for the dynamics of open quantum systems", Comput. Phys. Commun. **184**, 1234 (2013).

[242] M. B. Plenio and P. L. Knight, "The quantum-jump approach to dissipative dynamics in quantum optics", Rev. Mod. Phys. **70**, 101 (1998).

[243] R. Dum and P. Zoller, "Monte Carlo simulation of the atomic master equation for spontaneous emission", Phys. Rev. A **45**, 4879 (1992).

[244] J. Dalibard, Y. Castin, and K. Mgllmer, "Wave-Function Approach to Dissipative Processes in Quantum Optics", Phys. Rev. Lett. **68**, 580 (1992).

[245] A. J. Daley, "Quantum trajectories and open many-body quantum systems", Adv. Phys. **63**, 77 (2014).