Continuous Variable Optimisation of Quantum Randomness and Probabilistic Linear Amplification

Jing Yan Haw

B. Sc. (Hons.), National University of Singapore, 2011.

**A thesis submitted for the degree of
Doctor of Philosophy
of The Australian National University**

Feb, 2018

Declaration

This thesis is an account of research undertaken between January 2013 and May 2017 at The Department of Physics, Faculty of Science, The Australian National University, Canberra, Australia.

Except where acknowledged in the customary manner, the material presented in this thesis is, to the best of my knowledge, original and has not been submitted in whole or part for a degree in any university. ComponentLibrary by Alexander Franzen [1] is used in several illustrations in the thesis.

Jing Yan Haw
13 Feb 2018

to my wife Nelly, my parents and my siblings for their understanding and encouragement.

Acknowledgments

I thank God, who has always been guiding me in life, His Word being a lamp for my feet and a light on my path. He has been gracious to me despite my human weaknesses, and has always provided me with an abundance of blessings through the people and resources along the process of completing this dissertation, which I shall thank now:

I thank my supervisor Ping Koy Lam for all his help throughout my PhD years. In my opinion, he is a brilliant scientist who is not only innovative and constantly brewing new ideas, but is also eager and fearless in the pursuit of science. He leads his students by example and cares for them genuinely, often exhibiting servanthood leadership with a humble spirit.

Besides Ping Koy, several other people contributed to my supervision. Although Thomas Symul was not with me throughout the entire PhD, I have learned a lot from his expertise in continuous variable quantum information and quantum optics. I wish him all the best in his future endeavour of life. Tim Ralph has been my external supervisor in the University of Queensland. He has been an inspiration, due to his broad interests in physics, from wormholes to fundamental quantum optics. I am grateful to have learned from him the ways of doing quality theoretical work, and I look forward to more collaborations in the future. Ben Buchler did not directly supervise me, but I did thoroughly enjoy myself by picking from his deep physical insights, and am grateful for his positive attitude towards problem-solving.

Syed Assad was my mentor throughout my years in ANU. He's a rare breed: with the exceptional skills of a theorist, experimentalist and also a computational physicist all in one package. I would readily deem his as the "oracle" of our lab. During my course of my PhD, Assad has taught me many things, and I treasure all the good memories of working and discussing scientific problems with him. My 1064 lab team-mates worked hard with me in quantum information experiments, sharing optical tables (and the occasional music) together. I thank them all: Helen Chrzanowski, Sara Hosseini, Geng Jiao, Yong Shen, Seiji Armstrong, Oliver Thearle, Jie Zhao, Jiri Janousek, Alexandre Brieussel, Thibault Michel, Hao Jeng, Chunle Xiong, Mark Bradshaw, Siobhan Tobin; for all the quality scientific exchange, and for the joint effort of countless hours in the lab, setting up and performing the experiment, especially for the probabilistic protocols which required a humongous amount of data.

I am indebted to previous alumni of our group, for the resources they provided through the LabView acquisition system, thesis, and papers which have been extremely helpful for me. These resources allowed me to "stand on the shoulders of giants", building on their past insights and experiences to make further progress. I would also like to thank my colleagues in the ANU quantum optics group: Giovanni Guccione, Pierre Vernaz-Gris, Geoff Campbell, Jesse Everett, Daniel Higginbottom, Oliver Pinel, Ming-Tao Cao, Mehdi Hosseini, YoungWook Cho, Takeshi Toyama, Melanie Mraz, Andre Carvalho, Jiayi Qin, Ruvindha Lecamwasam, Jessica Eastman, Jinyong Ma, Anthony Leung, Aaron Tranter, and those who I might have missed. You guys are not just my science buddies, but also life buddies, and I retain all the pleasant memories of our time together, especially those with various activities, like international dinner night, board games night etc. And, just for the record, I am always happy to organize laksa night, if anyone should request so.

I am extremely grateful to work with my collaborators: Prof. Howard M Wiseman, Nathan Walk and Saleh Rahimi-Keshari, Jayne Thompson, Andrew Lance, Prof. Vlatko Vedral, Prof. Mile Gu, Christian Weedbrook, Xiao Yuan, Nelly Ng, Yimin Wang, and Vikram Sharma. A special thank you goes to Prof. Mile Gu who hosted me while I was visiting IIIS Tsinghua and CQT Singapore during my PhD. Meanwhile, the ANU HDR admin team (Amanda White, Laura Walmsley, Liudmila Mangos and Karen Nulty) has always been kind and helpful, making my life as a PhD student easier in various administrative ways. To them, I am very indebted.

My life in Canberra would have been rather lonesome, if it weren't for the warm presence of the community in Westminster Presbyterian Church Belconnen. I thank Pastor Geoff Findlay, who is an ANU alumni with some Physics background. He is a living testimony that science and faith coexist in harmony. The church family has been extremely supportive to me throughout the years, disciplining me in the faith and praying unswervingly for my strength and health, especially during the difficult times where I was struggling to meet academic deadlines. My housemates John Zhang, Hendra Gunadi, Kuangda He have been excellent friends to me, where we mutually encouraged each other in every aspect of life. I thank them for the guitar lessons too; I left that house with a marked improvement in my taste and skills in music.

Finally, I want to thank my family for providing me encouragement, love and financial and emotional support during my PhD; and my friends. Lastly, I thank Nelly, my lovely wife, for helping with the proofreading of my thesis, for all the discussions we had on quantum information, and for being my partner in science, life, and faith.

Abstract

In the past decade, quantum communication protocols based on continuous variables (CV) has seen considerable development in both theoretical and experimental aspects. Nonetheless, challenges remain in both the practical security and the operating range for CV systems, before such systems may be used extensively. In this thesis, we present the optimisation of experimental parameters for secure randomness generation and propose a non-deterministic approach to enhance amplification of CV quantum state.

The first part of this thesis examines the security of quantum devices: in particular, we investigate *quantum random number generators* (QRNG) and *quantum key distribution* (QKD) *schemes*. In a realistic scenario, the output of a quantum random number generator is inevitably tainted by classical technical noise, which potentially compromises the security of such a device. To safeguard against this, we propose and experimentally demonstrate an approach that produces side-information independent randomness. We present a method for maximising such randomness contained in a number sequence generated from a given quantum-to-classical-noise ratio. The detected photocurrent in our experiment is shown to have a real-time random-number generation rate of 14 (Mbit/s)/MHz.

Next, we study the one-sided device-independent (1sDI) quantum key distribution scheme in the context of continuous variables. By exploiting recently proven entropic uncertainty relations, one may bound the information leaked to an eavesdropper. We use such a bound to further derive the secret key rate, that depends only upon the conditional Shannon entropies accessible to Alice and Bob, the two honest communicating parties. We identify and experimentally demonstrate such a protocol, using only coherent states as the resource. We measure the correlations necessary for 1sDI key distribution up to an applied loss equivalent to 3.5 km of fibre transmission.

The second part of this thesis concerns the improvement in the transmission of a quantum state. We study two approximate implementations of a probabilistic noiseless linear amplifier (NLA): a physical implementation that truncates the working space of the NLA or a measurement-based implementation that realises the truncation by a bounded postselection filter. We do this by conducting a full analysis on the measurement-based NLA (MB-NLA), making explicit the relationship between its various operating parameters, such as amplification gain and the cut-off of operating domain. We compare it with its physical counterpart in terms of the Husimi Q-distribution and their probability of success.

We took our investigations further by combining a probabilistic NLA with an ideal deterministic linear amplifier (DLA). In particular, we show that when NLA gain is strictly lesser than the DLA gain, this combination can be realised by integrating an MB-NLA in an optical DLA setup. This results in a hybrid device which we refer to as the *heralded hybrid quantum amplifier*. A quantum cloning machine based on this hybrid amplifier is constructed through an amplify-then-split method. We perform probabilistic cloning of arbitrary coherent states, and demonstrate the production of up to five clones, with the fidelity of each clone clearly exceeding the corresponding no-cloning limit.

Contents

Chapter 1

Introduction

Background

Throughout the history of human civilization, while being at war against enemies, we have learned to communicate with our allies, by artfully hiding information from our enemies during transmission. These techniques are referred to as *cryptography*, in fact, the word *crypto* has its origin in ancient Greek, means "hidden" or "secret". With the rise of the internet and recent trends to the Internet of Things, an unbelievable amount of information makes is way through the internet every day. Such information includes not only our personal information such as financial or health data but also commercial dealings and military secrets. It is thus imperative to ensure the encryption remains secure, even with the advent of future technology.

There are various sets of encryption standards used in modern-day communication, such as advanced encryption standard (AES) and Rivest, Shamir and Adleman (RSA) ciphers. Though being efficiently implementable, most schemes rely on computational assumptions in order to achieve security. For example, the RSA cipher depends on the assumption that factorization of large numbers is a hard mathematical problem [2, 3]. Such encryptions, though safe against classical computer for most practical purposes, are however prone to attacks with the future advances of hardware and algorithm, including the construction of a large-scale quantum computer and Shor's algorithm [4][1].

Encryption can, in principle, be more reliable: information theoretic security does not rely on any such computational assumptions, and therefore poses a desirable alternative. A particular candidate that fulfil this is the one-time pad (OTP), wherein 1949, it was proven by Shannon that an OTP provides unconditional security. In such a scheme, the plaintext (message) is paired with a set of uniform random keys of equal length via simple modular operations. Provided the key is truly random, the only way to decipher the plain text is through the inverse application of the key, thus eliminating all potential vulnerability in mathematical assumptions.

Two questions follow from this discussion: How can we generate a truly random key? And how can we distribute this random key in the first place? The answer to

[1] We note the development of novel classical ciphers that would be invulnerable to quantum computer, known as post-quantum cryptography.

these questions lies in quantum communication technology or quantum cryptography. In particular, high-quality random number generators can be designed, and key distribution can be achieved by manipulating quantum systems or using them to encode information. This conforms with our intuition: fire against fire, quantum against quantum. Quantum random number generators (QRNGs) are devices that harness quantum mechanical effects to provide information-theoretically random bits. Quantum Key Distribution (QKD), on the other hand, is the sharing of such random keys over communicating parties by the encoding and transmission of quantum states. Owing to the quantum no-cloning theorem, unlike classical signals, an eavesdropper is unable to perfectly duplicate a quantum signal without being undetected [5]. These technologies, due to their simplicity and robustness, are already mature enough to leap out of the lab. For example, there are already several commercial QRNG products in the market [6] offered by quantum technology companies such as ID Quantique [7] and Quintessence Labs [8]. The effort runs worldwide: in Europe, there is the SECOQC QKD network demonstration [9], while in Tokyo, a QKD network is already running at the metropolitan scale [10]. With the recent demonstration of satellite-to-ground QKD in China [11], intercontinental quantum communication is now one step closer to the reality.

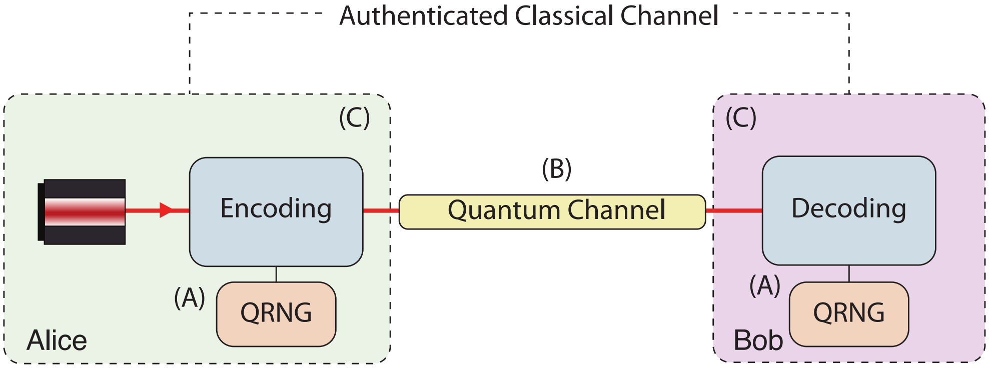


Figure 1.1: Conceptual diagram of a generic quantum cryptographic scheme. Alice and Bob share a set of information-theoretically secure one-time pad by communicating through both quantum and classical channels. Three components of a quantum communication protocol studied in this thesis are: (A) QRNG (B) the quantum channel and (C) the encoding and decoding stages.

A generic quantum cryptography channel is depicted in Fig. 1.1. Here, Alice, who controls the source, encodes random bits from the QRNG onto the quantum state. The quantum signal will then be sent to Bob through a (lossy) quantum channel, which could be attacked by an eavesdropper Eve. When the signal arrives at Bob, he measures the received quantum state, in a randomly chosen measurement basis determined by his QRNG. Through an authenticated classical channel, Alice and Bob compare part of their bits and decide whether the quantum channel is safe enough to proceed with the extraction of a secret key . Should the protocol succeed, Alice and Bob will share a pair of unconditionally secure key for secret communication.

The protocol above works well if we assume that Eve only has the ability to tap into the quantum channel. In reality, this is actually not quite the case. First, Eve might be monitoring the classical information produced within the QRNG, such as current fluctuations, thus obtaining further information about the random encodings. There is also no guarantee whether the devices used by Alice and Bob are trustworthy, especially when the devices were bought off-the-shelves, instead of being built by the in-house experimentalist. Eve could have been involved in the manufacturing process, and hence holds partial information of either the encoding or the decoding phase. Imagine an extreme case, where Eve is the one giving Alice and Bob the device. These devices could be simulating the entire QKD process, and Eve has access to the entire information without the need to intercept the channel at all [2]. This leads to investigations of device independent QKD, which eliminates the need for such assumptions, at a price of conducting a loophole-free Bell test. This, however, turns out to be a heroic task, as only a few experimental groups have managed to perform such a feat recently [12, 13, 14].

Another problem/challenge for QKD would be the transmission distance. This is because unlike classical signal, quantum states are much more fragile and prone to losses [15]. The longest transmission record with standard telecom fibre and avalanche photodiode to date is a mere 300 km [16], impressive by quantum standards but primitive when compared to classical communication. This transmission was demonstrated by using discrete-variable (DV) quantum systems. On the other hand, continuous-variable (CV) systems offer higher speeds, but the maximum transmission distance so far is 100 km [17]. This greatly hinders the applicability of QKD, not to mention the larger goal of having a global quantum internet.

In this thesis, we study how CV quantum communication may be improved. In particular, we seek to contribute towards in the following aspects:

- Security of Quantum Devices
  We propose an information-theoretic way to quantify the randomness in a QRNG, which allows us to evaluate and maximise the amount of secure random bits in a CV-QRNG. On the other hand, if only one side is untrusted in a quantum communication protocol, the stringent requirement for a device independent QKD can be relaxed. In fact, we show that it is possible to generate secret keys in a one-sided device independent fashion by using only coherent states, which are readily available in the lab.

- Transmission of the quantum state
  A noiseless linear amplifier (NLA) can mitigate the transmission problem at the expense of allowing probabilistic events. Such devices can be expensive to procure, but we show that the desired effect may be achieved through a measurement-based approach instead. In the context of cloning, we also show that you can

[2] During the QKD protocol, it is always an assumption that Alice's and Bob's labs are isolated from the outside world, and therefore Eve may not access their equipment. Otherwise, an easy practical hack would be to install transmitters in the devices.

improve the cloning fidelity beyond deterministic bound with reasonable success rate by combining a probabilistic NLA with a deterministic linear amplifier.

1.1 Thesis plan

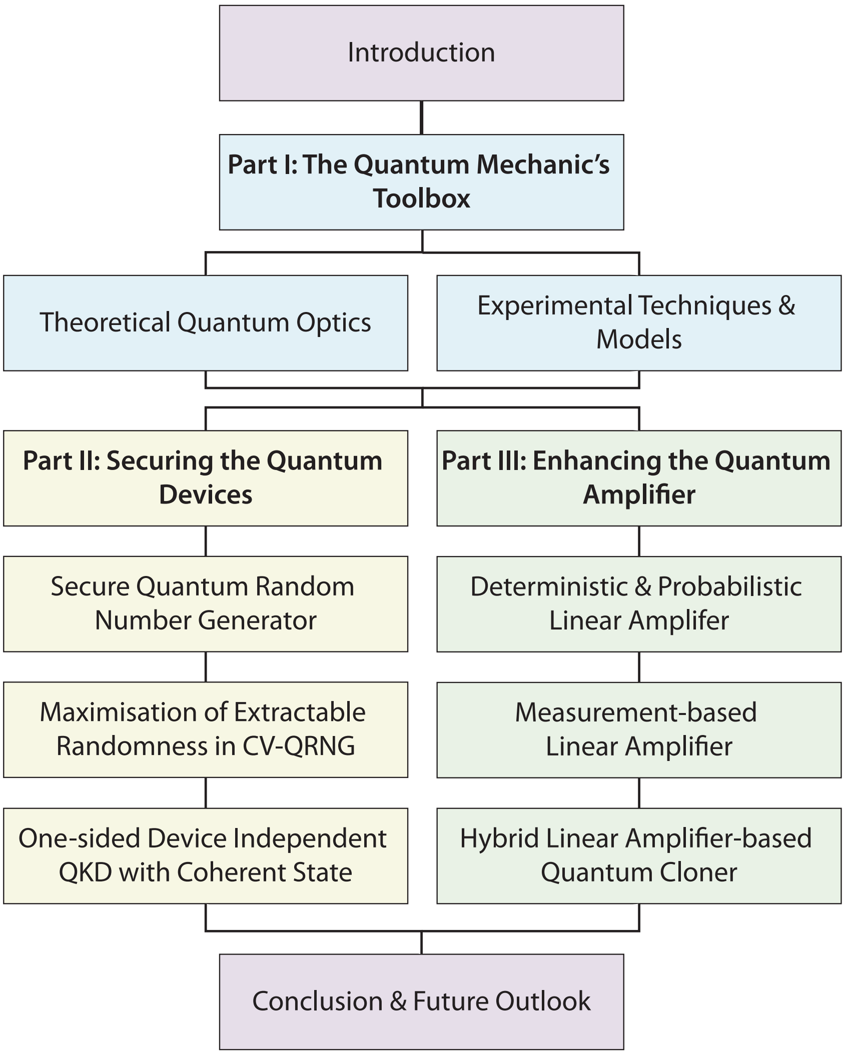

Introduction
Part I: The Quantum Mechanic's Toolbox
Theoretical Quantum Optics
Experimental Techniques & Models
Part II: Securing the Quantum Devices
Part III: Enhancing the Quantum Amplifier
Secure Quantum Random Number Generator
Deterministic & Probabilistic Linear Amplifer
Maximisation of Extractable Randomness in CV-QRNG
Measurement-based Linear Amplifier
One-sided Device Independent QKD with Coherent State
Hybrid Linear Amplifier-based Quantum Cloner
Conclusion & Future Outlook

Figure 1.2: The structure of this thesis.

In Fig. 1.2, we present the structure of this thesis. It can be divided into three parts: The quantum mechanic's toolbox, securing the quantum device and enhancing the quantum amplifier.

In Part I, we cover the theoretical and experimental background involved in the thesis. In the theory chapter, we first give a brief review of continuous variable quantum optics formalism, followed by a discussion on quantum information. For the experimental part, we introduce the essential linear optical components and digital control used for the experiments in this thesis.

We move on to the security of the quantum devices in Part II. In Chapter 4, we present the notion of quantum randomness, and further review and propose methods to quantify the randomness to guarantee its secrecy. Several techniques to extract uniform randomness from an otherwise bias entropy source is surveyed too. In Chapter 5, we propose a method to maximally harness randomness secure against classical eavesdropper and experimentally demonstrate it upon a CV-QRNG. In the last chapter of this part (Chapter 6), we introduce entropic uncertainty relations in CV and show how it unlocks the possibility of distilling secret keys, even when either of the communication parties may be using communication devices which are not secure. This possibility is proved with an experimental demonstration of one-sided device independent QKD protocol using only coherent states.

The Part III of the thesis discusses how quantum amplification can be enhanced by the adoption of a probabilistic approach. In Chapter 7, after a brief discussion on the deterministic amplification, two probabilistic amplifiers: physical-based and measurement-based amplifiers are compared and contrasted. We proposed a new type of amplifier, called the heralded hybrid linear amplifier. This novel amplifier brings the deterministic and probabilistic amplifier together as a unit, which is capable of generating propagating clones surpassing the deterministic approach.

We have also included two research projects in the appendix, which are related to a more general form of quantum correlations called quantum discord, which I have contributed.

1.2 Publications

The majority of the contents of this thesis have been published in international peer-reviewed journals or conference proceedings. Publications resulting from this thesis are as follows:

1. S. Hosseini, S. Rahimi-Keshari, J. Y. Haw, S. M. Assad, H. M. Chrzanowski, J. Janousek, T. Symul, T. C. Ralph, and P. K. Lam.
   "Experimental verification of quantum discord in continuous-variable states."
   Journal of Physics B: Atomic, Molecular and Optical Physics 47 (2), 025503 (2014).

2. S. Hosseini, S. Rahimi-Keshari, J. Y. Haw, S. M. Syed, H.M. Chrzanowski, J. Janousek, T. Symul, T. C. Ralph, P. K. Lam and M. Gu et al.
   "Experimental verification of quantum discord and operational significance of discord consumption."
   In CLEO: QELS Fundamental Science, pages FTh3A–6. Optical Society of America (2014).

3. H. Chrzanowski, N. Walk, J. Y. Haw, O. Thearle, S. Assad, J. Janousek, S. Hosseini, T. C. Ralph, T. Symul, and P. K. Lam.
   "Measurement-based noiseless linear amplification for quantum communication."
   In Proc. SPIE 9269, Quantum and Nonlinear Optics III, 926902 (2014).

4. J. Y. Haw, S. M. Assad, A. Lance, N. Ng, V. Sharma, P. K. Lam, and T. Symul.
"Maximization of extractable randomness in a quantum random-number generator."
Physical Review Applied 3 (5), 054004 (2015).

5. N. Walk, S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janousek, T. C. Ralph, T. Symul et al.
"Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution."
Optica 3 (6), 634-642 (2016).

6. J. Y. Haw, J. Zhao, J. Dias, S. M. Assad, M. Bradshaw, R. Blandino, T. Symul, T. C. Ralph, and P. K. Lam.
"Surpassing the no-cloning limit with a heralded hybrid linear amplifier for coherent states."
Nature Communications, 7, 13222 (2016).

7. M. Bradshaw, S. M. Assad, J. Y. Haw, S. H. Tan, P. K. Lam and M. Gu.
"The overarching framework between Gaussian quantum discord and Gaussian quantum illumination."
Physical Review A, 95 (2), 022333 (2017).

8. J. Zhao, J. Y. Haw, S. M. Assad, T. Symul, and P. K. Lam,
"Characterisation of measurement-based noiseless linear amplifier and its applications."
Physical Review A 96 (1), 012319 (2017).

9. J. Zhao, J. Dias, J. Y. Haw, T. Symul, M. Bradshaw, R. Blandino, T. Ralph, S. M. Assad, P. K. Lam. *"Quantum enhancement of signal-to-noise ratio with a heralded linear amplifier,"*
Optica 4 (11), 1421-1428 (2017).

10. J.Y. Haw, J. Zhao, J. Dias, S.M. Assad, M. Bradshaw, R. Blandino, T. Symul, T.C. Ralph, and P.K. Lam.
"Surpassing the no-cloning limit with a heralded hybrid linear amplifier."
2017 Conference On Lasers and Electro-Optics Pacific Rim (Cleo-Pr), IEEE (2017).

11. J. Zhao, J. Dias, J. Y. Haw, T. Symul, M. Bradshaw, R. Blandino, T. Ralph, S. M. Assad, P. K. Lam.
"Quantum Enhancement of Signal-to-noise Ratio for Arbitrary Coherent States Using Heralded Linear Amplifiers."
2017 Conference On Lasers and Electro-Optics Pacific Rim (Cleo-Pr), IEEE (2017).

Other works published during the course of my PhD are

1. X. Yuan, S. M. Assad, J. Thompson, J. Y. Haw, V. Vedral, T. C. Ralph, P.K. Lam, C. Weedbrook and M. Gu.

"Replicating the benefits of Deutschian closed timelike curves without breaking causality."
NPJ Quantum Information, 1:15007 (2015).

2. Y. Wang and J. Y. Haw.
"Bridging the gap between the Jaynes–Cummings and Rabi models using an intermediate rotating wave approximation."
Physics Letters A, 379(8):779–786 (2015).

Part I

The Quantum Mechanic's Toolbox

Chapter 2

Theoretical Quantum Optics

"And God said, 'Let there be light,' and there was light."

– Genesis 1:3, *The Bible*

Overview

This chapter comprises a short summary of the background knowledge underlying the scientific contributions of this thesis. We first give a few examples of quantum states that are relevant to this thesis, in particularly Gaussian states. We introduce briefly the covariance matrix formalism and provides examples of Gaussian states in this formalism, together with a selected number of Gaussian operations. After establishing the framework for continuous variable quantum states, we explain how (Gaussian) quantum measurements are performed, followed by a discussion on different approaches on visualising quantum states via quasi-probability distributions. Finally, we describe several ways to quantify information encoded in the quantum state.

2.1 The quantum optical field

The classical theory of the electromagnetic (EM) field as brought together in Maxwell's equations provides a highly accurate description of an astounding array of physical phenomena. Since the emergence of quantum physics, it was realized that classical electromagnetism had to be revised in order to explain more phenomenon in the quantum regime, in particular, the interaction of light and matter. This led to a full quantisation of the EM field, which was initially constructed by Paul Dirac [18], and further developed with Glauber's analysis of detection and coherence [19]. This theory, known as the quantum field theory, or sometimes referred to as second quantization, describes a broader range of phenomena that have no counterpart in the theories which are classical or semi-classical.

There are many excellent quantum optics books [20, 21, 22] out there that explain the topic of quantisation, so we will not reproduce them here. Colloquially, this involves taking the relevant physical observables, and putting "hats" on them, thereby changing them into physical operators. The quantisation of EM field can be done by realising that such fields may be elegantly described as a collection of independent harmonic oscillators, i.e., they share a similar Hamiltonian form. Therefore, one may perform a direct mapping between canonical variables of the radiation oscillator, and the non-commutative quantum-mechanical operators of the EM field.

The quantised EM field for a particular spatial mode is described by

$$\hat{E} = i\sum_k \left(\frac{\hbar\omega_k}{2\epsilon}\right)^{\frac{1}{2}} (\hat{a}_k e^{-i\omega_k t} - \hat{a}_k^\dagger e^{i\omega_k t}), \tag{2.1}$$

where k denotes the frequency and polarization modes of the light, ϵ is the permittivity of free space and ω is the frequency of the field. The symbols $\hat{a}_k$ and $\hat{a}_k^\dagger$ are referred to as creation and annihilation operators respectively, for reasons we shall observe later. These operators obey the bosonic commutation relations for a quantum harmonic oscillator, i.e.

$$[\hat{a}_k, \hat{a}_{k'}] = [\hat{a}_k^\dagger, \hat{a}_k^\dagger] = 0; \quad [\hat{a}_k, \hat{a}_{k'}^\dagger] = \delta_{kk'}. \tag{2.2}$$

Since these operators are non-Hermitian, they cannot be observed or measured directly in the lab. In other words, they do not correspond to a physical quantity associated with the system. It is hence more relevant to consider the Hermitian, so-called *quadrature operators*,

$$\hat{X}_k = \hat{a}_k + \hat{a}_k^\dagger \quad \text{and} \quad \hat{P}_k = i(\hat{a}_k^\dagger - \hat{a}_k). \tag{2.3}$$

Substituting this back to Eq. 2.1, we obtain

$$\hat{E} = \sum_k \left(\frac{\hbar\omega_k}{2\epsilon}\right)^{\frac{1}{2}} (\hat{X}_k \sin(\omega_k t) - \hat{P}_k \cos(\omega_k t)). \tag{2.4}$$

We see that the quadratures correspond to the in-phase and out-of-phase components of the EM field. Conventionally, $\hat{X}$ is known as the amplitude quadrature, and $\hat{P}$ is the phase quadrature. Following from the commutation relation $[\hat{a}_k, \hat{a}_k^\dagger] = 1$, one can show that $[\hat{X}, \hat{P}] = 2i$[1]. This is in agreement with the Heisenberg's Uncertainty Principle (HUP) of quantum mechanics, which states that it is impossible to simultaneously determine two non-commuting observables precisely. Analogous to the position and momentum in a classical harmonic oscillator, these quadrature operators are conjugate observables, and thus cannot be known perfectly at the same time.

We stress that HUP refers to the minimum spread of the non-commuting measurements over an ensemble, rather than the disturbance on the value of $\hat{B}$ caused by the prior measurement of $\hat{A}$ [23]. For the quadratures, HUP thus dictates that any attempt

[1] Throughout the thesis, we choose $\hbar = 2$, which corresponds to a variance of the vacuum $\Delta\hat{X}_v^\theta = 1$.

Mathematical formulation of the **Heisenberg Uncertainty Principle**: given the commutator relation between two arbitrary observables $\hat{A}$ and $\hat{B}$,

$$\Delta\hat{A}\Delta\hat{B} \geq \frac{1}{2}|\left\langle[\hat{A},\hat{B}]\right\rangle|^2, \tag{2.6}$$

where $\Delta\hat{O} = \sqrt{\left\langle\hat{O}^2\right\rangle - \left\langle\hat{O}\right\rangle^2}$ is the standard deviation of the observable $\hat{O}$ and the square root of the variance $\Delta^2\hat{O} = (\Delta\hat{O})^2$.

to simultaneously determine $\hat{X}$ and $\hat{P}$ is limited by

$$\Delta\hat{X}\Delta\hat{P} \geq 1. \tag{2.5}$$

This implies that when measuring the quadratures of the optical field, any attempt to increase the precision of one quadrature can only be done at the expense of the other conjugate quadrature.

The choice of using $\hat{X}$ and $\hat{P}$ here is simply one of convenience for demonstration. One may also consider a generalised quadrature operator formed by a linear combination of quadratures

$$\hat{X}^\theta = \cos\theta\hat{X} + \sin\theta\hat{P}, \qquad \theta \in [0, 2\pi]. \tag{2.7}$$

Such an operator also satisfies the HUP with its orthogonal quadratures, namely $\Delta\hat{X}^\theta\Delta\hat{X}^{\theta+\pi/2} = 1$ holds for any θ. We will now review several common quantum states, in particularly Gaussian states where its statistics can be fully characterized by the mean and variance of $\hat{X}$ and $\hat{P}$. We discuss how HUP can be used to unlock certain applications, which have an advantage compared to classical states due to their inherent quantum properties.

2.2 Optical quantum states

In this section, we limit our discussion to single mode states. For convenience of notation, we drop the subscript k for modes.

2.2.1 Number or Fock states

Given a particular quantised EM field described by a Hamiltonian

$$\hat{H} = \hbar\omega(\hat{a}^\dagger\hat{a} + \frac{1}{2}), \tag{2.8}$$

a commonly used state, known as the Fock state, $|n\rangle$, is the eigenstate of $\hat{H}$. Intuitively, if the system is in a particular Fock state $|n\rangle$, this implies that there are a number of n

photons in the system. The corresponding eigenvalues, $E_n = \hbar\omega(n+\frac{1}{2})$, shows that the energies of the oscillator are discretized and evenly spaced. In other words, each quanta of light contains the same amount of energy.

The creation (annihilation) operators act on $|n\rangle$, by adding (subtracting) a quanta of energy $\hbar\omega_k$, or otherwise represented as a single photon in the mode of interest:

$$\hat{a}^\dagger |n\rangle = \sqrt{n+1}\,|n+1\rangle \quad \text{and} \quad \hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle\,. \tag{2.9}$$

Together, the creation and the annihilation operators form the number operator $\hat{n} = \hat{a}^\dagger\hat{a}$. The ground state, or the vacuum state, $|0\rangle$ is defined as

$$\hat{a}\,|0\rangle = 0. \tag{2.10}$$

This allow us to rewrite the Fock states as successive applications of the creation operator on the vacuum state:

$$|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}|0\rangle. \tag{2.11}$$

Being linearly independent and normalised eigenstates, Fock states form a complete orthonormal basis for the Hilbert space of the quantum state. For example, any optical mode can be expanded as

$$\rho = \sum_{n,m} c_{n,m}\,|n\rangle\,\langle m|\,, \tag{2.12}$$

where ρ is the density matrix of the quantum state, and $c_{n,m}$ is a complex number.

In terms of the quadrature, one can verify that $\langle n|\,\hat{X}^\theta\,|n\rangle = \langle n|\,\hat{P}^\theta\,|n\rangle = 0$ for all n. This means regardless of the number of excitation in the mode, the amplitude and phase quadratures averages to zero. However, the uncertainty (or rather, the variance) in the amplitude quadrature in turn, scales as $2n$,

$$\Delta^2\hat{X}^\theta_n = \langle n|\,(\hat{X}^\theta)^2\,|n\rangle - \langle n|\,\hat{X}^\theta\,|n\rangle^2 = (2n+1). \tag{2.13}$$

2.2.2 Vacuum state

The zero-photon state of the quantum optical field, $|n=0\rangle$, is one of the most ubiquitous states in a quantum optics lab. This vacuum state exists throughout the electromagnetic spectrum, and more counter-intuitively, its energy is non-zero, i.e. $\langle 0|H|0\rangle = \hbar\omega/2$. Since the electromagnetic spectrum is continuous, there can in principle be an infinite number of zero-state photons, coexisting even in a finite volume [2].

Due to this non-zero ground state energy, the vacuum exhibits dynamical quantum fluctuations in the field. These quantum vacuum fluctuations lead to uncertainty in both the quadratures of the vacuum state according to $\Delta\hat{X} = \Delta\hat{P} = 1$, thus saturating the uncertainty principle seen in Eq. (2.5). In other words, the vacuum state is a state of min-

[2] Of course, this poses no significant technical problem since all energies may be evaluated relative to this infinite background.

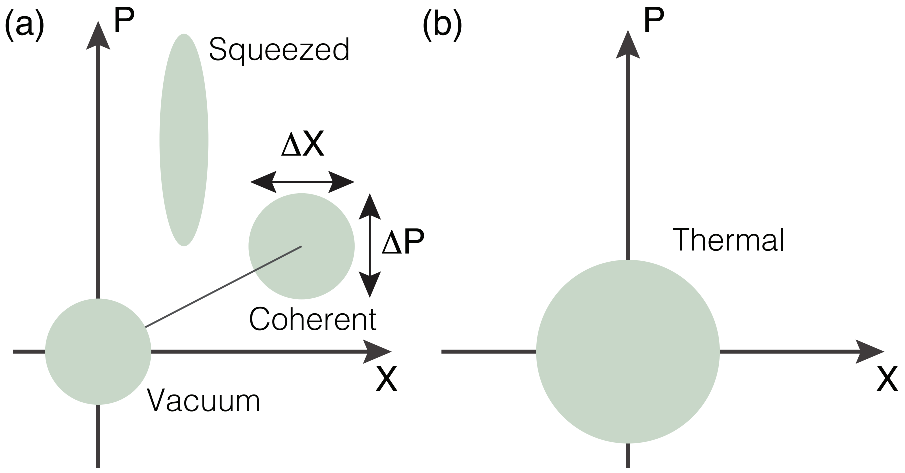


Figure 2.1: Ball-on-stick diagram for (a) vacuum state, coherent state, squeezed state and (b) thermal state. $\Delta X = \Delta P = 1$.

imal uncertainty. The noise which arises from measuring such a vacuum state is often referred to as the "quantum noise" or "shot noise". Meanwhile, its variance constitutes a reference in quantum optics, termed as the quantum noise limit (QNL). Despite the fact that quantum noise presents a fundamental limit to the precision of quantum measurements, we show that it is also the enabler of several quantum technologies, such as quantum random number generation (Chapter 5) and quantum cryptography (Chapter 6).

2.2.3 Coherent states

The coherent state, first introduced by Roy Glauber in 1967 - a result which in part constituted his Nobel prize - is the quantum mechanical state that most closely approximates the output of a laser light. It is defined as the eigenstate of the annihilation operator:

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,. \tag{2.14}$$

As $\hat{a}$ is a non-Hermitian operator, the eigenvalue α can be complex. A coherent state is simply a displaced vacuum state,

$$|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle\,, \tag{2.15}$$

where

$$\hat{D}(\alpha) = \exp\Big(\alpha\,\hat{a}^\dagger - \alpha^*\,\hat{a}\Big) \tag{2.16}$$

is a unitary displacement operator that shifts $|0\rangle$ by a coherent amplitude α. In the picture of a quantum mechanical version of phasor, a coherent state can be represented by a *ball-on-stick* diagram (Fig. 2.1). The ball is associated to the inherent quantum noise ($\Delta\hat{X}$ and $\Delta\hat{P}$) while the sticks is proportional to $|\alpha|$.

A coherent state can be expanded as the superposition of number states as

$$|\alpha\rangle = \sum_n |n\rangle \langle n|\alpha\rangle = e^{-|\alpha|^2/2} \sum_n \frac{\alpha^n}{(n!)^{1/2}} |n\rangle \,. \tag{2.17}$$

For $\alpha = 0$, we see that the vacuum state holds a unique position of simultaneously a number state and a coherent state. From this representation, it can also be shown that the coherent states are not pairwise orthogonal, with $|\langle\alpha|\beta\rangle|^2 = \exp\big(-|\alpha-\beta|^2\big)$. This feature of overlapping between coherent states allows the possibility of prepare-and-measure quantum communication (See Sec. 6.3.2). When $|\alpha-\beta|$ gets large, the overlap diminishes and the states are nearly orthogonal.

Given any coherent state $|\alpha\rangle$, there exists a useful relation between the expectation value of $\hat{X}$ and $\hat{P}$ quadratures. In particular, they give the real and imaginary parts of α:

$$\langle\hat{X}\rangle_\alpha = 2\,\mathrm{Re}\{\alpha\}, \quad \text{and} \quad \langle\hat{P}\rangle_\alpha = 2\,\mathrm{Im}\{\alpha\}. \tag{2.18}$$

Since coherent state is a displaced minimum uncertainty state, it also minimises all the quadrature variances simultaneously. In this regard, a coherent state is considered as the "most classical" state since it is closest to the case where both amplitude and phase are known exactly.

The mean number of photons contained in a coherent state is given by $\langle\alpha|\hat{n}|\alpha\rangle = |\alpha|^2$. It is spread according to a Poissonian distribution

$$P(n) = |\langle n|\alpha\rangle|^2 = \frac{|\alpha|^{2n}\, e^{-|\alpha|^2}}{n!}, \tag{2.19}$$

with a standard deviation of $\Delta\hat{n} = \alpha$.

2.2.4 Squeezed states

As mentioned in Sec. 2.1, the amount of uncertainty in one quadrature can be reduced provided the orthogonal quadrature is larger than the QNL. Such states are called squeezed states. The operation of the squeezing operator $\hat{S}(s) = \exp\big\{s(\hat{a}^2 - \hat{a}^{\dagger 2})/2\big\}$ upon the vacuum state gives rise to a squeezed state $|s\rangle = \hat{S}(s)\,|0\rangle$, with a squeezing level S[3]. By further acting a displacement operator $\hat{D}(\alpha)$ on the squeezed state, a displaced squeezed vacuum $|\alpha, s\rangle$ can be obtained.

The uncertainty in the quadratures of a squeezed vacuum state $|s\rangle$ can be derived as

$$\Delta X_s = e^{-s} \quad \text{and} \quad \Delta P_s = e^{s}. \tag{2.20}$$

[3] Here the squeezing parameter s is assumed to be real. A squeezed state along the quadrature axis θ_s can be considered by having a complex squeezing parameter $\xi = se^{i\theta_s}$.

Ideal (amplitude) squeezing is achieved in the limit of infinite squeezing, $s \to \infty$. In this limit, the squeezed amplitude quadrature will be known precisely, while the anti-squeezing quadrature will be fully unknown. The mean photon number for a displaced squeezed state is given by

$$\bar{n}_s = |\alpha|^2 + \sinh^2 s. \tag{2.21}$$

We observe that even for a squeezed vacuum ($\alpha = 0$), there are still photons in the state as long as the squeezing is finite ($s > 0$).

2.2.5 Thermal states

We now depart from pure states, and introduce a common type of mixed states encountered in the lab - thermal states. Such states are produced by thermal sources, such as a light bulb or a discharge lamp. It is diagonal in the Fock basis,

$$\rho_{\text{th}} = \frac{1}{1+\bar{n}_{\text{th}}} \sum_{n=0}^{\infty} \left(\frac{\bar{n}_{\text{th}}}{1+\bar{n}_{\text{th}}} \right)^n |n\rangle\langle n| \,, \tag{2.22}$$

or in other words, such state do not contain quantum coherences/superpositions relative to the Fock basis.

In the phase space, the thermal state is centered at zero ($\langle \hat{X}^\theta \rangle = 0$) and is symmetrical in all directions. In fact, it can be seen as the statistical mixture of the coherent state,

$$\rho_{\text{th}} = \int \mathrm{d}^2\alpha \, \frac{1}{\pi \bar{n}_{\text{th}}} e^{-|\alpha|^2/\bar{n}_{\text{th}}} \, |\alpha\rangle\langle\alpha| \,, \tag{2.23}$$

Unlike coherent states, the variance scales with the mean number of photon $\bar{n}_{\text{th}}$, i.e. $\Delta^2 \hat{X}^\theta = 2\bar{n}_{\text{th}} + 1$.

2.2.6 Two-mode squeezed state

Another significant quantum state in CV quantum optics is the two-mode squeezed state or EPR state. A two-mode vacuum squeezed state can simply be generated by interfering two squeezed vacuum states upon a beam splitter (Sec. 3.2.2). The Gaussian unitary, known as *two-mode squeezing operator*, acts on the two-mode vacuum to give,

$$\begin{aligned} |s\rangle_{\text{EPR}} &= \hat{S}_2(s) \, |0,0\rangle \\ &= \exp\Big\{ s(\hat{a}\hat{b} - \hat{a}^\dagger \hat{b}^\dagger)/2 \Big\} \, |0\rangle_a \, |0\rangle_b \\ &= \sqrt{1-\lambda^2} \sum_{n=0}^{\infty} (-\lambda)^n \, |n\rangle_a \, |n\rangle_b \ . \end{aligned} \tag{2.24}$$

where $\lambda = \tanh(s)$ denotes the strength of the correlation between the two modes. Such a highly correlated state, when considered locally, is actually a fully mixed, or a thermal state. This can be illustrated performing partial trace over a mode, say mode b

$$\begin{aligned}\rho_a = \mathrm{Tr}_b(|s\rangle\langle s|_{\mathrm{EPR}}) &= \frac{1}{\cosh^2 s}\sum_{n=0}^{\infty}(\tanh(s))^{2n}\ |n\rangle_a\langle n|_a \\ &= \frac{1}{1+\bar{n}}\sum_{n=0}^{\infty}\left(\frac{\bar{n}}{1+\bar{n}}\right)^n |n\rangle_a\langle n|_a\,, \end{aligned} \tag{2.25}$$

which is equivalent to the thermal state ρ_{th} defined in Eq. 2.22. Here, we have used $\bar{n} = \sinh^2 s$. Although the individual state inherits the properties of a thermal state, and hence is classical, the correlation between the quadratures is distinguishably quantum. Consider the the joint quadrature operators $\hat{X}_- = (\hat{X}_a - \hat{X}_b)/\sqrt{2}$ and $\hat{P}_+ = (\hat{P}_a - \hat{P}_b)/\sqrt{2}$. Their variances can be shown to be

$$\Delta^2\hat{X}_- = \Delta^2\hat{P}_+ = e^{-2s}, \tag{2.26}$$

which beats the QNL of $\Delta^2\hat{X} = \Delta^2 P = 1$.

2.3 Gaussian states and Gaussian operations

The Gaussian state is a class of CV states where the first two moments are sufficient for complete characterisation [24]. The first moment, namely the mean value, is defined as

$$\bar{r} := \langle\hat{r}\rangle = \mathrm{Tr}(\hat{r}\hat{\rho}), \tag{2.27}$$

where $\hat{r} = (\hat{X}_1, \hat{P}_1, ..., \hat{X}_N, \hat{P}_N)$ for a N mode states, while the second moment, called the covariance matrix γ, is defined as

$$\gamma_{ij} := \frac{1}{2}\langle\{\Delta\hat{r}_i, \Delta\hat{r}_j\}\rangle. \tag{2.28}$$

For any physical covariance matrix, the HUP imposes a fundamental constraint,

$$\gamma + i\Omega \geq 0, \tag{2.29}$$

where $\Omega = \omega^{\oplus N}$, with $\omega = ((0,1),(-1,0))$. We summarise the Gaussian states described in Sec. 2.2 in the Table 2.3. These Gaussian states can be transformed by Gaussian unitaries by the following relations:

$$\bar{r} \to S\bar{r} + d, \qquad \gamma \to S\gamma S^\dagger. \tag{2.30}$$

Here, S is a sympletic transformation, i.e. $S\Omega S^\dagger = \Omega$ that preserves the Gaussianity of the state. A few useful transformations deployed throughout the thesis are summarized in Table 2.3. It is often useful to note that any single-mode Gaussian state can generally be expressed as $\gamma = (2\bar{n}+1)R(\theta)S(2s)R(\theta)^\dagger$.

Gaussian states	$\bar{r}$	γ
Vacuum state	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Coherent state	$\begin{pmatrix} x \\ p \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Thermal state	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 2\bar{n}+1 & 0 \\ 0 & 2\bar{n}+1 \end{pmatrix}$
Displaced squeezed state	$\begin{pmatrix} x \\ p \end{pmatrix}$	$\begin{pmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{pmatrix}$
Two-mode squeezed vacuum state	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} \cosh(2r)\cdot\mathbb{I} & \sinh(2r)\cdot\mathbb{I} \\ \sinh(2r)\cdot\mathbb{I} & \cosh(2r)\cdot\mathbb{I} \end{pmatrix}$

Table 2.1: The first and second moments of several commonly used Gaussian states.

Gaussian operations	
Displacement	$d(\alpha) = \begin{pmatrix} x \\ p \end{pmatrix}, \alpha = \frac{x+ip}{2}$
Squeezing	$S(s) := \begin{pmatrix} e^{-s} & 0 \\ 0 & e^{s} \end{pmatrix}$
Phase rotation	$R(\theta) := \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$
Beam splitting	$B(T) := \begin{pmatrix} \sqrt{T}\,\mathbb{I} & \sqrt{1-T}\,\mathbb{I} \\ -\sqrt{1-T}\,\mathbb{I} & \sqrt{T}\,\mathbb{I} \end{pmatrix}, \mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Two-mode squeezing	$S_2(s) := \begin{pmatrix} \cosh(s)\mathbb{I} & \sinh(s)\mathbb{Z} \\ \sinh(s)\mathbb{Z} & \cosh(s)\mathbb{I} \end{pmatrix}, \mathbb{Z}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Table 2.2: Several Gaussian operations utilised throughout the thesis. α is the displacement amplitude, s is the squeezing parameter, θ is the rotation angle, and T is the transmission ratio of a beam splitter.

2.4 Measuring the quantum state

We move on to introducing the theoretical description of how one measures a quantum state. In quantum mechanics, measurements are represented by a set of linear operators, denoted as $\{M_m\}$, acting upon the state space of the system under observation. The indices "m" denote the possible outcomes of the measurement process. Consider a particular state vector $|\psi\rangle$ that describes a quantum system before the observation, the probability of obtaining a particular result "m" from the measurement can be calculated with the following equation, known as the Born rule:

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle \,. \tag{2.31}$$

After the measurement has been performed, the system is now described by the post-measurement state instead, which is given by

$$|\psi'\rangle = \frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}. \tag{2.32}$$

Besides, the measurement operators should meet the completeness criterion as

$$\sum_m M_m^\dagger M_m = \mathbb{I}, \tag{2.33}$$

since this guarantees that for any state $|\psi\rangle$, the sum of all the probabilities is equal to one:

$$\sum_m p(m) = \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle = 1. \tag{2.34}$$

2.4.1 Positive operator-valued measure (POVM)

POVM operators form the most generalized description of quantum measurements. In particular, they are described by a set of POVM operators denoted by $\{E_m\}$. The probability of a particular measurement outcome m is given by

$$p(m) = \langle\psi| E_m |\psi\rangle. \tag{2.35}$$

Since $p(m)$ has to be non-negative for any state $|\psi\rangle$, it follows that $E_m \geq 0$, or in other words, E_m is a positive operator. Similarly to the completeness relation in Eq. (2.33), we also need $\sum_m E_m = \mathbb{I}$.

Looking back to the picture of having measurement operators $\{M_m\}_m$, we see that the POVMs corresponding to such a measurement scheme is given exactly by

$$E_m = M_m^\dagger M_m. \tag{2.36}$$

The complete set of POVM operators $\{E_m\}$ (without using measurement operators $\{M_m\}$) are already sufficient to evaluate the probability values $p(m)$. However, given a particular POVM $\{E_m\}$, it may correspond to many different sets of measurement operators, and this is why POVM operators do not provide sufficient information for one to reconstruct the post-measurement state.

2.4.2 Gaussian measurement

For a continuous variable systems, the measurement outcomes are no longer discrete, i.e. $m \in \mathbb{R}$, and the probability $p(m)$ in Eq. (2.35) is replaced by a probability density instead. In a continuous variable system, a Gaussian measurement is defined as a quantum measurement that produces Gaussian statistics upon measurement on the Gaussian states. The two most common Gaussian measurements in a CV experiments are the *homodyne* and *heterodyne* measurements.

From a theoretical perspective, a homodyne measurement projects a Gaussian state to an arbitrary quadrature $\hat{X}^{\theta}$. In other words, its measurement operators consists of projections $M(x^{\theta}) := |x^{\theta}\rangle\langle x^{\theta}|$ over the quadrature basis $|x^{\theta}\rangle$, i.e. the infinitely squeezed states along quadrature angle θ. When θ is 0 ($\pi/2$), the state is projected to the amplitude (phase) quadrature. Meanwhile, in a heterodyne measurement, the state is projected onto coherent states via the POVMs $M(\alpha) := \pi^{-1/2}\,|\alpha\rangle\langle\alpha|$. The experimental realisation of these measurements will be described in Sec 3.3.2.

2.5 Visualising the quantum state

While any quantum state can be adequately described by its density operator ρ, this representation does not provide an intuitive picture of states lying on an infinite dimensional Hilbert space. The phase space formulation of quantum optics, on the contrary, allows one to access features and properties of the quantum states without resorting to the notion of density matrices or Hilbert spaces. The mapping of operators in a Hilbert space to function in a complex phase space leads to an entire family of *quasi-probability distribution*. We now present three most commonly used representation: The Wigner representation, the Husimi Q representation and the Glauber-Sudarshan P representation, which are all linked by Gaussian convolution [25].

2.5.1 The Wigner representation

The representation of the Wigner function seems contradictory at first glance since it describes both the amplitude and phase information of the quantum state on equal footing. However, as dictated by HUP, simultaneous exact measurements of the amplitude and phase quadratures are impossible. This paradox is resolved once we realise that unlike classical statistical mechanics, a Wigner representation does not allow the construction of a joint probability distribution. Rather, negative values are permissible in this quasi-probability representation due to the non-commutativity of the quadratures. The projections, or the marginals of the Wigner function, nonetheless, describe the quadrature measurements of the quantum state, and always yield a positive definite probability distribution.

The Wigner distribution, or Wigner function, for the quantum state described by ρ is

$$W(x,p) = \frac{1}{\pi\hbar}\int_{-\infty}^{\infty} \mathrm{d}q\; \langle x-q|\hat{\rho}|x+q\rangle\, e^{ipq}, \tag{2.37}$$

where x and p are the eigenvalues of the quadrature eigenstates $|x\rangle$ and $|p\rangle$ respectively. We see that the Wigner function maps the density matrix to a real function in phase space. The key feature of the Wigner function is that the marginalised distribution across any quadratures will return the probability distribution of the corresponding measurement outcome:

$$P(x) = \int_{-\infty}^{\infty} \mathrm{d}p\, W(x,p) \ \text{ and } \ P(p) = \int_{-\infty}^{\infty} \mathrm{d}x\, W(x,p). \tag{2.38}$$

In practice, the corresponding Wigner function for a continuous variable quantum state can be constructed from homodyne measurement of $\hat{X}^{\theta}$ over multiple angles θ, together with the application of quantum tomography techniques such as inverse radon transformation or maximum entropy principle [25].

Several important features of the Wigner function are as follows: firstly, the trace of an operator $\hat{O}$ is the integral of its Wigner function

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \mathrm{d}x\, \mathrm{d}p\, W_O(x,p) = \mathrm{Tr}(\hat{O}). \tag{2.39}$$

This property also implies that Wigner function of a quantum state is normalised, since $\mathrm{Tr}(\rho) = 1$. Meanwhile, the trace between two Hermitian operators $\hat{O}_1, \hat{O}_2$ can be simply calculated by

$$\mathrm{Tr}\Big(\hat{O}_1\hat{O}_2\Big) = 4\pi \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \mathrm{d}x\, \mathrm{d}p\, W_{O_1}(x,p) W_{O_2}(x,p)\ . \tag{2.40}$$

This useful property allows us to directly calculate several important quantities, including expectation values of an operator, purity of the state and the transition probability between two pure states, without invoking the density matrix formalism.

In this thesis, we focus mostly on Gaussian quantum states, whose Wigner functions are positive everywhere and the marginals distribution are of a Gaussian form. As discussed in Sec. 2.3, these Gaussian states are fully characterized by the first and second moments of the amplitude and phase quadratures,

$$W_G(x,p) = \frac{1}{2\pi \Delta X \Delta P} \exp\bigg(\frac{(x - \langle X\rangle)^2}{2\Delta^2 X} + \frac{(p - \langle P\rangle)^2}{2\Delta^2 P}\bigg), \tag{2.41}$$

which corresponds to a two-dimensional Gaussian distribution with variances $\Delta^2 X$ and $\Delta^2 P$ displaced by $(\langle X\rangle, \langle P\rangle)$ in the phase space.

For non-Gaussian quantum states that have no classical counterpart, such as number states, the corresponding Wigner functions will exhibit negativity. Since negative probabilities have no classical explanation, the "negativity" of Wigner function often serves as a signature of non-classicality.

2.5.2 The Glauber-Sudarshan P function

Another widely used phase space distribution is the P representation, also known as the Glauber-Sudarshan P function [26, 27]. It is closely related to coherent states, and is famously expressed as the optical equivalence theorem

$$\hat{\rho} = \int \mathrm{d}^2\alpha \; P(\alpha) \, |\alpha\rangle\langle\alpha| \, , \tag{2.42}$$

where $P(\alpha)$ is the Glauber-Sudarshan P distribution corresponding to the quantum state $\hat{\rho}$. This equation shows that the density operator $\hat{\rho}$ of a quantum state can sometimes be written as a statistical mixture of coherent states. The thermal state, as mentioned in Eq. (2.23), is such an example. Interestingly, the P function for any coherent state $|\alpha_0\rangle$, is in fact a Dirac delta function $\delta^2(\alpha - \alpha_0)$, representing a single point in the phase space.

For quantum states that cannot be decomposed into coherent states, their P functions will exhibit negativity. This implies that even for states that have a positive Wigner function, such as squeezed states, the P function will be able to reveal its inherent quantumness. Upon first glance, such non-classical P functions can have a very strange behaviour, for example, they may contain derivatives of Dirac delta function, rendering them inaccessible experimentally. However, recent work [28] showed that it is possible to regularize the P function without compromising its sensitivity towards the non-classicality of its corresponding quantum state. This allows for the reconstruction of negative P quasi-probabilities via experimental techniques [29].

2.5.3 The Husimi Q representation

Unlike the previously introduced distributions, the Husimi Q function is a non-negative distribution,

$$Q(\alpha) = \frac{1}{\pi} \langle\alpha| \, \hat{\rho} \, |\alpha\rangle \geq 0, \tag{2.43}$$

since ρ is a positive operator. Consisting of the diagonal elements of the state ρ in the coherent state basis, it is bounded from above ($Q(\alpha) \leq 1/\pi$), and can be directly measured via a coherent state projection, or a dual-homodyne detection (see Sec. 2.4.2 and 3.3.2).

The Q function relates to the P function by taking the diagonal element of ρ in Eq. (2.42)

$$Q(\alpha) = \frac{1}{\pi} \int P(\beta) \exp\bigl(-|\alpha - \beta|^2\bigr) \mathrm{d}^2\beta. \tag{2.44}$$

This can also be interpreted as the Gaussian convolution of the P function. It follows that the Q function for a coherent state $|\alpha_0\rangle$ is

$$Q_{\alpha_0}(\alpha) = \frac{1}{\pi} \int \delta^2(\beta - \alpha_0) \exp\bigl(-|\alpha - \beta|^2\bigr) \mathrm{d}^2\beta = \frac{1}{\pi} \exp\bigl(-|\alpha - \alpha_0|^2\bigr), \tag{2.45}$$

which agrees with definition of Eq. (2.43) by having $\rho = |\alpha_0\rangle\langle\alpha_0|$.

2.6 From classical to quantum information theory

2.6.1 Classical entropy

Shannon entropy

With his seminal work published in 1948 [30], Claude Shannon laid down the cornerstone of information theory. In this work, he introduced the Shannon entropy as a uniquely well-behaved measure of *unpredictability*. This quantity, often denoted as $H(X)$, is assigned to a piece of information X, which mathematically can simply be viewed as a random variable associated with some probability distribution P_X. It is defined as

$$H(X) := -\sum_i P_X(x_i) \log_b P_X(x_i), \tag{2.46}$$

where $P_X(x_i)$[4] is the probability of obtaining outcome x_i, and b is the base of the logarithm[5]. Eq. (2.46) quantifies the *unevenness* of P_X.

Consider the elementary example of a fair die toss: there are six possible outcomes, each occurring with equal probability. For integers $i = \{1, 2, \cdots, 6\}$, let $X = i$ denote the event where the die toss outcome is i. If nothing else is known, the best we can do is make a guess at the outcome, and we will be correct with probability $\frac{1}{6}$ no matter what we guess. In other words, for all possible values of i, we have $P_X(i) = \frac{1}{6}$. The Shannon entropy is then given by $H(X) = -6 \cdot \frac{1}{6} \log_2 \frac{1}{6} = \log_2 6 \approx 2.58$.

Should the die be a biased one, certain outcomes would be more favourable. One may intuitively see that the *unevenness* of P_X increases, and indeed this is reflected by the Shannon entropy. Whenever the uncertainty is symmetrically distributed between all possible outcomes, the entropy of the system is uniquely maximal.

Joint entropy

Consider the case where we have multiple random variables, $\{X_i\} = X_1 \cdots X_k$, where the outcomes are associated with a joint probability distribution $P_{X_1 \cdots X_k}$. These variables may be inter-correlated: taking an extreme example, let $k = 2$, and X_2 to be an exact copy of X_1, hence $P_{X_1 X_2}(i, j) = \delta_{ij} P_{X_1}(x_i)$, where δ_{ij} is the Kronecker delta function. By treating $\{X_i\}$ as a single *joint random variable*, we may also write down its entropy

$$H(\{X_i\}) = -\sum_{x_1} \ldots \sum_{x_n} P_{\{X_i\}}(x_1, \ldots, x_k) \log_2 P_{\{X_i\}}(x_1, \ldots, x_k). \tag{2.47}$$

[4] To deal with probability values equal to zero, one also needs to specify that $0 \log 0 = 0$ is taken.

[5] Conventionally, $b = 2$ is used, to match the basic unit of information, i.e. a 2-outcome random variable called a bit. The Shannon entropy is also used in statistical physics, where $b = e$ is more often used.

Let us return to our example of X_2 being an exact copy of X_1, or in other words, X_1 and X_2 are completely correlated. In such a case, we see that

$$H(X_1, X_2) = -\sum_{x_1}\sum_{x_2} \delta_{x_1 x_2} P_{X_1}(x_1) \log_2 \delta_{x_1 x_2} P_{X_1}(x_1) \tag{2.48}$$

$$= -\sum_{x_1} P_{X_1}(x_1) \log_2 P_{X_1}(x_1) = H(X_1). \tag{2.49}$$

What is observed is that the random variable X_2 does not contribute further to increase the entropy, since all information contained in X_2 is obtained already from X_1. Therefore, the joint entropy reflects, to some degree, the amount of correlation between random variables, as we will see more explicitly later on. A useful inequality to note is that the joint entropy can be bounded below and above by a function of individual entropies, i.e. $\max(H(X_1), \ldots, H(X_k)) \leq H(\{X_i\}) \leq H(X_1) + \ldots + H(X_k)$.

Conditional entropy

Suppose we have 2 random variables X, Y, and the outcome of Y is revealed. The entropy of X, further conditioned on the outcome of Y (averaged over all possible outcomes y) is denoted as the *conditional entropy*:

$$H(X|Y) := -\sum_{y} P_Y(y) \sum_{x} P_{X|Y}(x|y) \log_2 P_{X|Y}(x|y) \tag{2.50}$$

$$= \sum_{y} P_Y(y) H(X|y). \tag{2.51}$$

Here $H(X|y) = -\sum_x P_{X|Y}(x|y) \log_2 P_{X|Y}(x|y)$ is the entropy of X conditioned upon a particular outcome y. Again, we look at the example where Y is an exact copy of X. Upon knowing X, we also immediately gain full knowledge of Y, hence $H(Y|X) = 0$. Similarly, $H(X|Y) = 0$, although the conditional entropy is not symmetric in general. More interestingly, one may readily derive its relation with the joint entropy:

$$H(X, Y) \equiv H(Y) + H(X|Y) \equiv H(X) + H(Y|X). \tag{2.52}$$

For classical random variables, the conditional entropy, like any other entropy, is non-negative.

Mutual information

To quantify the amount of shared information existing between two random variables, one defines the mutual information

$$I(X\!:\!Y) := H(X) + H(Y) - H(X, Y). \tag{2.53}$$

It is easy to see that this quantity is symmetric, i.e. $I(X:Y) = I(Y:X)$. Using Eq. (2.52), we may also understand the mutual information in a different light:

$$I(X:Y) = H(X) - H(X|Y) = H(Y) - H(Y|X). \tag{2.54}$$

This also implies that for classical random variables, the mutual information is always bounded by the individual entropies, i.e. $I(X:Y) \leq \min(H(X), H(Y))$. Intuitively one may understand this as saying that the amount of information shared between X and Y cannot exceed the amount of information containable in the individual variables.

2.6.2 Quantum entropies

Until now we have introduced several entropic quantities in the framework of classical information theory. In quantum information theory, these quantities were extended from random variables to describe quantum states. The von Neumann entropy is the quantum counterpart of the Shannon entropy, which is defined with respect to a quantum system A described by density operator ρ_A,

$$S(A) = S(\rho_A) := -\mathrm{tr}(\rho \log_2 \rho) = -\sum_i \lambda_i \log_2 \lambda_i, \tag{2.55}$$

where λ_i are the eigenvalues of ρ_A. Since a density operator is a positive semi-definite matrix with trace equal to 1, its eigenvalues $\{\lambda_i\}$ form a normalised probability distribution, and hence the von Neumann entropy inherits all properties of the Shannon entropy. For example, $S(\rho_A) = 0$ if and only if $\rho_A = |\psi\rangle\langle\psi|_A$ is pure. On the other hand, if the dimension of the system is given by $\dim(A) = d_A$, then $S(\frac{\mathrm{id}}{d_A}) = \log d_A$, where the density operator $\frac{\mathrm{id}}{d_A}$ is also known as the maximally mixed state.

Given a bipartite system ρ_{AB}, the joint entropy is simply $S(AB) = S(\rho_{AB}) = -\mathrm{tr}(\rho_{AB} \log_2 \rho_{AB})$. However, to evaluate the individual entropies, one has to first compute the *reduced states* on A and B: $\rho_A = \mathrm{tr}_B(\rho_{AB})$, and likewise $\rho_B = \mathrm{tr}_A(\rho_{AB})$. The entropy of the reduced subsystems is then given by $S(\rho_A)$ and $S(\rho_B)$. The von Neumann entropy satisfies

$$S(AB) \leq S(A) + S(B), \tag{2.56}$$

with equality only when A and B are completely uncorrelated, i.e. $\rho_{AB} = \rho_A \otimes \rho_B$ is of tensor product form.

One may also consider quantum versions of the conditional entropy

$$S(\rho_A|\rho_B) \equiv S(\rho_{AB}) - S(\rho_B), \tag{2.57}$$

and mutual information

$$\mathcal{I}(\rho_{AB}) = S(\rho_A) + S(\rho_B) - S(\rho_{AB}) \tag{2.58}$$

$$= S(\rho_A) - S(\rho_A|\rho_B) \tag{2.59}$$

$$= S(\rho_B) - S(\rho_B|\rho_A). \tag{2.60}$$

Despite having similar forms as the classical version, these quantities behaves differently from them, and this is a result of strong quantum correlations between systems. Consider, for instance, a pure two-mode squeezed state (Sec. 2.2.6). While the entropy of the joint system is zero, the individual subsystems are simply locally thermal states with a large amount of entropy, and therefore according to Eq. (2.57), $S(\rho_A|\rho_B) < 0$! In other words, this means sometimes we can be more certain about the joint system when compared to the individual systems. [6]

Lastly, we note a very useful inequality given by the Holevo's bound [31], which is one of the landmark results in quantum information. It gives the maximum possible amount of information that can be known upon measuring a quantum state. Its significance is best illustrated by considering a following state-discrimination problem between two parties, Alice (A) and Bob (B). Alice has a classical random variable X from which she draws values x with a probability p_x. Based on her outcome x, Alice prepares a quantum state ρ_x which she transmits to Bob. The density matrix describing this piece of quantum information is given by the mixture

$$\rho = \sum_x p_x \rho_x. \tag{2.61}$$

Upon receiving ρ, Bob's goal is to determine which state ρ_x was transmitted in the first place, or in other words, guess the outcome x. To do this, he performs a measurement on ρ, obtaining a classical outcome denoted by a random variable Y. Holevo's bound says that the mutual information between X and Y is given by:

$$I(X\!:\!Y) \leq S(\rho) - \sum_x p_x S(\rho_x). \tag{2.62}$$

2.7 CV quantum information

For the transmission of information using a continuous quantum source, a continuous version of the Shannon entropy has to be considered. For a continuous variable X with probability density $p_X(x)$, it is defined as [32]

$$h(X) = -\int p_X(x) \log_2 p_X(x) \mathrm{d}x \tag{2.63}$$

[6] We also note an alternate measurement-based definition of the conditional entropy, as describe in C.2.1. Such a definition actually leads to a mismatch between Eq. (2.58) and Eqs. (2.59) and (2.60), known as quantum discord.

This definition, which is also known by the name of differential entropy, is maximized by a normal distribution with a given variance. Let us now consider a case where a sender (Alice) is transmitting information to a receiver (Bob) by encoding her data onto the quadrature of a CV quantum state with variance $\Delta^2\hat{X}_N$. Alice's data is a random number $\mathcal{S}$ drawn from Gaussian distributions with zero mean and a variance of $\Delta^2\mathcal{S}_A$. This forms an additive white Gaussian noise (AWGN) channel, allowing the signal that Bob receives in a lossless channel to be written as $\hat{X}_B = \mathcal{S}_A + \hat{X}_N$ in terms of quadrature. Since both the signal and the noise are from independent normal distributions, $\hat{X}_B$ has a variance of $\Delta^2\hat{X}_B = \Delta^2\mathcal{S}_A + \Delta^2\hat{X}_N$. Given the fact that a Gaussian signal maximises the differential entropy for a given variance, the differential entropies for Alice and Bob can be expressed as

$$h(A) = \frac{1}{2}\log_2\left(2\pi e\Delta^2\mathcal{S}_A\right), \tag{2.64}$$

$$h(B) = \frac{1}{2}\log_2\Big(2\pi e(\Delta^2\mathcal{S}_A + \Delta^2\hat{X}_N)\Big). \tag{2.65}$$

where e is the exponential constant, and the Shannon entropy is in units of bits/symbol. The information transmission rate between Alice and Bob through the quantum channel is given by Alice's mutual information with Bob:

$$\begin{aligned} I(A{:}B) &= h(B) - h(B|A) && (2.66)\\ &= h(B) - h(N) && (2.67)\\ &= \frac{1}{2}\log_2\left(1 + \frac{\Delta^2\mathcal{S}_A}{\Delta^2\hat{X}_N}\right), && (2.68)\end{aligned}$$

Here, we have used the fact that $h(B|A) = h(A+N|A) = h(A)$ since the encoding signal is independent from the quantum noise. Hence, by encoding Gaussian signals on the quadrature of the light field, Alice and Bob can transmit information at the Shannon capacity of a continuous quantum channel, where the information capacity is dependent on the ratio between the variance of the Gaussian signal $\Delta^2\mathcal{S}_A$ and the variance of the quantum noise $\Delta^2\hat{X}_N$.

Chapter 3

Experimental Techniques & Models

"You cannot go on 'seeing through' things for ever. The whole point of seeing through something is to see something through it."

– C.S. Lewis, *The Abolition of Man*

Overview

In this chapter, we briefly discuss the necessary experimental techniques and methods to perform and model the experiments conducted in this thesis. By extending discrete mode of light to continuous representation, we described the encoding of information in the quantum sidebands. We also introduce several elementary components of a typical CV experiment, including the laser system, a beam splitter, and electro-optical modulators. Quantum measurements (direct, homodyne and heterodyne) are discussed in continuous mode description. Finally, we explained how the digital locking and sampling is done in a CV quantum experiment. We refer our reader to the PhD thesis of ANU Quantum Optics group for more details, in particularly the thesis of Lam [33] and Bowen [34].

3.1 From discrete to continuous mode

In the last chapter, we introduced the quantization formulation, which is motivated by the scenario of having an electromagnetic field confined within a hypothetical cavity with a finite length L. Each quantized mode is identified as eigenmodes separated by frequency $\Delta\omega = 2\pi c/L$. While some experiments do assume a real cavity or confined space, in most cases, quantum opticians deal more often with travelling light. Most typically, light is emitted from a source, and passes through certain kinds of interaction regions such as those induced by optical elements, and finally arriving at detectors. For such situations, it is thus desirable to consider the quantisation of freely propagating electromagnetic waves with eigenmodes characterized by a continuous wave vector. As the length of the quantisation cavity L tends to infinity, the mode spacing $\Delta\omega$ tends to zero, while the sums we see over discrete wave numbers in Eq. (2.1) become integrals over continuous frequencies [35]

$$\sum_k \rightarrow \frac{1}{\Delta\omega}\int \mathrm{d}\omega. \tag{3.1}$$

The continuous mode operators transform from their discrete mode counterparts by

$$\hat{a}_k \rightarrow \sqrt{\Delta\omega}\,\hat{a}(\omega) \text{ and } \hat{a}_k^\dagger \rightarrow \sqrt{\Delta\omega}\,\hat{a}^\dagger(\omega). \tag{3.2}$$

Similarly, the discrete Kronecker and the continuous Dirac delta function are related by $\delta_{k,k'} \rightarrow \Delta\omega\,\delta(\omega-\omega')$, which leads to the continuous-mode commutation relation,

$$\left[\hat{a}(\omega),\hat{a}^\dagger(\omega')\right] = \delta(\omega-\omega'). \tag{3.3}$$

The integration of Eq. (3.1) is strictly from 0 to ∞. However, for most experiments, since the frequency bandwidth is much smaller than the central frequency, we can extend the lower limit of integration to $-\infty$ without significant error. This allows us to write the Fourier-transformed operators as

$$\hat{a}(t) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} \mathrm{d}\omega\,\hat{a}(\omega)\exp\{(-i\omega t)\} \tag{3.4}$$

$$\hat{a}^\dagger(t) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} \mathrm{d}\omega\,\hat{a}^\dagger(\omega)\exp\{(i\omega t)\}, \tag{3.5}$$

with the definition $\hat{a}^\dagger(t) = [\hat{a}(t)]^\dagger$. It can be shown that $[\hat{a}(-\omega)]^\dagger = \hat{a}^\dagger(\omega)$ through inverse Fourier transform. The amplitude and phase quadrature operators in frequency domain are thus given by

$$\hat{X}(\omega) = \hat{a}(\omega) + \hat{a}^\dagger(\omega) = \hat{a}(\omega) + [\hat{a}(-\omega)]^\dagger \tag{3.6}$$

$$\hat{P}(\omega) = i\left(\hat{a}^\dagger(\omega) - \hat{a}(\omega)\right) = i\left([\hat{a}(-\omega)]^\dagger - \hat{a}(\omega)\right). \tag{3.7}$$

In the rotating frame of the carrier frequency ω_0, these expressions can be interpreted as the positive and negative sidebands of ω centred around ω_0.

3.1.1 Sidebands and modulation of light

In the sideband picture, the quantum noise can be treated as beating with the carrier mode at all frequencies. These sidebands are due to non-zero ground state energy of the vacuum state. All modes are uncorrelated, and hence appear as a random fluctuation of amplitude and phase along the positive and negative frequency axis (Fig. 3.1 (a)).

An amplitude modulation is a direct modulation of the light intensity at certain modulation frequency, ω. The upper and the lower sidebands are correlated with each other at all time (Fig. 3.1 (b)). Assuming a small modulation depth $\zeta \ll 1$, the positive part of

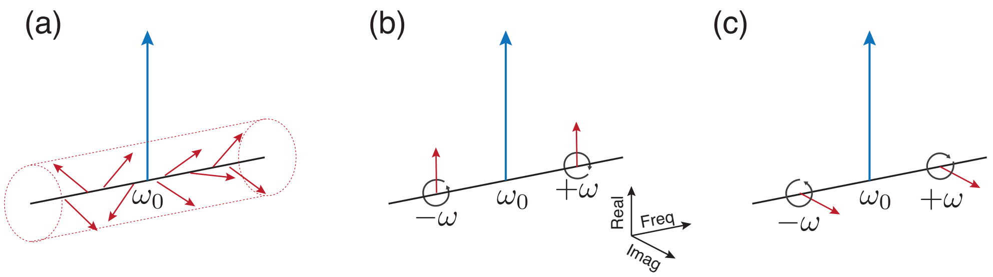


Figure 3.1: Sideband picture for (a) a vacuum state. (b) A phase-modulated coherent state and (c) an amplitude-modulated coherent state around the carrier frequency ω_0, with sidebands at $\pm\omega$.

the quantized field reads as

$$\hat{a}_{\text{AM}}(t) = \hat{a}_0(t)(1 + \zeta\cos(\omega t)) = \hat{a}_0(t)\left[1 + \frac{\zeta}{2}(e^{i\omega t} + e^{-i\omega t})\right]. \tag{3.8}$$

It can be seen that modulation ζ distributes the energy from the carrier to the two generated sideband modes. Changing our frame to frequency domain gives

$$\hat{a}_{\text{AM}}(\omega_0) = \hat{a}_0(\omega_0) + \frac{\zeta}{2}\left[\hat{a}(\omega_0 + \omega) + \hat{a}(\omega_0 - \omega)\right], \tag{3.9}$$

and from this we observe that the field is modulated at sidebands $\omega_0 \pm \omega$, with a real amplitude of depth ζ.

The phase modulation, on the other hand, modifies the phase component of the field,

$$\hat{a}(t) = \hat{a}_0(t)\, e^{i\zeta\cos\omega t}. \tag{3.10}$$

Again, for $\zeta \ll 1$, the first order expansion gives

$$\begin{aligned}\hat{a}(t) &= \hat{a}_0(t)(1 + i\zeta\cos\omega t)\\ &= \hat{a}_0(t)\left[1 + \frac{i\zeta}{2}(e^{i\omega t} + e^{-i\omega t})\right].\end{aligned} \tag{3.11}$$

Repeating similar steps as before, the annihilation operators in frequency domain are

$$\hat{a}_{\text{PM}}(\omega_0) = \hat{a}_0(\omega_0) + \frac{i\zeta}{2}\left[\hat{a}(\omega_0 + \omega) + \hat{a}(\omega_0 - \omega)\right]. \tag{3.12}$$

Comparing Eq. (3.12) and (3.9), we note that the phase modulation modifies the imaginary component of the field (Fig. 3.1 (c)). Together with the amplitude modulation, the vacuum state at the sidebands can be excited to arbitrary amplitude and phase.

In continuous variable systems, information can often be encoded onto the quantum state by modulating the sidebands of the carrier light. A typical scenario is the generation of coherent states via the amplitude and phase modulation.

3.1.2 Linearised decomposition of the operators

Most quantum optics experiments operate in the regime where the fluctuations of the field are negligible when compared to the average intensity of the field. In this case, good approximation of the experiment can be obtained in analytical form via the linearization of the operators. The essence of linearization is to expand an operator $\hat{O}$ around its steady state value, and keep only the first order fluctuating terms. Applying the linearization procedure over the creation and annihilation operator gives

$$\hat{a}(t) = \alpha + \delta\hat{a}(t) \text{ and } \hat{a}^\dagger(t) = \alpha^* + \delta\hat{a}^\dagger(t). \tag{3.13}$$

where $\langle \hat{a} \rangle = \alpha$ and $\langle \hat{a}^* \rangle = \alpha^*$. The operators have been decomposed into a steady state time-independent term, plus a contribution from the fluctuation throughout the spectrum in the frequency picture. To this end, it has been assumed that

$$\langle \delta\hat{a}(t) \rangle = \langle \delta\hat{a}^\dagger(t) \rangle = 0 \;\text{ and }\; |\delta\hat{a}(t)| \ll \alpha. \tag{3.14}$$

That is, the fluctuation term, which has zero mean, is much smaller compared to the steady-state amplitude α. This allows us to simplify the expression by neglecting higher order product terms of the quantum fluctuations. For example, under linearisation, the quadrature variance can be written as

$$\Delta^2\hat{X}(t) = \langle (\delta\hat{a}^\dagger(t) + \delta\hat{a}(t))^2 \rangle = \langle (\delta\hat{X}(t))^2 \rangle \,, \tag{3.15}$$

$$\Delta^2\hat{P}(t) = \langle (i(\delta\hat{a}^\dagger(t) - \delta\hat{a}(t)))^2 \rangle = \langle (\delta\hat{P}(t))^2 \rangle \,. \tag{3.16}$$

3.2 Experimental system

3.2.1 Laser system

Apart from Chapter 5, the laser source for the experiments throughout the thesis is an *Innolight Diabolo* ND:Yag continuous wave laser at 1064nm. It is also capable of producing 532nm light via an internal frequency doubler. The natural relaxation oscillation of the laser, which induces intensity fluctuations, can be suppressed by 30 dB with an internal noise eater option.

Immediately after the laser system is a Faraday isolator, which prevents optical damage due to unintended backscattering of light from the experimental optics. In order to stabilise the laser frequency and to generate a well-defined, single TEM-00 spatial mode for the experiment, the laser is passed through and locked to the resonant frequency of a high finesse optical cavity, or *mode cleaner* (MC). Our mode cleaner is a 3-mirror triangular ring resonator, featuring a piezoelectric transducer actuated end mirror. It has an optical path length of 800mm and linewidth of 0.4 MHz. The MC also further suppresses laser intensity fluctuations at a low frequency regime, thus providing a shot

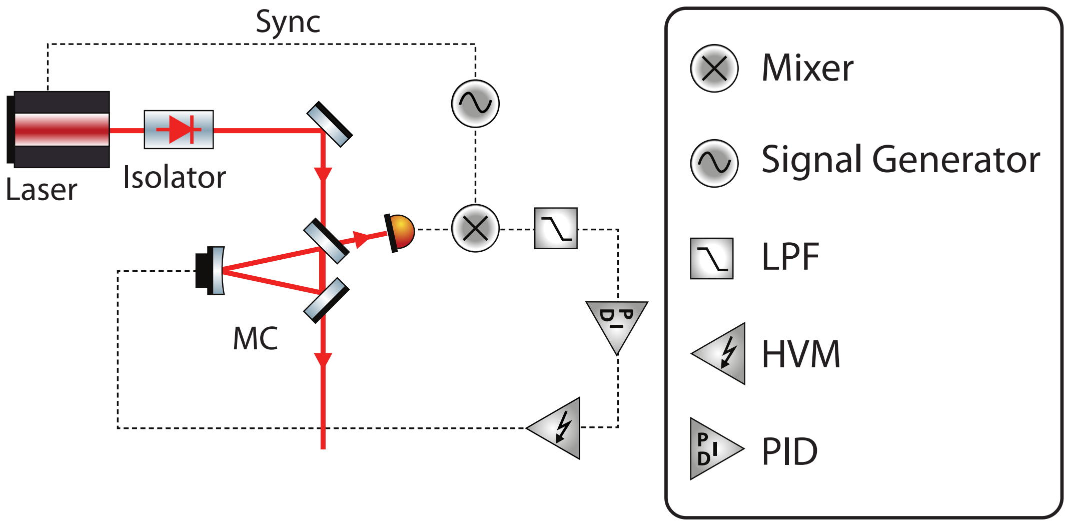


Figure 3.2: The schematic diagram of a PID controlled laser system. MC: mode cleaner, LPF: low-pass filter, HV: high voltage amplifier. PID: Proportional-Integral-Derivative.

noise limited laser field with a frequency above 4 MHz.

To control the MC, we use Pound-Drever-Hall (PDH) technique [36], which utilises phase modulation to determine the locking point. First, the phase modulation is obtained directly from the internal phase modulation of the laser unit for frequency doubling. Sidebands at a frequency of 40 MHz are used, which is well above the cavity linewidth (0.4 MHz). After an analog demodulation with a synced signal generator, an error signal is obtained. This error signal is then fed into a digital PID (Proportional-Integral-Derivative) controller, which is implemented using software written in *National Instruments LabView* developed by Ben Sparks and Thomas Symul. More details on this control can be found in [37]. Finally, the cavity length is kept in resonance with the optical field according to the amplified feedback signal. A schematic of the laser system is depicted in Fig. 3.2.

3.2.2 Beam splitter

A beam splitter (BS), as naive as it may seem, plays an indispensable role in day-to-day quantum optics lab. As an elementary linear optical element, this 4-port BS mixes two input modes $\hat{a}$ and $\hat{b}$ with identical frequency, polarization and spatial profile. Assuming a beam splitter with transmissivity η, the transmitted and the reflected modes of the BS, denoted by $\hat{c}$ and $\hat{d}$, are given by

$$\begin{aligned}\hat{c} &= \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{b},\\ \hat{d} &= \sqrt{1-\eta}\hat{a} - \sqrt{\eta}\hat{b}.\end{aligned} \tag{3.17}$$

A π phase shift is required between the output modes to honour the energy conservation rule. When mode $\hat{b}$ takes the role of an empty mode, it becomes an effective tool to model many linear processes, such as optical attenuation, imperfection in photodetection and mismatch in spatial mode. They can be modelled as an 100% effective process coupled to a vacuum mode by a BS. The transmittivity parameter of the BS then governs the efficiency of the concerned process. For example, let us consider the amplitude quadrature of the transmitted field with the input $\hat{X}_{\text{in}}$ coupled to the vacuum $\hat{X}_{\text{v}}$:

$$\hat{X}_{\text{out}} = \sqrt{\eta}\hat{X}_{\text{in}} + \sqrt{1-\eta}\hat{X}_{\text{v}}. \tag{3.18}$$

The mean and the variance of $\hat{X}_{\text{out}}$ are given by

$$\langle \hat{X}_{\text{out}} \rangle = \sqrt{\eta}\,\langle \hat{X}_{\text{in}} \rangle\,, \tag{3.19}$$

$$\Delta^2 \hat{X}_{\text{out}} = \langle \delta \hat{X}^2_{\text{out}} \rangle = \eta\,\langle \delta \hat{X}^2_{\text{in}} \rangle + 1 - \eta, \tag{3.20}$$

where we have invoked $\langle \hat{X}_{\text{v}} \rangle = 0$ and $\langle \delta \hat{X}^2_{\text{v}} = 1 \rangle$. Under linear loss, the mean is reduced by a factor of $\sqrt{\eta}$. Meanwhile, depending on the magnitude of $\langle \delta \hat{X}^2_{\text{in}} \rangle$, lossy detection can either underestimate ($\langle \delta \hat{X}^2_{\text{in}} \rangle > 1$) or overestimate ($\langle \delta \hat{X}^2_{\text{in}} \rangle < 1$) the input variance. If the input is a coherent state ($\langle \delta \hat{X}^2_{\text{in}} \rangle = 1$), the variance remains unaffected. Therefore, in order to ensure accurate inference of the input's variance, it is important to take into account losses in the detection process.

In a discrete variable picture, the balanced beam splitter is treated as a fair die, distributing quantized photons to either port with 50% probability. As we have seen, in a continuous variable picture, such a random process is due to vacuum fluctuations coupled to the unused port of the beam splitter. These pictures allow us to utilize a BS as the building block of an optical source of entropy.

3.2.3 Electro-optical modulation

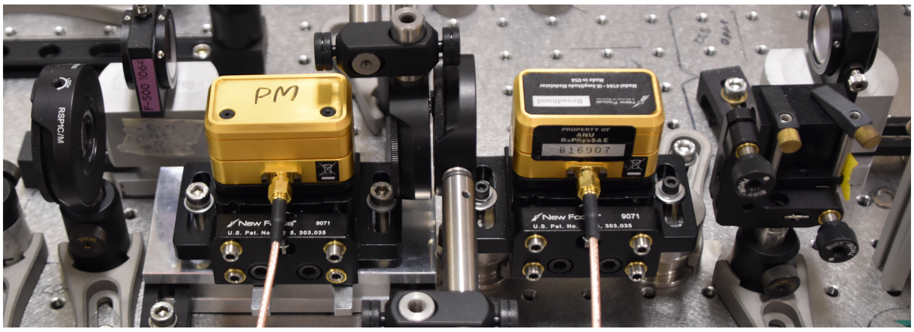


Figure 3.3: The electro-optical modulators. The phase modulator (PM) is followed by the amplitude modulator (AM), where the waveplates in between changes the light from linearly polarised light to circularly polarised light before entering the AM.

The sideband modulations discussed in Sec. 3.1.1 are usually achieved in the lab through the electro-optical effect (Fig. 3.3). By sinusoidally changing the electric field applied across crystals such as lithium niobate, the refractive index along a particular optical axis can be modulated. This in turn modifies the optical path length, and hence the phase of the exiting field.

To achieve amplitude modulation, the field first has to be prepared as circularly polarized light. The beam is then passed through a birefringent electro-optical crystal, where only the polarized component at the slow axis of the crystal is modulated. The output field, which is now modulated in polarization, is fed into a series of polarising optics, consisting of Glan-Thompson prism and polarising BS to select only the fast axis component of the light. This results in a purely amplitude modulated light.

Several precautions have to be taken in order to ensure proper sidebands modulation. First, to ensure high quality mode matching at the detection stage, the modulators have to be aligned carefully to prevent clipping and distortion of light. Secondly, to minimize cross-quadrature modulation, i.e. unwanted amplitude modulation from phase modulator and vice versa, the crystal axis and the beam polarization have to be matched as closely as possible.

3.3 Quantum measurements

3.3.1 Direct detection

A direct measurement of light can be done with a photodiode, which converts photons into electrons. The detection efficiency is thus given by the ratio of electrons and photons, $\eta_{\mathrm{Det}} = N_{\mathrm{e}}/N_{\mathrm{ph}}$. This measurement probes the intensity of the light, i.e. $\hat{a}^\dagger \hat{a}$. After an internal gain, the output photocurrent, $i(t)$, which is proportional to the number of photons in the optical field, is given by

$$i(t) \propto \hat{a}^\dagger(t)\, \hat{a}(t) \approx\; |\alpha|^2 + \alpha\, \delta\hat{X}^+(t). \tag{3.21}$$

Here, we have performed linearization (Eq. (3.14)) and assumed α to be real. Rewriting this expression in Fourier representation,

$$i(\omega) \propto \hat{a}^\dagger(\omega)\, \hat{a}(\omega) \approx\; |\alpha|^2\delta(0) + \alpha\, \delta\hat{X}(\omega). \tag{3.22}$$

We note that this expression consists of a DC term linked to the optical intensity, and an RF fluctuating amplitude quadrature amplified by the DC field amplitude.

3.3.2 Homodyne and heterodyne detections

In order to interrogate the phase information of the quadrature, it is necessary to introduce a phase reference. By interfering two optical fields (signal and probe) differing by phase θ with a balanced BS, an arbitrary quadrature amplitude $\hat{X}^\theta$ can be extracted from the difference of the photocurrents from the two BS output ports (Fig. 3.4(a)). This technique, which allows the suppression of probe noise during measurement, was termed

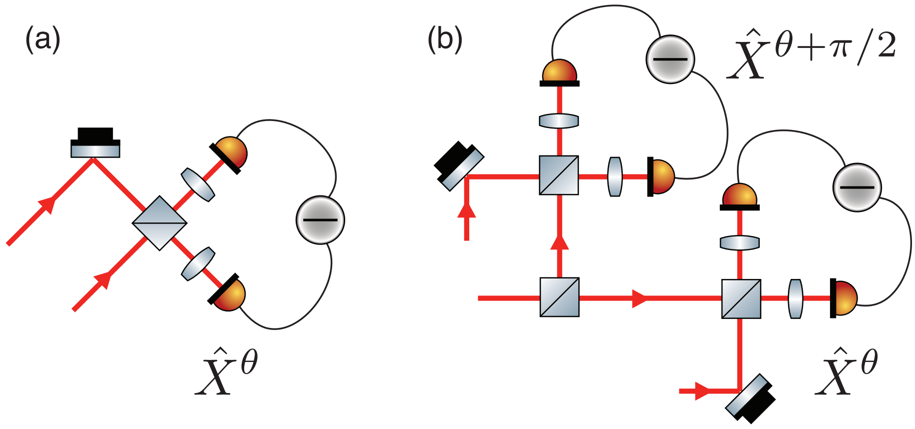


Figure 3.4: Schematic of CV quantum measurements. (a) Balanced homodyne detection. The difference current is proportional to the quadrature observable of $\hat{X}_\theta$. (b) Dual-homodyne or heterodyne detection, where two conjugate quadratures $\hat{X}_\theta$ and $\hat{X}_{\theta+\pi/2}$ of the input beam are probed by dividing the signal strength by half.

as an two-port optical homodyne detection [38].

Let us consider two optical fields, signal $\hat{a}$ and probe $\hat{b}$ interfering on a $50:50$ beam splitter ($\eta = 0.5$). Following Eq. 3.17, the photon numbers $\hat{n}_c$ and $\hat{n}_d$ at the output ports are given by

$$\begin{aligned} i_c \propto \hat{n}_c = \hat{c}^\dagger \hat{c} &= \frac{1}{2}(\hat{a}^\dagger \hat{a} + \hat{b}^\dagger \hat{b} + \hat{a}^\dagger \hat{b} + \hat{a}\hat{b}^\dagger), \\ i_d \propto \hat{n}_d = \hat{d}^\dagger \hat{d} &= \frac{1}{2}(\hat{a}^\dagger \hat{a} + \hat{b}^\dagger \hat{b} - \hat{a}^\dagger \hat{b} - \hat{a}\hat{b}^\dagger). \end{aligned} \tag{3.23}$$

The photocurrent difference, i^- is proportional to the difference between the photon numbers,

$$\begin{aligned} i^- &\propto \hat{n}_c - \hat{n}_d \\ &= \hat{a}^\dagger \hat{b} + \hat{a}\hat{b}^\dagger. \end{aligned} \tag{3.24}$$

Depending on the presence of a linearized input mode $\hat{a} = \alpha + \delta\hat{a}$, we may consider different cases as detailed below. [1]

Self homodyne detection

In the absence of the input signal at mode a, i.e. only vacuum fluctuations are present, $\hat{a} = \delta v$. The difference in the current i_- becomes

$$\begin{aligned} i^-_{\mathrm{v}} &\propto (\beta + \delta\hat{b}^\dagger)\delta v + (\beta + \delta\hat{b})\delta v^\dagger \\ &= \beta(\delta v + \delta v^\dagger) = \beta\delta\hat{X}_{\mathrm{v}}. \end{aligned} \tag{3.25}$$

[1] Without loss of generality, we assume the steady state amplitudes to be real.

We see that this measurement reveals the amplitude quadrature of the vacuum field, magnified by a factor of α. The variance of this current is $\Delta^2 i_{\mathrm{v}}^- \propto \beta^2$, since $\langle \delta \hat{X}_{\mathrm{v}}^2 \rangle = \Delta^2 \hat{X}_v = 1$. This is also the measured variance of the Gaussian probability distribution associated with the amplitude quadrature of the vacuum state.

Balanced homodyne detection

When the signal field is not blocked, we have $\hat{a} = \alpha + \delta\hat{a}$. We now require the probe beam b to be an intense coherent beam ($\beta \gg \alpha$). This beam, termed as a *local oscillator*, has a phase difference of θ relative to the signal field, i.e. $\hat{b} = \beta e^{i\theta}$. This angle θ can be controlled by adjusting the path difference between the beams with a piezoelectric transducer mirror. Subtracting the photocurrents from the signal and the probe gives

$$i^- \propto 2\alpha\beta\cos\theta + \beta\delta\hat{X}^\theta. \tag{3.26}$$

Here, we have $\delta\hat{X}^\theta = \delta a^\dagger e^{i\theta} + \delta a e^{-i\theta}$. Setting the phase to 0 and $\pi/2$ allows us to sample the amplitude ($\hat{X}$) and phase ($\hat{P}$) quadrature of the input signal respectively. By diving the variance of the signal's photocurrent, $\Delta^2 i^- \propto \beta^2 \Delta^2 \hat{X}^\theta$, with that of vacuum's, we get the quadrature amplitude normalized to the quantum noise limit,

$$\frac{\Delta^2 i^-}{\Delta^2 i_{\mathrm{v}}^-} = \Delta^2 \hat{X}^\theta. \tag{3.27}$$

We thus see that cancellation of classical steady state amplitude grants us the access to intricate quantum features, such as the vacuum fluctuation. By simply blocking and unblocking the signal, measurement normalised to the quantum noise can be achieved. In practise, however, the beam splitter might not be perfectly balanced, and the detectors might have different electronic gain as well. These imperfections can be mitigated by means of electronic attenuation of photocurrent in one port. Meanwhile, the homodyne detection efficiency, η_{HD} is equal to the product of the detector efficiency and the mode-matching efficiency: $\eta_{\mathrm{HD}} = \eta_{\mathrm{Det}} \times \eta_{\mathrm{vis}}$. When the steady state amplitudes of the inputs are equal, the mode-matching efficiency is related to the visibility as [39]

$$\eta_{\mathrm{vis}} = \mathrm{VIS}^2 = \left(\frac{i_{\mathrm{max}} - i_{\mathrm{min}}}{i_{\mathrm{max}} + i_{\mathrm{min}}} \right)^2. \tag{3.28}$$

Through careful design of the experimental optical path lengths and lens arrangements, together with the help of beam steering mirrors and polarising optics, typically we can achieve mode-matching efficiencies up to 99%.

Heterodyne detection

While it is impossible to precisely determine the amplitude and phase of a quantum state, as dictated by the Heisenberg's uncertainty principle, simultaneously measuring the conjugate quadrature of the light field is not forbidden by the laws of quantum physics, as we will now demonstrate below [40].

Here, we consider an attempt to simultaneously measure the conjugate quadrature amplitudes of our input signal with homodyne detections. We split the input mode $\hat{a}_{\text{in}}$ into modes $\hat{a}_1$ and $\hat{a}_2$, followed by two homodyne detections sampling the orthogonal quadratures $\hat{X}^{\theta}$ and $\hat{X}^{\theta+\pi/2}$. The modes after splitting are given by

$$\begin{aligned}\hat{a}_1 &= \frac{1}{\sqrt{2}}(\hat{a}_{\text{in}} + \hat{v}),\\ \hat{a}_2 &= \frac{1}{\sqrt{2}}(\hat{a}_{\text{in}} - \hat{v}).\end{aligned} \tag{3.29}$$

Strictly speaking, we are actually probing two different modes $\hat{a}_1$ and $\hat{a}_2$. Hence, there is no compatibility issue with the HUP. Repeating similar calculations as before in Eq. 3.26, the variances of the homodyne detections normalised to the vacuum are

$$\begin{aligned}\frac{\Delta^2 i_1^-}{\Delta^2 i_{\text{v}}^-} &\propto \frac{1}{2}(\Delta^2\hat{X}^{\theta} + \Delta^2\hat{X}_v),\\ \frac{\Delta^2 i_2^-}{\Delta^2 i_{\text{v}}^-} &\propto \frac{1}{2}(\Delta^2\hat{X}^{\theta+\pi/2} + \Delta^2\hat{X}_v).\end{aligned} \tag{3.30}$$

We see that our information regarding the quantum state is *contaminated* by the shot noise coupled in through the first beam splitter, which is akin to the case of a lossy detection in Eq. (3.20) with $\eta = 0.5$. This detection, though noisy, turns out to be a projection on coherent state basis, thus allowing the reconstruction of Husimi Q distribution.

3.4 Interefometric locking and control

A typical routine in a quantum optics lab is the locking of pairs of optical fields. This is usually done by interfering two beams via a beam splitter. As discussed in Sec. 3.3.2, we can choose to measure either the amplitude or the phase quadrature of the input signal by locking the phase difference between the interfering fields. This can be done via PDH technique, which relies upon sidebands modulation to generate the error signal for locking.

In this thesis, the experiments that require locking are controlled digitally by field programmable gate arrays (FPGA) system. A digital control system offers the capacity to integrate the control loops and the data acquisition together. The National Instrument LabView codes deployed in these systems were developed previously in our group by Sparkes et al. [37], and further modified by Dr. Syed Assad.

In order to lock the homodyne station to the desired quadrature, sinusoidal signals at two distinct frequencies are applied on the phase and amplitude modulators respectively. In order to ensure a clear detection band, analog or manual switching of the band pass filters is used prior to digital demodulation of the error signal. Finally, the demodulated signal is fed into a digital PII (proportional-double integral) controller. This approach thus allows us to easily switch between the quadratures without requiring any changes to the electronic hardware. More details on other types of locking techniques, such as offset locking can be found in [34].

3.5 Optical quantum state measurements

A spectrum analyzer (SA) allows us to measure the power spectrum of the a signal in the frequency domain. In conjunction with a homodyne detector, SA measures the fluctuations of the optical field with some bandwidth W about the optical carrier frequency ω_0. For a general quadrature measurement of an optical field $\hat{X}^\theta(\omega)$, the normalized power spectrum can be expressed as

$$V(\omega) = \langle \hat{X}^\theta(\omega) \rangle^2 + \Delta^2 \hat{X}^\theta(\omega), \tag{3.31}$$

consisting of both the variance and the mean squared of the quadrature. For example, the power spectrum for a vacuum state is $V(\omega) = 1$. We can also perform our measurement in the time domain using a digital oscilloscope. For a sampling time interval of $T = 1/(2W)$, Shannon's sampling theorem dictates that

$$\hat{X}^\theta(t) = \int_{-W/2}^{W/2} \hat{X}^\theta(\omega) e^{i\omega t} \mathrm{d}\omega, \tag{3.32}$$

thus allowing us to infer the mean and the variance of the quadrature in time domain.

Part II

Securing the Quantum Devices

Chapter 4

Secure Quantum Random Number Generator (QRNG)

"Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin."

– John von Neumann, *Various techniques used in connection with random digits*

Overview

In this chapter, we come to discuss the topic of quantum randomness, which has the uniqueness of being inherently unpredictable, solely due to the laws of physics. We begin the chapter by giving a general introduction on randomness, highlighting its defining characteristics, and briefly reviewing the current state of art in randomness generation.

The rest of this chapter is divided into two main parts: randomness source characterization and post-processing methods. The aim of this chapter is, however, to provide a sufficiently general overview, in order to put the results of this thesis into perspective. For a detailed review of quantum random number generators and randomness quantification, we refer the reader to recent review papers and surveys [6, 41, 42].

A subset of this chapter is published in the following paper:

- J. Y. Haw, S. Assad, A. Lance, N. Ng, V. Sharma, P. K. Lam, and T. Symul. *"Maximization of extractable randomness in a quantum random-number generator."* Physical Review Applied, 3(5), 054004 (2015).

4.1 Quantum randomness

From a philosophical point of view, the notion of randomness has always been an intriguing concept. It is inherently linked to the understanding of whether our world is deterministic, and also whether free-will is possible or not. From a pragmatist's perspective, however, randomness can be simply seen as the result of *subjective ignorance*, i.e. when an observer does not have a complete description of the particular physical system. For example, the outcome of a coin toss can be seen as random since we do not know, with infinite precision, all the parameters involved, such as the angle of toss, the force applied and so on.

Randomness is a vital resource in many information and communications technology applications, such as computer simulations, statistics, gaming, and cryptography. To ensure the integrity of these applications, a high-quality entropy source which produces good randomness, i.e. uniform and unpredictable, is paramount. The unbreakable security of the one-time pad in cryptography is also based on the assumption of availability of uniformly random bits, unpredictable by any eavesdropper.

There exists also applications which are not concerned with matters of security, and therefore do not have a high demand on perfect randomness. In such cases, a sequence of uniformly distributed numbers mostly suffices. Such sequences can be generated using a pseudorandom number generator (PRNG) that works via certain deterministic algorithms. Although PRNGs can offer highly unbiased random numbers, they cannot be used for applications that require information-theoretic security for two reasons: Firstly, PRNG-generated sequences are unpredictable only under limitations of computational power, since PRNGs are inherently based on deterministic algorithms. One famous example is `randu`, a type of linear congruential generators which generates numbers by recurrence relations. Though being widely used in the 70s for Monte Carlo simulations, this generator actually fails the spectral test due to the correlation between the triplets in the sequence [43], thus rendering the aforementioned simulations questionable. Secondly, the random seeds, which are required to define the initial state of a PRNG, limit the amount of entropy in the random-number sequences they generate. This compromises the security of an encryption protocol.

For cryptographic applications [44], a random sequence is required to be truly unpredictable and to have maximum entropy. To achieve this, intensive efforts have been devoted to developing high-speed hardware RNGs that generate randomness via physical noise [45, 46, 47, 48, 49]. Hardware RNGs are attractive alternatives because they provide fresh randomness based on physical processes that are extremely hard to predict. Moreover, they also provide a solution to the problem of having insufficient entropy. Because of the deterministic nature of classical physics, however, some of these hardware generators may be only truly random under practical assumptions that cannot be validated.

All PRNGs and hardware RNGs can be categorised as processes that are *apparently* random. Ultimately, the produced randomness arises from a lack of full knowledge of the system, such as the seed or the initial condition of the system. On the other hand, RNGs that rely on quantum processes (quantum RNG, or QRNGs), offer guaranteed indeterminism and entropy, since quantum processes are *intrinsically* random [50, 51]. This is the implication of Born's rule in quantum mechanics [52], where the measurement outcome of a quantum state is inherently probabilistic – and not just because the

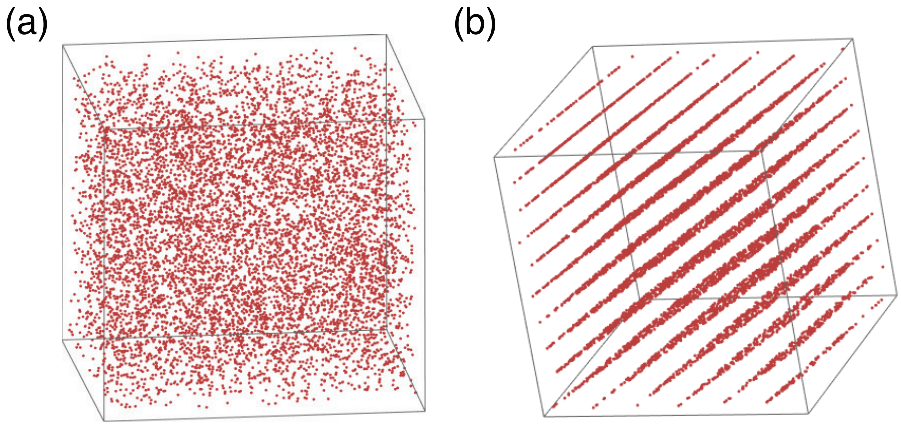


Figure 4.1: `Randu`, an ill-conceived pseudo RNG. The three-dimensional scatter plot of the triplets of three consecutive numbers, while seemingly random from an arbitrary perspective (a), turns out to be falling on 15 2-dimensional plane (b) due to correlations between the triplets. Generated from codes in [54].

observer is ignorant. Meanwhile, the Heisenberg's uncertainty principle, which bounds the precision of the outcome of two non-commuting measurements, necessitates unpredictability in the statistics of quantum measurement. Previously, it was still debatable whether such randomness may still simply be apparent by means of a hidden variable model, i.e. there exist unknown parameters that dictate the evolution of the system deterministically. However, recent loophole-free Bell experiments [12, 13, 14] have sufficiently refuted this possibility. These experiments have put such a deterministic model to test by observing the measurement statistics of two correlated spacelike separate devices. Such space-separated devices allow the invoking of no-signalling from relativity, which implies no faster-than-light communication is allowed. However, the experiments are able to produce measurement statistics that feature correlations much stronger than allowed by a deterministic no-signalling model. This means that the measurement outcomes cannot be pre-established in advance, and therefore are intrinsically indeterministic [1].

The very first quantum entropy source was conceived in 1956, which was based on the radioactive decay counts [55]. Contemporary QRNG realisations are usually in favour of optical systems, owing to the ease of implementation and affordability of the source. For optical QRNGs, two major camps can be identified: photon(s) detection and coherent detection. The simplest example in the former camp is the detection of paths taken by a single photon after a beam splitter, assigning say '0' for a particular detector and '1' for the other [56, 57]. More sophisticated realisations are based on photon detection including photon arrival time [58, 59, 60] and the Poissonian distribution of coherent light [61]. The generation rate of these RNGs is generally limited by the speed of the photon detectors (either single photon detectors or photon number

[1] An alternative would be to abandon the no-signaling principle and embrace definite predefined state properties instead, for instance as advocated by the Bohmian interpretation [53]

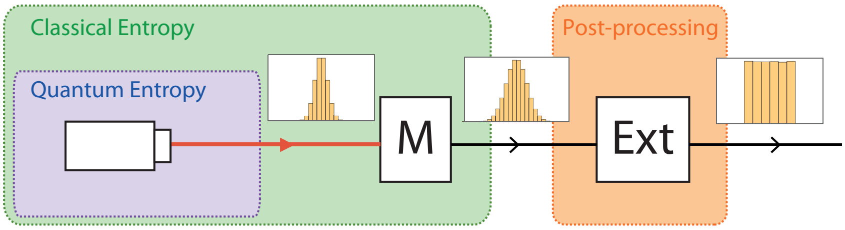


Figure 4.2: Block diagram of a QRNG. During measurement (denoted by "M"), the statistics of the quantum state is inevitably mixed with the entropy of classical origin. By sacrificing partial random bits, the postprocessing stage, or the randomness extractor (denoted by "Ext") transforms the distribution into an almost uniform and unpredictable output.

resolving detectors). One can overcome this bottleneck by means of coherent detection, where highly efficient detectors are used to measure continuous variable properties of light encoded in the quadratures (see Sec. 3.3.2), such as quantum phase fluctuations [62, 63, 64, 65, 66, 67, 68], spontaneous emission noise [69, 70, 71], stimulated Raman scattering [72] and vacuum fluctuations [73, 74, 75].

These QRNGs resolve the shortcomings of apparent RNGs. Theoretically, it would always be desirable to have quantum randomness. However in practice, in order to distil randomness from quantum-mechanical sources, we inevitably need to manipulate or measure the quantum state. Therefore, the final output is often a mixture of genuine quantum randomness and classical noise. The distillation of good quality randomness from such a mixture is, therefore, a question of utmost importance. Without proper characterization, the security of the generator may be compromised if the noise is compromised, or even untrusted. For example, a malicious vendor can supply a detector with predetermined values that may be added on top of the measurement signal, causing the output bits to be less unpredictable (for the vendor). By modelling the physical devices adequately, the effect of these noise contributions can be minimised or eliminated.

In cases where the internal working of the devices is either unknown or inaccessible, genuine randomness based on quantum physics can still be obtained in a device independent fashion. In particular, certification of randomness based on observing the violation of fundamental inequalities such as Bell-inequalities will guarantee that the randomness produced has no classical counterpart, and is genuinely random independent of the working principle of the measurement devices [76]. If only either the source or the measuring device is untrusted, an intermediate approach called semi self-testing is conceivable [41]. We will discuss these further in Sec. 4.4.3.

4.2 Block description of a QRNG

As shown in Fig. 4.2, a QRNG can be divided into two segments: the entropy source and the post-processing procedures [6]. The entropy source produces an amount of raw randomness, as a direct result of certain physical processes in the source. Such a raw randomness may possibly contain uncertainty of both quantum and classical origin. The classical entropy includes noise from classical devices such as from the measuring devices and from the analog-to-digital converter (ADC). In order to access the intrinsically secure randomness, both the classical entropy and the noise of quantum origin, which may be untrusted, have to be treated as side-information.

The second block in Fig. 4.2 indicates post-processing, which transforms a non-uniform raw randomness into a bias-free, side-information-independent randomness. The ratio of extraction is dependent on the amount of truly unpredictable entropy in the source. We will now briefly describe several ways to quantify this extractable randomness via an information-theoretic approach (Sec. 2.6), and how it may be made independent of side-information (classical or quantum).

4.3 Quantifying the randomness

Defining randomness is by no means trivial. Inspired by Kolmogorov complexity [77], Martin-Lof put forth an algorithmic definition [78]: a random sequence should pass all possible statistical tests and should be incompressible. In this context, incompressibility means that the random sequence cannot be generated by a program shorter than its length. This definition, however, is only applicable for infinitely long sequences. Moreover, its shortcomings become more apparent because the algorithmic complexity for a sequence is generally incomputable [79]. Meanwhile, statistical test suites, such as NIST [80] and Diehard [81] tests, consist of a series of hypothesis tests to determine if the generator involved output identically and identically distributed (iid). though able to detect inherent patterns in a random sequence, do not guarantee its privacy. For example, a random sequence possessed by a user may pass all conceivable statistical tests, yet can be fully predictable by a malicious provider who might own an exact copy of the sequence.

This predicament can be resolved by anchoring our definition on the *process* that generates this randomness. Instead of relying on the sequence itself, the randomness is guaranteed as long as the process that generates it is inherently probabilistic. Such is the case for QRNGs, whose randomness is guaranteed by the law of quantum physics (Sec. 4.1). In practice, bias cannot be avoided in implementation due to the inherent measurement outcome distribution, as well as the classical noise accompanying the measurement process. A properly designed QRNG always comes with a post-processing stage to ensure that the final output is (almost) uniformly distributed and uncorrelated with existing information, such as all previous device settings or side information. This ensures that the final output of the QRNG is genuinely random.

To perform source characterization, we explain several different measures of entropy that have been commonly used in the literature to quantify randomness. We also see how one may account for randomness in the eyes of an observer who potentially has

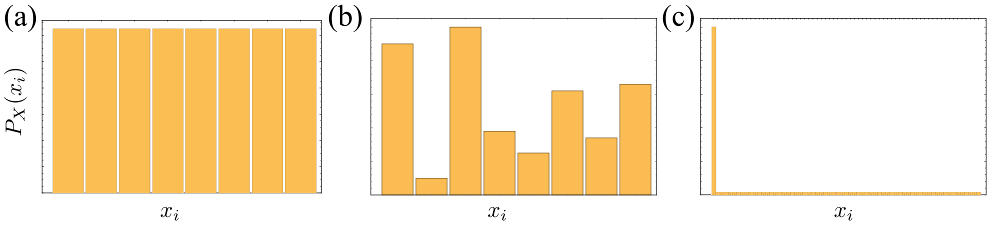


Figure 4.3: The Shannon entropy of an uniform distribution is maximal (a), and decreases when the the distribution deviates from uniformity (b). For an extremely skewed distribution (c), the Shannon entropy is no longer sufficient to quantify the unpredictability of the outcomes.

access to some side information. This is particularly important whenever randomness is used for cryptographic purposes, and needs to be kept private from a malicious eavesdropper. When such side information is classical, depending on physical assumptions of the eavesdropper, we show that variants of the *conditional min-entropy* quantify the maximum amount of bits produced by the source which are *fully random conditioned on the eavesdropper*. This will be the main quantity of interest for the setting of our QRNG described in Chapter 5. In the case where side information is quantum, for example, when the eavesdropper may be entangled with the quantum source itself, a quantum version of the conditional min-entropy must be used instead, which we briefly mention.

4.3.1 Shannon entropy

Shannon entropy, $H(X)$ (Eq. 2.46) tells us about how much information we gain on average once we have learned about the outcome of X. In fact, it can also be seen as how uncertain we are, on average, about X. This quantification is sufficient if we want to gauge the uncertainty in a particular distribution used over many instances, but it is inadequate for single-shot tasks, especially those of a cryptographic setting. As an example, consider the distributions shown in Fig. 4.3. The uniform distribution in Fig. 4.3(a) describes an event with 2^3 equally probable outcomes. In this case, the Shannon entropy of the distribution is maximal and is equal to $\log_2(2^3) = 3$. As the distribution departs from being uniform (Fig. 4.3(b)), the Shannon entropy becomes smaller. This can be interpreted as a case where some outcomes are more likely to occur, hence less "surprise" there is upon obtaining a particular outcome on average. In an extreme case, where the distribution is particularly skewed, Shannon entropy ceases to be a good indicator of the unpredictability. For example, in Fig. 4.3(c), we plot a distribution with $2^q + 1$ outcomes, where there is an extreme outlier, with the rest of the outcomes being equally likely, i.e. $P_X(x_i = 1) = 1/2, P_X(x_j) = 1/2^{q+1}$ and $j \neq 1$. In the limit of $q \gg 1$, $H(X) \to q/2$. In this case, even though the Shannon entropy of the distribution is large, the outcome of the event is highly predictable, since with a very good chance the outcome x_1 is obtained. The moral of this example is that the Shannon entropy is an inadequate measure when it comes to quantifying randomness. In fact, it is at best an upper bound of the randomness [42, 79].

4.3.2 Min-entropy

With the definition of randomness as unpredictability, the guessing probability emerges naturally as a figure of merit. This quantity tells us what is the best chance we have in predicting the outcome of a random variable X. In the unit of bits, this quantity is linked to the min-entropy, which is defined as [82, 83]:

$$H_{\min}(X) := -\log_2 \left[\max_{x_i \in X} P_X(x_i) \right]. \tag{4.1}$$

Operationally, this corresponds to the entropy associated with the optimal strategy for an eavesdropper to guess X, which is to bet on the most likely outcome. The min-entropy also gives a common lower bound on all the Rényi entropies [2]. For a uniform distribution, the min-entropy coincides with the Shannon entropy. For example, the min-entropy for Fig. 4.3(a) is $\log_2 2^3 = 3$. Remarkably, for the distribution in Fig. 4.3(c), the min-entropy is always the logarithm of the bin with highest probability, i.e. $-\log_2 0.5 = 1$, regardless of the number of outcomes. Contrary to the Shannon entropy, min-entropy thus is more robust against skewness of a distribution. The min-entropy is also a crucial parameter for the randomness extractor mentioned in Sec. 4.2. It quantifies the maximum amount of (almost) uniform randomness that can be extracted out of the distribution $P_X(x_i)$ (See sec. 4.5.4).

4.4 Side-information

In the existing literature of QRNG development, usually, the side information is not accounted for since the lab is assumed to be trusted. However, such an assumption is inapplicable when it comes to stringent circumstances such as those in quantum cryptography. Moreover, knowing the source of the randomness is paramount for choosing measurement settings in fundamental physics tests [84]. For example, in experiments that are aimed at investigating fundamental physics, such as those of a Bell test, the choice of measurement settings has to be genuinely random for the collected data to be even considered as valid. As such, the main goal of entropy evaluation of a secure QRNG is to quantify the amount of randomness available in the measurement outcome M, conditioned upon side-information E. This side-information might be accessible by, controllable by, or correlated with an adversary.

The concept of side-information-independent randomness, which includes privacy amplification and randomness extraction, is well established in both classical and quantum information theory [82, 85, 86, 87]. This security aspect of randomness generation started to get considerable attention recently in the framework of QRNG [57, 66, 72, 74, 79, 88, 89, 90]. In particular, Ref. [90] examines the amount of randomness

[2] The Rényi entropy is defined as $H_\alpha(X) = \frac{1}{1-\alpha} \log_2 \left[\sum_{x_i \in X} P_X(x_i)^\alpha \right]$, with respect to a real-valued parameter $\alpha \geq 0$. Min-entropy comes from taking the limit $\alpha \to \infty$.

extractable under various levels of characterisation of the device and power given to the adversary.

We will now review several approaches for dealing with untrusted side information, focusing on classical side information, while seeing that conditional min-entropy best accomplishes the task. Finally in Sec. 4.4.3 we briefly discuss device independent randomness generation.

4.4.1 Classical side-information

Classical side information arises from various sources of classical origin, such as technical electronic noise and thermal noise (Fig. 4.2). Since these sources are not from the desired quantum source, it could be known by the adversary either due to monitoring or direct manipulation. For example, imagine a malicious detector which contaminates the measurement result with pre-established values known to the detector. The raw randomness, though is still correlated to the quantum source, has its security compromised since it is also correlated to the eavesdropper. Hence, unless the lab is completely secure, classical side-information has to be taken into account. Also, this step is necessary if we want to call our device a *bona fide* QRNG. For example, say that the detector is noisy or has low efficiency. Without any form of calibration, the randomness is then more likely to be of classical origins, such as from dark counts.

Mutual information between measured data and quantum entropy

One way of getting randomness of quantum origin would be to quantify the correlation between the measured data M and the quantum data Q. These quantities are related to each other by $M = Q + E$, where E is the electronic noise. From a cryptographic perspective, E can be viewed as any classical noise generated by a malicious party. This approach is used in [75] for a QRNG based on the quantization of self-homodyning detection (Sec. 3.3.2). The statistics follow a channel with additive Gaussian noise introduced in Sec. 2.7. The mutual information between M ($m \sim \mathcal{N}(0, \sigma_M^2)$) and Q ($q \sim \mathcal{N}(0, \sigma_Q^2)$) is considered [3]:

$$I(M\!:\!Q) = H(M) - H(M|Q) \tag{4.2}$$

$$= \sum_{\text{all bins}} P(m_i) \log_2 P(m_i) - \int \mathrm{d}q P(q) H(M|q). \tag{4.3}$$

Maximum entropy for $H(M)$ can be achieved by partitioning the measured bins with $N = 2^n$ bins of equal area, thus giving $H(M) = n$. With this binning method, there will be more bins near the origin. As a result, the conditional entropy $H(M|q)$ is largest when evaluated at $q = 0$. This is actually equivalent to the entropy of the measured data without any quantum fluctuation contributions $H(E)$. We can then derive a lower

[3] Here for brevity we omit the subscripts for the distributions.

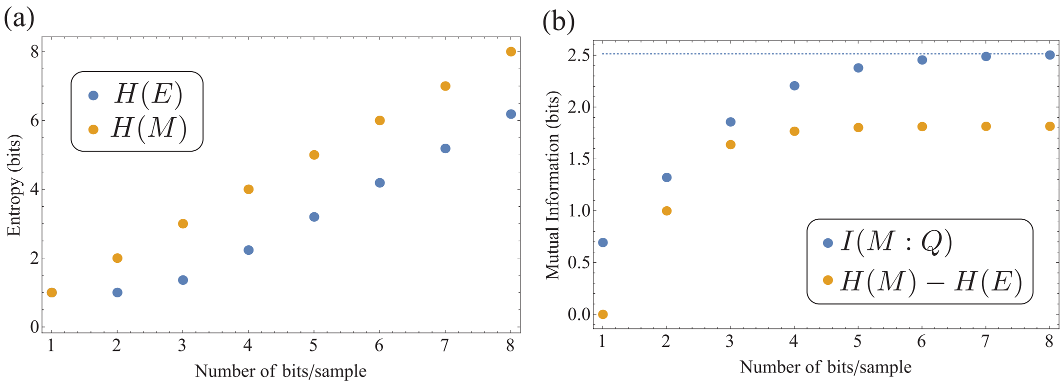


Figure 4.4: (a) Shannon entropy for the measured signal $H(M)$ and the electronic noise $H(E)$. (b) The mutual information between the measured signal and the quantum entropy $I(M:Q)$, together with the difference between $H(M)$ and $H(E)$. The dashed line is the upper bound for $I(M\!:\!Q)$ at the infinite binning limit. The SNR is 15 dB.

bound for $I(M\!:\!Q)$ by having:

$$\begin{aligned} I\left(M:Q\right) &\geq n - H(M|q=0) \\ &= n - H(E). \end{aligned} \tag{4.4}$$

This equation can also be reinterpreted as $H(M)-H(E)$, the entropy of the measured signal subtracted the noise entropy. This approach, as shown in Fig. 4.4 for signal-to-noise ratio (SNR) of 15 dB [4] , however does not allow us to extract more randomness even if we increase the number of bins, which is contradictory to what we would expect. Upon observation of Fig. 4.4(a), the entropy of the electronic noise increases at almost the same rate as the measured signal after a threshold binning value. Due to equal area binning of the measured signal, the bin width around the centre is smaller. As the number of bins increases beyond a threshold, the electronic noise will also be binned, and increases as the binning further increase. Hence increasing the number of bins does not lead to any further increase in the *effective* number of bits, as reflected in Fig. 4.4(b).

The mutual information $I(M\!:\!Q)$ can be calculated exactly (for arbitrary amounts of partitioning) once we obtain the joint probability table between M and Q. This is done using the formula

$$I\left(M\!:\!Q\right) = \sum_{\text{all bins}(A_i,B_j)} P(m\in A_i, q\in B_j)\log_2\frac{P(m\in A_i, q\in B_j)}{P(m\in A_i)P(q\in B_j)}\,. \tag{4.5}$$

On the other hand, in the limit of infinitely many bins $n\to\infty$, we can calculate the maximum value of $I\left(M:Q\right)$ with Eq. (2.68)

$$I\left(M:Q\right) = \frac{1}{2}\log_2\left(1+\frac{\sigma_Q^2}{\sigma_E^2}\right), \tag{4.6}$$

[4] SNR is defined as $10\log_{10}(\sigma_M^2/\sigma_E^2)$, where M is the measurement signal and E is the noise.

where $\sigma_E^2 = \sigma_M^2 - \sigma_Q^2$. We see that the exact amount of $I(M\!:\!Q)$ approaches the asymptotic value, and does not increase with further binning. This is rather undesirable, as it unnecessarily limits the extractable randomness, and ultimately the speed of the QRNG.

To understand this approach in more detail, note that the quantity $I(M\!:\!Q)$ is actually the channel capacity of the QRNG, i.e. it can tell us how easy it is to recover Q when given M. However, for the purposes of an RNG, it is actually not our goal to recover the quantum signal. Consider an example of $M = Q + E$ mod 2, where both Q and E represent a single random bit and an eavesdropper Eve has access to E. Therefore, the measurement outcome M is also one random bit. This means M and Q are not correlated at all, implying that the mutual information vanishes, i.e. $I(M\!:\!Q) = 0$. However, the eavesdropper Eve cannot learn the value of M since $I(M\!:\!E)$ is also zero. The measured signal conditioned on the electronic noise, in this case, is $H(M|E) = H(M)$ and is hence 1 bit. Therefore, even if $I(M\!:\!E)$ is zero, one can still hope to extract random bits. Hence, the channel capacity does not seem to have the desired operational significance in terms of quantifying extractable randomness.

This motivates the detailing of our next approach, where we consider $H(M|E)$, the entropy of M conditioned on the classical side-information E.

Entropy of measured data conditioned on classical noise

In order to evaluate $H(M|E)$, we need to figure out the amount of correlation between M and E. As before, given the joint probability table between the measured data and the electronic noise, we can calculate the mutual information $I(M : E)$. To obtain an upper bound for this, we assume that Eve has a continuous noise source to grant her infinite measurement precision

$$I\left(M : E\right) = \sum_{\text{all bins}(A_i)} \int \mathrm{d}e P(M \in A_i, E = e) \log_2 \frac{P(M \in A_i, E = e)}{P(M \in A_i)P(E = e)} \,. \tag{4.7}$$

This quantity is plotted in Fig. 4.5(a) for various bin sizes, with an 15dB of SNR. It is bounded from above,

$$I\left(M : E\right) \leq \frac{1}{2} \log_2 \left(1 + \frac{\sigma_E^2}{\sigma_Q^2}\right) \,, \tag{4.8}$$

and approaches the bound as the number of measurement bins goes to infinity. For equal area binning of the measured data, the quantity $H(M|E)$ is evaluated via the following relation:

$$H(M|E) = n - I(M\!:\!E). \tag{4.9}$$

We plot this in Fig. 4.5(b). In contrary to what we see in the case of $I(M\!:\!Q)$, as we have more binning, the effect of the electronic noise E is actually bounded rather than increasing. In this case, increasing the binning allow us to continuously increase the conditional

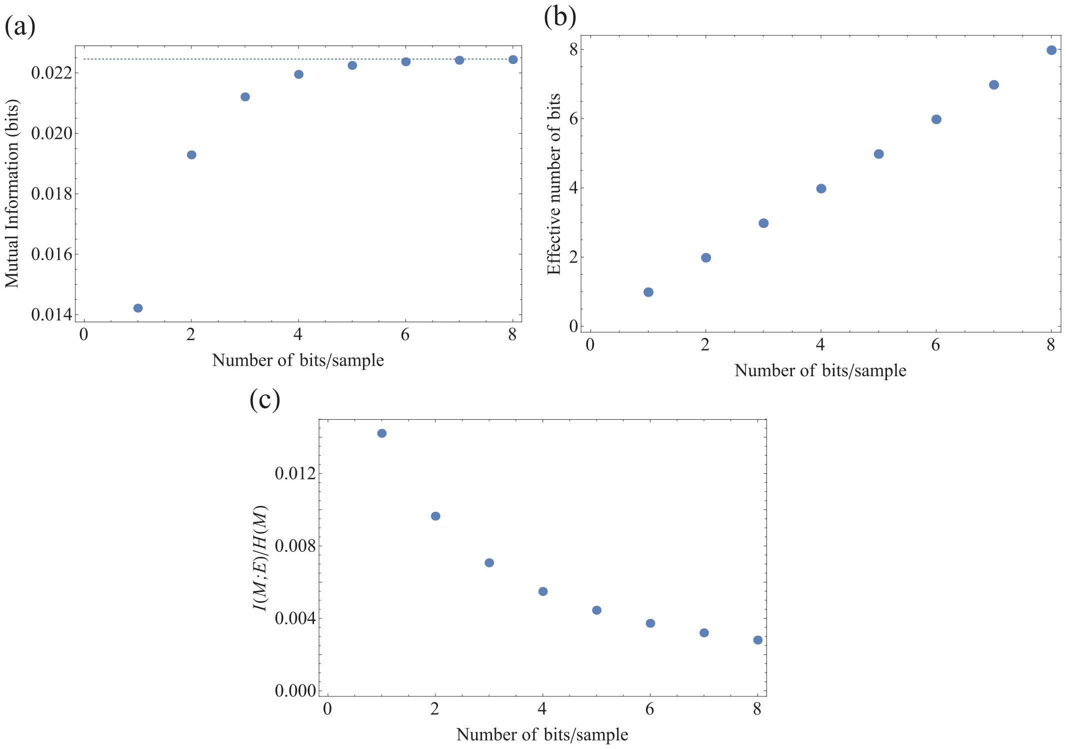


Figure 4.5: (a) The mutual information between the measured and the electronic noise $I(M:E)$. Dashed line represent the upper bound at infinite binning limit. (b) The effective number of bits quantified by the conditional Shannon entropy $H(M|E)$. (c) The ratio between $I(M:E)$ and $H(M|E)$ decreases as the binning increases. The SNR is 15 dB.

Shannon entropy $H(M|E)$. As shown in Fig. 4.5(c), the ratio of $I(M:E)/H(M|E)$ reduces by 5 times from a 1-bit to an 8-bit binning.

For the case of infinite binning, we can adopt the use of differential entropy $h(X)$, which is an extension of the Shannon entropy for continuous variables (Sec. 2.7). In this case, we have

$$\begin{aligned} h(M|E) &= h(M) - I(M:E) \\ &= \frac{1}{2}\log_2(2\pi e\sigma_M^2) - \frac{1}{2}\log_2\left(1+\frac{\sigma_E^2}{\sigma_Q^2}\right) \\ &= \frac{1}{2}\log_2(2\pi e\sigma_Q^2) = h(Q), \end{aligned} \tag{4.10}$$

where we see that $h(M|E)$ is actually equal to the continuous Shannon entropy of the quantum signal Q alone. This is expected as $h(M|E) = h(Q+E|E) = h(Q|E) = h(Q)$, given the fact that quantum noise and the classical noise are independent of each other. The variance σ_Q^2 is inferred by subtracting the σ_E^2 from σ_M^2.

Despite the advantage of being useful in utilising the binning methods, this quantification based on conditioning of measured data over classical noise seems to be overly generous. For example, in the case of finite binning, in Fig. 4.5(b), 99.72% of 8 bits is considered as effective entropy independent of the eavesdropper. Ultimately, as the number of bits increases, the bits to be subtracted is bounded too. Also, we remind the reader that in Sec. 4.3, we have seen that the min-entropy is the appropriate candidate, instead of the Shannon counterpart.

Estimating the amount of quantum contribution to raw randomness

More recently, Ma *et al.* [88] proposed a framework to obtain randomness that is independent of classical noise. By using *min-entropy* as the quantifier for randomness, they extracted a higher rate of random bits of 6.7 bits per sample from 8 bits (approximately 84%), where the quantum contribution of the randomness was obtained by inferring the signal-to-noise ratio. Similar to the previous case, the quantum entropy is inferred, however, it is evaluated upon min-entropy instead. This method, though provides a more realistic description, calls for a more rigorous mathematical treatment. For example, the min-entropy version for Eq. (4.10) might not work here, i.e. the relation between $H_{\min}(M|E)$ and $H_{\min}(Q)$ is unclear. We will explore this in the next section. Furthermore, as we will demonstrate in the Chapter 5, this approach misses the opportunity to maximise the randomness, since there are no parameters (such as the bounding of electronic noise and the choice of dynamical range) left to be optimised.

Conditional min-entropy

Given a random variable X potentially correlated with some other classical information K, the worst-case conditional min-entropy $H_{\min}(X|K)$ is defined as [91]

$$H_{\min}(X|K) := -\log_2 \left[\max_{k_j \in \mathrm{supp}(P_K)} \max_{x_i \in X} P_{X|K}(x_i|k_j) \right] , \tag{4.11}$$

where the support $\mathrm{supp}(f)$ is the set of values x_i such that $f(x_i) > 0$. It tells us the amount of (almost) uniform and independent random bits that one can extract from a biased random source, with respect to untrusted parameters.

For the purpose of illustration, let us consider the two extreme cases:

- $I(X : K) = 0$, i.e. the random variable does not depend on the classical information K. In this case, we get $P_{X|K}(x_i|k_j) = P_X(x_i)$, and $H_{\min}(X|K) = H_{\min}(X)$ which is the typical formula for randomness extraction (Eq. 4.1).

- $X = K$, i.e. we are only detecting the untrusted classical information. In this case $P_{X|K}(x_i|k_j) = \delta(x_i - k_j)$, and $\max P_{X|K}(x_i|k_j) = 1$, hence $H_{\min}(X|K) = 0$, implying that there is no randomness remaining to be extracted.

Applying this quantity in the case of randomness quantification of a QRNG, Eq. 4.11 takes the form of $H_{\min}(M_{\text{dis}}|E)$, where M_{dis} is the discretized measured signal, and E is the classical noise. The worst-case conditional min-entropy is a very stringent quantifier for randomness, since it assumes that the malicious party has full control over E. As we will describe in Sec. 5.2.1, without a bound on the range of E, one cannot extract any secure randomness at all! However, if we assume that an adversary can only eavesdrop on E (or compute it), but has no control over it, we can estimate the average chance of successful eavesdropping with the *average* guessing probability of M_{dis} given E_{dis} [82, 83, 92],

$$\begin{aligned} &P_{\text{guess}}(M_{\text{dis}}|E_{\text{dis}}) \\ &= \left[\sum_{e_j \in E_{\text{dis}}} P_{E_{\text{dis}}}(e_j) \max_{m_i \in M_{\text{dis}}} P_{M_{\text{dis}}|E_{\text{dis}}}(m_i|e_j) \right], \end{aligned} \tag{4.12}$$

which denotes the probability of correctly predicting the value of discretized measured signal M_{dis} using the optimal strategy, given access to discretized classical noise E_{dis}. Here $P_{E_{\text{dis}}}(e_j)$ is the discretized probability distribution of the classical noise. The extractable secure randomness from our device is then quantified by the average conditional min-entropy

$$\bar{H}_{\min}(M_{\text{dis}}|E_{\text{dis}}) = -\log_2 P_{\text{guess}}(M_{\text{dis}}|E_{\text{dis}}). \tag{4.13}$$

4.4.2 Quantum side-information

Analogous to classical side-information, a random variable X can also be correlated with another quantum system R. An observer with access to system R can, by measuring or performing quantum operations on R, gain knowledge about X. In this case, a generalisation of the conditional min-entropy to the quantum regime is warranted.

Let us first understand how the joint state of X and R looks like. Since X is classical and R is quantum, such states are also known as *cq-states*:

$$\rho_{XR} = \sum_{x \in \mathcal{X}} P_X(x) |x\rangle\langle x| \otimes \rho_R^x , \tag{4.14}$$

where one thinks of the classical value $x \in \mathcal{X}$ as encoded in mutually orthogonal states $\{|x\rangle\}_{x \in \mathcal{X}}$ on a quantum system X. The conditional min-entropy of X given R is then defined as [93]

$$H_{\min}(X|R) := \max_{\sigma_R \in H_R} \sup\{\lambda : 2^{-\lambda} \mathbb{I}_X \otimes \sigma_R - \rho_{XR} \geq 0; \sigma_R \geq 0, \text{tr}(\sigma_R) \leq 1\} . \tag{4.15}$$

Here, $\mathbb{I}_X$ is the identity matrix of the Hilbert space H_X and the maximisation is performed over the reduced density matrix σ_R of the subsystem R. Conditional min-entropy tells us how much we know about X, inferred from measurements on R alone. It has been shown that this corresponds to the maximum probability of guessing X given system R [82], and therefore naturally generalises the classical conditional min-entropy defined above in Eq. (4.13).

4.4.3 Source and device independent randomness

The quantification of the entropy in the QRNG we discussed so far made the assumptions that the underlying quantum physical process and measurement device can be characterized and calibrated. This type of device falls under the category of *practical* QRNG, where effect from the unwanted classical (or quantum) noises can be isolated with appropriate modelling. In situation such as a black-box scenario, where the source and the measurement devices are unknown, it is hard to pinpoint whether the "QRNG" produces fresh random bits. The worst case would be the scenario where the device is merely a pseudo-random number generator in disguise, which could be correlated to the malicious provider.

To overcome these restrictions, certifiable randomness based on a violation of fundamental inequalities has recently been proposed and demonstrated [76, 92, 94]. These *self-testing* devices do not rely on the assumption of a trusted device. For example, consider a device independent QRNG based on the violation of Bell correlations. Even if the output randomness is tainted with spurious noise, genuine randomness can be certified and bounded based on the measured correlations alone; it is thus independent from the internal structure of the generator [76]. However, achieving a high generation rate with such devices is experimentally challenging, since a large amount of the raw output has to be used for statistical analysis instead. Moreover, for the generated randomness to be considered fully device-independent, all the loopholes in the experiments have to be addressed simultaneously too. And this milestone has only been checked off very recently with state-of-the-art devices [13, 14, 12].

As described in the block description of QRNG (Fig. 4.2), the entropy source comprises a quantum source plus measurement devices. In a practical scenario, usually either part is accessible to the user. This opens up the possibility of an intermediate solution known as *semi-self-testing*. By making realistic assumptions on either the source or the measuring devices, a semi-self-testing QRNG offers a trade-off between the practical QRNGs and self-testing QRNGs. The key idea is that by using some initial randomness, the measurement basis or the quantum state can be chosen according to some random variables, in order to bound the effect of untrusted parties. We refer our reader to [41] for a more detailed exposition of these three regimes.

4.5 Randomness extraction

Lastly, we explain the notion of randomness extraction, and its role in distilling fully random bits out of raw, non-uniform randomness. We discuss how randomness extraction is achieved via post-processing methods, and provide a review of the different approaches used to date.

Most of the times, quantum sources are not ideal sources of randomness, in the sense that the distribution is often biased, while uniform randomness is required for application purposes. In our situation, the quantum vacuum state measured by our CV QRNG exhibits a Gaussian distribution. To generate ideal randomness, postprocessing of the raw output is necessary to produce shorter, yet almost uniformly distributed random strings. Therefore, an important phase in postprocessing is randomness extraction. Randomness extractors are functions that take raw, imperfect randomness as input, while outputting a random sequence of shorter length, leaving most of the unpredictability intact, in a condensed form.

4.5.1 Algorithm extractor

Ad hoc algorithms such as the Von Neumann extractor, XOR corrector, and least significant bit operation are widely used [95, 71, 47, 96, 97, 70]. These methods, although simple in practice, might fail to produce randomness at all if non-negligible correlations exist among the raw bits [98].

4.5.2 Cryptographic extractor

Another attractive alternative for secure randomness extraction is the use of cryptographic hashing functions [99, 100, 101, 102]. While these cryptographic hashing functions are not information-theoretically proven to be secure, they are still suited for many cryptographic applications and settings where the adversary is assumed to be computationally bounded. The reason for utilizing them over universal hashing functions is that they can have high throughput due to efficient hardware implementation. Previously, cryptographic hashing extractors have been deployed in [66, 75, 64, 59], with functions such as SHA-512 and Whirlpool. Most of the implementations keep a number of bits exactly equal to the min-entropy, which might not be fully secure (see Section 4.5.4).

4.5.3 Information theoretic extractor

From an information-theoretic standpoint, universal hashing functions are desirable candidates for randomness extraction [85, 88]. These functions act to recombine bits within a sample according to a randomly chosen seed, and map them to truncated, almost uniform random strings. They constitute a strong extractor which implies that the seed can be reused without sacrificing too much randomness. In recent development of QRNGs [72, 88, 103, 89, 79], they have been used to construct hashing functions such as the Toeplitz-hashing matrix. These constructions require a long (but reusable) seed [104]. A different implementation of an information-theoretic randomness extractor, the Trevisan extractor, [86, 87, 88] has also received considerable attention. This particular construction of a strong extractor has been proven secure against quantum side information, and, furthermore, it requires a relatively short seed. Despite so, the complexity of the algorithm imposes a very stringent limit on the extraction speed (0.7 kb/s achieved in Ref. [88] and 150 kb/s in Ref. [87]).

4.5.4 Notes on the Leftover Hash Lemma

From an information-theoretic standpoint, the most prominent advantage of universal hashing functions described in Sec. 4.5 is the randomness of the output guaranteed unconditionally by the leftover hash lemma (LHL). More specifically, LHL states that for any real-valued parameter $\varepsilon > 0$, if the output of a universal hashing function has length

$$l \leq t - 2\log_2(1/\varepsilon), \tag{4.16}$$

where t denotes the (conditional) min-entropy, then the output will be ε-close in terms of statistical distance to a perfectly uniform distribution [93]. Moreover, a universal hashing function constructs a strong extractor, where the output string is also independent of the seed of the function [85, 88].

Meanwhile, the quantum leftover hash lemma is a extension of its classical counterpart, proven only recently in [93], where the statistical distance ε is replaced by the trace distance of the global state, while the uniform distribution is represented by a maximally mixed state on the system encoding the random variable of interest.

On the other hand, for a strong cryptographic extractor, the output is ε'-computationally indistinguishable from the uniform distribution (see Refs. [101, 100] for formal definitions). It is shown in Refs. [93, 102] that LHL can be generalized to take into account almost universal functions (functions statistically ξ-close to being universal hashing functions). This generalized LHL takes the form of $l = \min(t, \log_2(1/\xi)) - 2s$, where s is an integer related to ε'. Under suitable parameter constraints and operating modes, an ε'-cryptographic extractor can be treated as a ξ-almost universal function, and, hence a strong randomness extractor [102, 101]. Hence for a cryptographic extractor, it is necessary to sacrifice some bits according to the desired security parameter s to ensure the security and uniformity of the output.

Chapter 5

Maximisation of Extractable Randomness in Continuous Variable QRNG

> *"If you know the enemy and know yourself you need not fear the results of a hundred battles."*
>
> – Sun Tzu, *The Art of War*

Overview

Intrinsic uncertainty is a distinctive feature of quantum physics, which can be used to harness high-quality randomness. However, in realistic scenarios, the raw output of a quantum random-number generator is inevitably tainted by classical technical noise. The integrity of the device can be compromised if this noise is tampered with, or even controlled by some malicious party. In this chapter, we propose and experimentally demonstrate an approach that produces side-information independent randomness that is quantified by min-entropy conditioned on this classical noise. We present a method for maximizing the conditional min-entropy of the number sequence generated from a given quantum-to-classical-noise ratio. The spectral response of the detection system shows the potential to deliver more than 70 Gbit/s of random numbers in our experimental setup. The majority of work in this chapter has been published in the following article:

- J. Y. Haw, S. Assad, A. Lance, N. Ng, V. Sharma, P. K. Lam, and T. Symul. *"Maximization of extractable randomness in a quantum random-number generator."* Physical Review Applied, 3(5), 054004 (2015).

5.1 Continuous Variable QRNG

Following the previous work of ANU Quantum Optics group in [74], our source of randomness is the based on the continuous variable (CV) homodyne measurement of the vacuum state (Sec. 3.3.2). Our CV-QRNG exploits the uncertainty principle to harness entropy from quantum states. The projection of the Wigner function, or the distribution of the amplitude quadrature $\hat{X}$, follows a Gaussian random distribution. There are several distinct advantages of this approach. First, the resource of quantum randomness, the vacuum state, can be easily prepared with a high fidelity. Second, the performance of the QRNG is insensitive to detector loss, which can be simply compensated by increasing the local oscillator power.

5.1.1 Characterization of noise and measurement

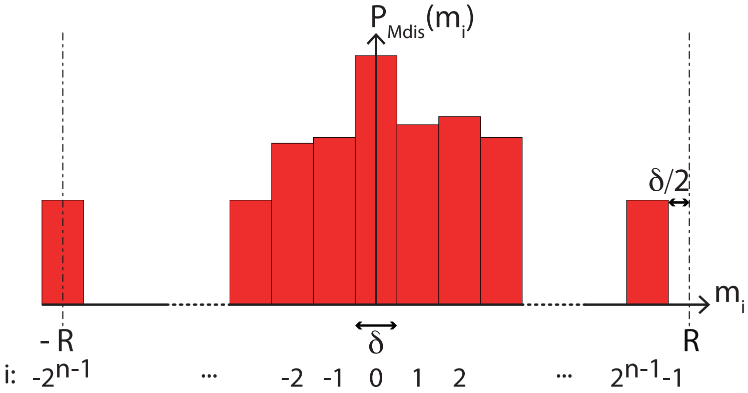


Figure 5.1: Model of the n-bit ADC, with analog input in the ADC dynamical range $[-R+\delta/2, R-3\delta/2]$ and bin width $\delta = R/2^{n-1}$. We choose the central bin centred around 0, the lowest bin $i_{\min} = -2^{n-1}$ centered around $-R$, and the highest bin $i_{\max} = 2^{n-1}-1$ centered around $R-\delta$.

We first discuss the model for our CV QRNG. A homodyne measurement of the vacuum state gives Q, the quadrature values of the vacuum state. The theory of quantum mechanics states that these values are random and have a probability density function (PDF) p_Q which is Gaussian and centred at zero with variance σ_Q^2. In practice, these quadrature values cannot be measured in complete isolation from sources of classical noise E. The measured signal M is then $M = Q + E$. Denoting the PDF of the classical noise as p_E, the resulting measurement PDF, p_M is then a convolution of p_Q and p_E. Assuming that the classical noise follows a Gaussian distribution centred at zero and with variance σ_E^2, the measurement PDF is

$$p_M(m) = \frac{1}{\sqrt{2\pi}\sigma_M} \exp\left(-\frac{m^2}{2\sigma_M^2}\right), \tag{5.1}$$

for $m \in M$ where the measurement variance $\sigma_M^2 = \sigma_Q^2 + \sigma_E^2$. The ratio between the variances of the quantum noise and the classical noise defines the QCNR, i.e. QCNR$=10\log_{10}(\sigma_Q^2/\sigma_E^2)$. The sampling is performed over an n-bit ADC with dynamical ADC range $[-R+\delta/2, R-3\delta/2]$. Upon measurement, the sampled signal is discretized over 2^n bins with bin width $\delta = R/2^{n-1}$. The range is chosen so that the central bin is centered at zero. The resulting probability distribution of discretized signal M_{dis} reads

$$P_{M_{\text{dis}}}(m_i) = \begin{cases} \int_{-\infty}^{-R+\delta/2} p_M(m)\mathrm{d}m, & i = i_{\min}, \\ \int_{m_i-\delta/2}^{m_i+\delta/2} p_M(m)\mathrm{d}m, & i_{\min} < i < i_{\max}, \\ \int_{R-3\delta/2}^{\infty} p_M(m)\mathrm{d}m, & i = i_{\max}, \end{cases} \tag{5.2}$$

as shown in Fig. 5.1 and $m_i = \delta \times i$, where the i are integers $\in \{-2^{n-1}, ..., 2^{n-1} - 1\}$. The two extreme cases $i = i_{\min}$ and $i = i_{\max}$ are introduced to model the saturation on the first and last bins of an ADC with finite input range, i.e. all the input signals outside $[-R + \delta/2, R - 3\delta/2]$ will be accumulated in the first and last bins. Figure 5.2 shows the discretized distribution $P_{M_{\text{dis}}}(m_i)$ with different R. We see that an appropriate choice of dynamical ADC range for a given QCNR and digitization resolution n is crucial, since overestimating or underestimating the range will either lead to excessive unused bins or unnecessary saturation at the edges of the bins [97], causing the measurement outcome to be more predictable. However, in designing a secure CV QRNG, R should not be naively optimized over the measured distribution $P_{M_{\text{dis}}}(m_i)$ but over the distribution conditioned on the classical noise. The conditional PDF between the measured signal M and the classical noise E, $p_{M|E}(m|e)$ is given by

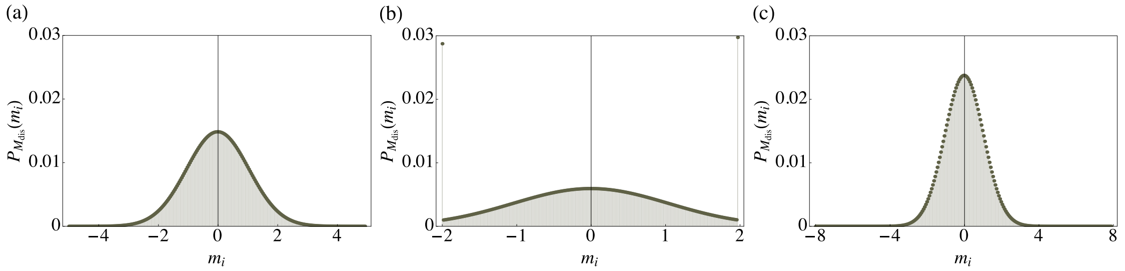


Figure 5.2: Numerical simulations for the measured distribution probabilities $P_{M_{\text{dis}}}(m_i)$ versus quadrature values, with different dynamical ADC range parameters $R =$ (a) 5, (b) 2 and (c) 8. Without optimization, one will have either an oversaturated or unoccupied ADC bins, which will compromise both the rate and the security of the random-number generation. The parameters used are $n = 8$ and QCNR$= 10$ dB.

$$\begin{aligned} p_{M|E}(m|e) &= \frac{1}{\sqrt{2\pi(\sigma_M^2 - \sigma_E^2)}} \exp\left[-\frac{(m-e)^2}{2(\sigma_M^2 - \sigma_E^2)}\right] \\ &= \frac{1}{\sqrt{2\pi}\sigma_Q} \exp\left[-\frac{(m-e)^2}{2\sigma_Q^2}\right]. \end{aligned} \tag{5.3}$$

This is the PDF of the quantum signal shifted by the classical noise outcome e. By setting $\sigma_Q^2 = 1$, we normalize all the relevant quantities by the quantum noise. From Eq. (5.2), the discretized conditional probability distribution is, thus,

$$
\begin{aligned}
&P_{M_{\text{dis}}|E}(m_i|e) \\
&= \begin{cases} \int_{-\infty}^{-R+\delta/2} p_{M|E}(m|e)\mathrm{d}m, & i = i_{\text{min}}, \\ \int_{m_i-\delta/2}^{m_i+\delta/2} p_{M|E}(m|e)\mathrm{d}m, & i_{\text{min}} < i < i_{\text{max}}, \\ \int_{R-3\delta/2}^{\infty} p_{M|E}(m|e)\mathrm{d}m, & i = i_{\text{max}}. \end{cases}
\end{aligned} \tag{5.4}
$$

With these, we are now ready to discuss how R should be chosen under two different definitions of min-entropy, namely worst-case min-entropy and average min-entropy.

5.2 Maximising the min-entropy

5.2.1 Worst-case min-entropy

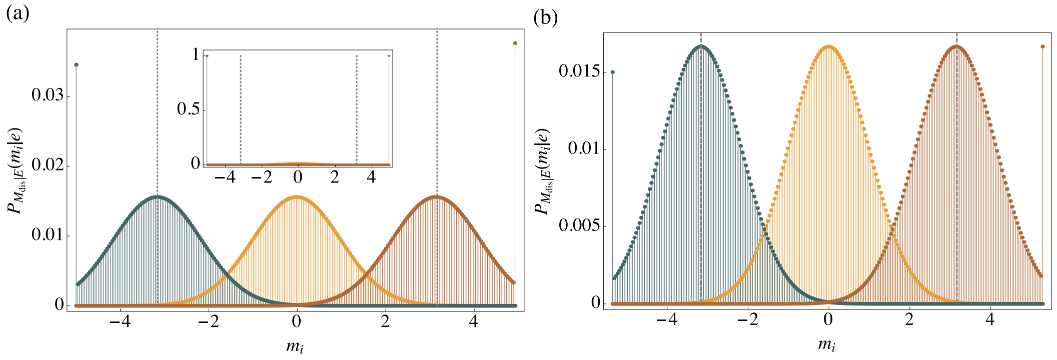


Figure 5.3: Numerical simulations of: (a) conditional probability distributions $P_{M_{\text{dis}}|E}(m_i|e)$, with $e = \{-10\sigma_E, 0, 10\sigma_E\}$ (from left to right) and $R = 5$. Without optimizing R, when $e = \pm 10\sigma_E$, saturations in the first and last bins affect the maximum of the conditional probability distribution. Inset: $P_{M_{\text{dis}}|E}(m_i|e)$, with $e = \{-100\sigma_E, 0, 100\sigma_E\}$ (from left to right). Unbounded classical noise will lead to zero randomness due to the oversaturation of dynamical ADC. (b) Optimized $P_{M_{\text{dis}}|E}(m_i|e)$, with $e = \{-10\sigma_E, 0, 10\sigma_E\}$ (from left to right). From Eq. (5.9), the optimal R is chosen to be 5.35. The saturations do not exceed the maximum of the conditional probability distribution whenever $-10\sigma_E \leq e \leq 10\sigma_E$. The parameters are $n = 8$, QCNR= 10 dB. Dashed lines indicate $m_i = \pm 10\sigma_E$.

In the case of Gaussian distributions, the support of the probability distribution will be $\mathbb{R}$. Following Eq. (5.4), upon discretization of the measured signal M, the worst-case min-entropy conditioned on classical noise E is

$$
H_{\text{min}}(M_{\text{dis}}|E) = -\log_2 \left[\max_{e \in \mathbb{R}} \max_{m_i \in M_{\text{dis}}} P_{M_{\text{dis}}|E}(m_i|e) \right]. \tag{5.5}
$$

Here we assumed that from the eavesdropper's perspective, the classical noise is known fully with arbitrary precision. Performing the integration in Eq. (5.4), the maximization over M_{dis} in Eq. (5.5) becomes

$$\max_{m_i \in M_{\text{dis}}} P_{M_{\text{dis}}|E}(m_i|e) \\ = \max \begin{cases} \frac{1}{2}\left[1 - \text{erf}\left(\frac{e+R-\delta/2}{\sqrt{2}}\right)\right], \\ \text{erf}\left(\frac{\delta}{2\sqrt{2}}\right), \\ \frac{1}{2}\left[\text{erf}\left(\frac{e-R+3\delta/2}{\sqrt{2}}\right) + 1\right], \end{cases} \tag{5.6}$$

where $\text{erf}(x) = 2/\sqrt{\pi}\int_0^x e^{-t^2}dt$ is the error function. We note that we have $\max_{e\in\mathbb{R}} \max_{m_i\in M_{\text{dis}}} P_{M_{\text{dis}}|E}(m_i|e) = 1$, achieved when $e \to -\infty$ or $e \to \infty$. This results in $H_{\min}(M_{\text{dis}}|E) = 0$ [see inset of Fig. 5.3 (a)]. Indeed it is intuitive to see that in the case where the classical noise e takes on an extremely large positive value, the outcome of M_{dis} is almost certain to be $m_{i_{\max}}$ with large probability. However, this scenario happens with a very small probability. Hence for practical purposes, one can bound the maximum excursion of e, for example $-5\sigma_E \leq e \leq 5\sigma_E$, which is valid for 99.9999% of the time. With this bound on the classical noise, we now have

$$\max_{e\in[e_{\min},e_{\max}]} \max_{m_i \in M_{\text{dis}}} P_{M_{\text{dis}}|E}(m_i|e) \\ = \max \begin{cases} \frac{1}{2}\left[1 - \text{erf}\left(\frac{e_{\min}+R-\delta/2}{\sqrt{2}}\right)\right], \\ \text{erf}\left(\frac{\delta}{2\sqrt{2}}\right), \\ \frac{1}{2}\left[\text{erf}\left(\frac{e_{\max}-R+3\delta/2}{\sqrt{2}}\right) + 1\right], \end{cases} \tag{5.7}$$

and when $e_{\min} = e_{\max}$,

$$H_{\min}(M_{\text{dis}}|E) = -\log_2\left[\max\left\{\frac{1}{2}\left[\text{erf}\left(\frac{e_{\max} - R + 3\delta/2}{\sqrt{2}}\right) + 1\right]; \text{erf}\left(\frac{\delta}{2\sqrt{2}}\right)\right\}\right], \tag{5.8}$$

which can be optimized by choosing R such that

$$\frac{1}{2}\left[\text{erf}\left(\frac{e_{\max} - R + 3\delta/2}{\sqrt{2}}\right) + 1\right] = \text{erf}\left(\frac{\delta}{2\sqrt{2}}\right). \tag{5.9}$$

This optimized worst-case min-entropy $H_{\min}(M_{\text{dis}}|E)$ is directly related to the extractable secure bits that are independent of the classical noise. As shown in Fig. 5.3(a), when Eq. (5.8) is not optimized with respect to R, the saturation in the first (last) bin for $e_{\min/\max} = \pm 10\sigma_E$ becomes the peaks of the conditional probability distribution, hence compromising the attainable min-entropy. By choosing the optimal value for R via Eq. (5.9), as depicted in Fig. 5.3(b), the peaks at the first and last bins will always be lower than or equal to the probability within the dynamical range. Thus, by allowing the dynamical ADC range to be chosen freely, one can obtain the lowest possible conditional probability distribution, and hence produce the highest possible amount of

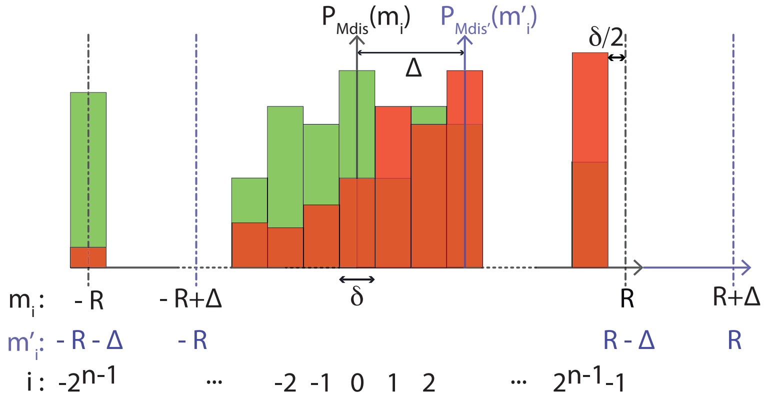


Figure 5.4: Model of the n-bit ADC, with analog input in the ADC dynamical range $[-R+\delta/2, R-3\delta/2]$ and bin width $\delta = R/2^{n-1}$. Offset of the distribution is modeled by another reference frame m' centered at offset Δ. In the original frame m, the lowest and highest bins are now centered around $-R-\Delta$ and $R-\delta-\Delta$.

secure random bits per sample for a given QCNR and n-bit ADC.

In a realistic scenario, the mean of the measured signal's probability distribution is often nonzero. It is possible that such an offset might be induced by a malicious party over the sampling period. The model is depicted in Fig. 5.4, where the offset Δ of the distribution is captured by another reference frame m' centered at Δ. In this model, Eq. (5.4) can now be rewritten as

$$P^{(\Delta)}_{M_{\text{dis}}|E}(m_i|e) = \begin{cases} \int_{-\infty}^{-R-\Delta+\delta/2} p_{M'|E}(m'|e)\mathrm{d}m', & i = i_{\min}, \\ \int_{m'_i-\Delta-\delta/2}^{m'_i-\Delta+\delta/2} p_{M'|E}(m'|e)\mathrm{d}m', & i_{\min} < i < i_{\max}, \\ \int_{R-3\delta/2-\Delta}^{\infty} p_{M'|E}(m'|e)\mathrm{d}m', & i = i_{\max}. \end{cases} \tag{5.10}$$

Following the similar procedure as before and bounding Δ, we finally arrive at the generalization of Eq.(5.8),

$$H_{\min}(M_{\text{dis}}|E) = -\log_2 \max(c_1, c_2). \tag{5.11}$$

Here $c_1 = \frac{1}{2}\left[\operatorname{erf}\left(\frac{e_{\max}+\Delta_{\max}-R+3\delta/2}{\sqrt{2}}\right)+1\right]$ and $c_2 = \operatorname{erf}\left(\frac{\delta}{2\sqrt{2}}\right)$. The results are tabulated in Tables 5.1 and 5.2.

In Fig. 5.5(a), we show the extractable secure random bits for different digitization n under the confidence interval of $5\sigma_E \leq |e+\Delta| \leq 20\sigma_E$. At the high QCNR regime, the classical noise contribution does not compromise the extractable bits too much. As the classical noise gets more and more comparable to the quantum noise, although more bits have to be discarded, one can still extract a decent amount of secure random bits. More surprisingly, even if the QCNR goes below 0, that is, classical noise becomes larger than quantum noise, in principle, one can still obtain a nonzero amount of random

Table 5.1: Optimized $H_{\min}(M_{\text{dis}}|E)$ (and R) for an 8-bit ADC

QCNR (dB)	$\lvert e+\Delta\rvert$				
	0	$5\sigma_E$	$10\sigma_E$	$15\sigma_E$	$20\sigma_E$
∞	7.03 (2.45)	7.03 (2.45)	7.03 (2.45)	7.03 (2.45)	7.03 (2.45)
20		6.79 (2.90)	6.58 (3.35)	6.40 (3.81)	6.23 (4.27)
10		6.37 (3.88)	5.91 (5.35)	5.55 (6.85)	5.26 (8.36)
0		5.50 (7.10)	4.75 (11.92)	4.25 (16.82)	3.88 (21.75)
-∞		0	0	0	0

Table 5.2: Optimized $H_{\min}(M_{\text{dis}}|E)$ (and R) for a 16-bit ADC

QCNR (dB)	$\lvert e+\Delta\rvert$				
	0	$5\sigma_E$	$10\sigma_E$	$15\sigma_E$	$20\sigma_E$
∞	14.36 (3.90)	14.36 (3.90)	14.36 (3.90)	14.36 (3.90)	14.36 (3.90)
20		14.20 (4.38)	14.05 (4.85)	13.91 (5.33)	13.79 (5.81)
10		13.89 (5.40)	13.53 (6.92)	13.25 (8.46)	13.00 (9.99)
0		13.20 (8.70)	12.56 (13.59)	12.12 (18.51)	11.77 (23.45)
-∞		0	0	0	0

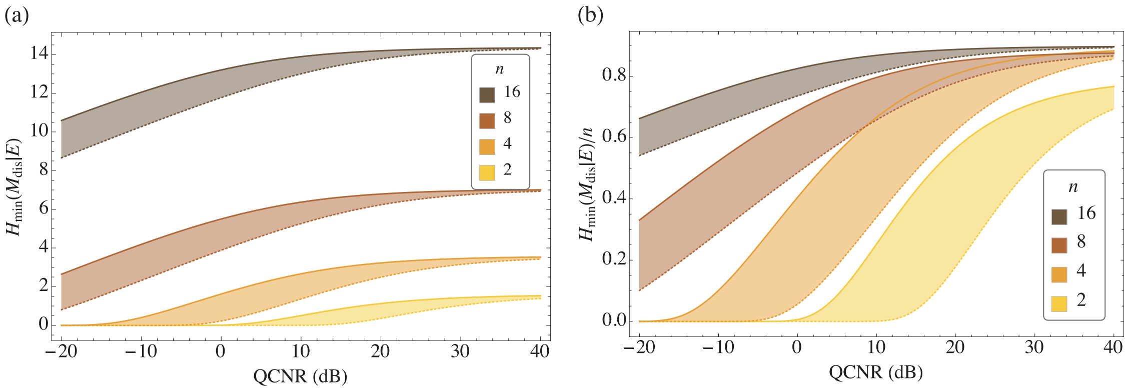


Figure 5.5: (a) Optimized $H_{\min}(M_{\text{dis}}|E)$ and (b) normalized $H_{\min}(M_{\text{dis}}|E)$ as a function of QCNR for different n-bit ADCs. Shaded areas: $5\sigma_E \leq |e+\Delta| \leq 20\sigma_E$. The extractable bits are robust against the excursion of the classical noise, especially when the QCNR is large. A non-zero amount of secure randomness is extractable even when the classical noise is larger than the quantum noise. The extractable secure randomness per bit increases as the digitization resolution n is increased.

bits that are independent of classical noise. From Fig. 5.5(b), we notice the extractable secure randomness per bit increases as we increase the digitization resolution n. This interplay between the digitization resolution n and QCNR is further explored in Fig. 5.6, where normalized $H_{\min}(M_{\text{dis}}|E)$ is plotted against n for several values of QCNR. We can see that for higher ratios of quantum-to-classical-noise, a lesser amount of digitization resolution is required to achieve a certain value of secure randomness per bit. In other words, even if QCNR cannot be improved further, one can achieve a higher ratio of secure randomness per bit simply by increasing n.

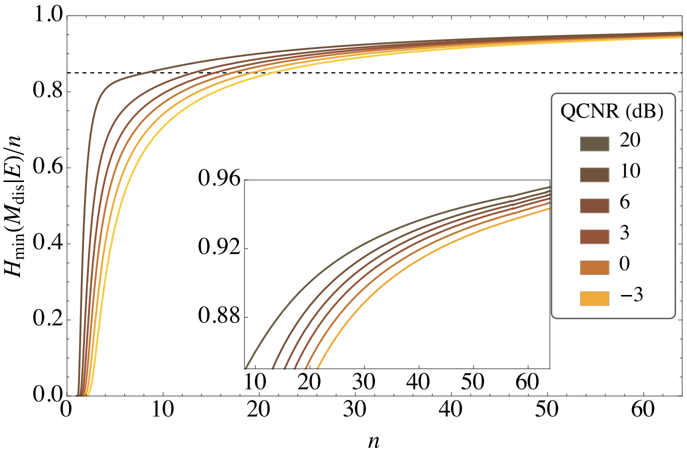


Figure 5.6: Normalized worst-case conditional min-entropy $H_{\min}(M_{\text{dis}}|E)$ as a function of n-bit ADC for different QCNR values. $|\Delta| = 0$ and $|e| \leq 5\sigma_E$. The interplay between the QCNR and digitization resolution n is shown, where one can improve the rate of secure randomness per bit either by improving the QCNR or increasing n. Inset: Zoom in for $H_{\min}(M_{\text{dis}}|E)/n \geq 0.85$ (dashed line). Even when the classical noise is more dominating compared to the quantum noise (QCNR= -3 dB), 85 % of the randomness per bit can be recovered by having at least approximately 22 bits of digitization.

5.2.2 Average conditional min-entropy

As described in Section 5.2.1, without a bound on the range of classical noise, one cannot extract any secure randomness. However, if we assume that an adversary can only listen to, but has no control over the classical noise, the extractable secure randomness from our device is then quantified by the average conditional min-entropy

$$\bar{H}_{\min}(M_{\text{dis}}|E_{\text{dis}}) = -\log_2 P_{\text{guess}}(M_{\text{dis}}|E_{\text{dis}}). \tag{5.12}$$

where $P_{\text{guess}}(M_{\text{dis}}|E_{\text{dis}})$ is defined in Eq. 4.12.

Binning of electronic noise - from eavesdropper's perspective

From Eq. (5.2), the discretized electronic noise distribution on the eavesdropper's ADC with dynamical range R_e and digitization n_e is given by

$$P_{E_{\text{dis}}}(e_j) = \begin{cases} \int_{-\infty}^{-R_e+\delta_e/2} p_E(e)\text{d}e, & j = j_{\min}, \\ \int_{e_j-\delta_e/2}^{e_j+\delta_e/2} p_E(e)\text{d}e, & j_{\min} < j < j_{\max}, \\ \int_{R_e-3\delta_e/2}^{\infty} p_E(e)\text{d}e, & j = j_{\max}, \end{cases} \tag{5.13}$$

where $\delta_e = R_e/2^{n_e-1}$ is the corresponding bin width. In order to achieve the lower bound of the average conditional min-entropy described in Eq. (5.12), we imagine that the eavesdropper possesses a device with infinite dynamical ADC range and digitization bits, i.e. $R_e \to \infty$ and $n_e \to \infty$. As $R_e \to \infty$, the first and last cases in Eq. (5.13) can be discarded, and we are left with

$$P_{E_{\mathrm{dis}}}(e_j) = \int_{e_j-\delta_e/2}^{e_j+\delta_e/2} p_E(e)\mathrm{d}e. \tag{5.14}$$

To evaluate the expression for the discretized conditional probability distribution, we make use of the mean value theorem stated below:

Theorem 1 *Mean value theorem: For any continuous function $f(x)$ on an interval $[a,b]$, there exists some $\bar{x} \in [a,b]$ such that,*

$$\int_a^b f(x)\mathrm{d}x = (b-a)f(\bar{x}). \tag{5.15}$$

By invoking Theorem 1, there exists $\bar{e}_j \in [e_j - \delta_e/2, e_j + \delta_e/2]$ such that Eq. (5.14) can be written as

$$P_{E_{\mathrm{dis}}}(e_j) = p_E(\bar{e}_j)\delta_e. \tag{5.16}$$

Substituting this back to Eq. (4.12), we end up with

$$\begin{aligned} &P_{\mathrm{guess}}(M_{\mathrm{dis}}|E_{\mathrm{dis}}) \\ &= \left[\sum_{e_j \in E_{\mathrm{dis}}} p_E(\bar{e}_j)\delta_e \max_{m_i \in M_{\mathrm{dis}}} P_{M_{\mathrm{dis}}|E_{\mathrm{dis}}}(m_i|e_j) \right]. \end{aligned} \tag{5.17}$$

Assuming an infinite binning $\delta_e \to 0$, the sum becomes an integral,

$$\begin{aligned} &P_{\mathrm{guess}}(M_{\mathrm{dis}}|E) \\ &= \lim_{\delta_e \to 0} P_{\mathrm{guess}}(M_{\mathrm{dis}}|E_{\mathrm{dis}}) \\ &= \left[\int_{-\infty}^{\infty} p_E(e) \max_{m_i \in M_{\mathrm{dis}}} P_{M_{\mathrm{dis}}|E}(m_i|e)\mathrm{d}e \right]. \end{aligned} \tag{5.18}$$

Together with Eq. (5.6), we finally arrive at

$$\begin{aligned} &P_{\mathrm{guess}}(M_{\mathrm{dis}}|E) \\ &= \left[\int_{-\infty}^{\infty} p_E(e) \max_{m_i \in M_{\mathrm{dis}}} P_{M_{\mathrm{dis}}|E}(m_i|e) de \right] \\ &= \frac{1}{2} \left(\int_{-\infty}^{e_1} P_e(e) \left[1 - \mathrm{erf}\left(\frac{e + R - \delta/2}{\sqrt{2}} \right) \right] \mathrm{d}e \right. \\ &+ \left[\mathrm{erf}\left(\frac{e_2}{\sqrt{2}\sigma_E} \right) - \mathrm{erf}\left(\frac{e_1}{\sqrt{2}\sigma_E} \right) \right] \mathrm{erf}\left(\frac{\delta}{2\sqrt{2}} \right) \\ &+ \left. \int_{e_2}^{\infty} P_e(e) \left[\mathrm{erf}\left(\frac{e - R + 3\delta/2}{\sqrt{2}} \right) + 1 \right] \mathrm{d}e \right), \end{aligned} \tag{5.19}$$

where e_1 and e_2 are chosen to satisfy the maximization upon M_{dis} for a given R. The optimal R is then determined numerically. This result can be easily generalized to take into account a DC offset with the steps described in Sec. 5.2.1, giving

$$
\begin{aligned}
&P_{\text{guess}}(M_{\text{dis}}|E)\\
&=\frac{1}{2}\Bigg(\int_{-\infty}^{e_1} p_E(e-\Delta)\left[1-\operatorname{erf}\left(\frac{e+\Delta+R-\delta/2}{\sqrt{2}}\right)\right]\mathrm{d}e\\
&+\left[\operatorname{erf}\left(\frac{e_2-\Delta}{\sqrt{2}\sigma_E}\right)-\operatorname{erf}\left(\frac{e_1-\Delta}{\sqrt{2}\sigma_E}\right)\right]\operatorname{erf}\left(\frac{\delta}{2\sqrt{2}}\right)\\
&+\int_{e_2}^{\infty} p_E(e-\Delta)\left[\operatorname{erf}\left(\frac{e+\Delta-R+3\delta/2}{\sqrt{2}}\right)+1\right]\mathrm{d}e\Bigg).
\end{aligned}
\tag{5.20}
$$

Here, we again assume that the eavesdropper can measure the full spectrum of the classical noise, with arbitrary precision. This gives the eavesdropper maximum power, including an infinite ADC range $R_e \to \infty$ and infinitely small binning $\delta_e \to 0$. As detailed in Appendix 5.2.2, under these limits, Eq. (5.12) takes the form of

$$
\begin{aligned}
&\bar{H}_{\min}(M_{\text{dis}}|E)\\
&=\lim_{\delta_e\to 0}\bar{H}_{\min}(M_{\text{dis}}|E_{\text{dis}})\\
&=-\log_2\left[\int_{-\infty}^{\infty} P_E(e)\max_{m_i\in M_{\text{dis}}} P_{M_{\text{dis}}|E}(m_i|e)\mathrm{d}e\right].
\end{aligned}
\tag{5.21}
$$

The optimized result for the average min-entropy $\bar{H}_{\min}(M_{\text{dis}}|E)$ with the corresponding

Table 5.3: Optimized $\bar{H}_{\min}(M_{\text{dis}}|E)$ (and R) for 8- and 16-bit ADCs

QCNR (dB)	$n = 8$	$n = 16$
∞	7.03 (2.45)	14.36 (3.90)
20	6.93 (2.59)	14.28 (4.09)
10	6.72 (2.93)	14.11 (4.55)
0	6.11 (4.33)	13.57 (6.48)
-∞	0	0

dynamical ADC range R is depicted in Table 5.3. Similar to the worst-case min-entropy scenario in Sec. 5.2.1, one can still obtain a significant amount of random bits even if the classical noise is comparable to quantum noise. On the contrary, a conventional unoptimized QNRG requires high operating QCNR to access the high-bitrate regime. When QCNR→ ∞, the measured signal does not depend on the classical noise and the result coincides with that of the worst-case conditional min-entropy. In fact, the worst-case conditional min-entropy (Eq. (5.5)) is the lower bound for the average conditional min-entropy (Eq. (5.12)). In the absence of side-information E, both entropies will reduce to the usual min-entropy Eq. (4.1) [92]. Compared to the worst-case min-entropy, the average conditional min-entropy is more robust against degradation of QCNR; hence, it allows one to extract more secure random bits for a given QCNR. This is expected, since in this case, we do not allow the eavesdropper to influence our device, which is a valid assumption for a trusted laboratory.

5.3 Experimental implementation

5.3.1 Physical setup and characterization

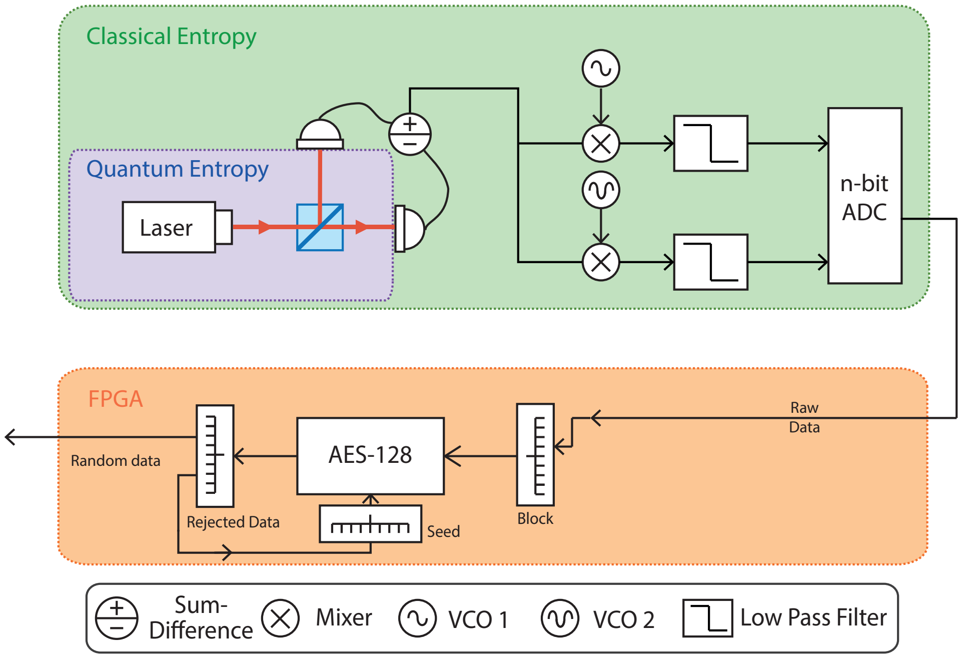


Figure 5.7: Schematic setup of CVQRNG, where a continuous-variable homodyne detection is performed on the quantum vacuum state, followed by mixing down at 1.375 GHz and 1.625 GHz. The mixing signals are generated by voltage-controlled oscillators. The dynamical ADC range of the ADC is chosen appropriately according to the QCNR and ADC digitization resolution n to maximize the extractable randomness. The raw output, which consists of both quantum and classical contributions, will be post processed by field-programmable gate array. A cryptographic hashing function (AES-128) is applied to extract secure randomness quantified by conditional min-entropy.

As depicted in Fig. 5.7, our CV-QRNG setup consists of a homodyne detection of the quantum vacuum state, or a self-homodyning (Sec. 3.3.2) followed by post-processing. We now segment our setup according to the block diagram picture (Sec. 4.2). In the quantum entropy block, a 1550-nm fibre-coupled laser (NP Photonic Rock) operating at 60 mW serves as the local oscillator of the homodyning setup. This local oscillator is sent into one port of a 50:50 beam splitter, while the other one is physically blocked and serves as the vacuum input. Entering to the classical entropy domain, the outputs are then optically coupled to a pair of balanced photodetectors with 30 dB of common-mode rejection. The intensity of the output ports are recorded over a detection bandwidth of 3 GHz. Since the local oscillator's amplitude α is significantly larger than the quantum vacuum fluctuation, the difference of the photocurrents from the pair of detectors is proportional to $|\alpha|X_v$, where X_v is the quadrature amplitude of the vacuum state. Hence, the contribution of quantum noise is essentially amplified via the balanced homodyne detection.

In order to sample the vacuum field at the spectral range where technical noise is less significant and where the laser is shot-noise limited (Fig. 5.8(a)), the electronic output is split and mixed down at 1.375 GHz and 1.625 GHz (dashed lines in Fig. 5.8(b)). The QCNR clearances are about 13 dB for both channels, which are sampled at 250 MSamples per second. The shaded region between the measured signal and classical noise indicates the available quantum randomness in our broadband 3-GHz photocurrent detectors, with an average QCNR of approximately 10 dB. The peaks in the classical signal are due to technical noise and pick-up signals from radio stations. The peak at 2.4 GHz is due to the Wi-Fi transmissions. Afterwards, low-pass filters with cutoff frequency at 125 MHz are used to minimize the correlations between the sampling points [73] (Fig. 5.8(c)). The signal is then amplified (Fig. 5.8(d)) before digitization to choose the optimal dynamical ADC range parameter R. The measured signal from two sidebands (channel 0, 1.25-1.50 GHz), and (channel 1, 1.50-1.75 GHz) are recorded using two 16-bit ADCs (National Instruments 5762) at 250 MSamples per second. Finally, the data processing is performed using a National Instruments field-programmable gate array. The average QCNR clearances for channel 0 (ch 0) and channel 1 (ch 1) are 13.52 and 13.32 dB, respectively. The noise measurements for both channel with local oscillator on (off) are depicted in Fig. 5.9. Taking into account the intrinsic dc offsets, which is $-0.02\sigma_Q$ for both channels, we quantify our conditional min-entropies using the method described in Sec. 5.2. For our ADC with 16 bits of digitization, the worst-case conditional min-entropies are 13.76 bits (ch 0) and 13.75 bits (ch 1), while the average conditional min-entropies are 14.19 bits for both channels. Here, by assuming that the eavesdropper cannot manipulate the classical noise, we evaluate our entropy with average conditional min-entropy and set R as $4.32\sigma_Q$ according to Eq. (5.20).

5.3.2 Upper bound of extractable min-entropy

The extractable randomness of our QRNG is limited by the sampling rate and the digitization resolution, which is defined by Nyquist's theorem on maximum data rate C,

$$C = 2H \log_2 V, \tag{5.22}$$

where H is the bandwidth of the spectrum and $V = 2^n$ is the quantization level for digitization resolution n. For our 16-bit ADC, the shot-noise-limited and technical-noise-free bandwidth is around 2.5 GHz out of 3 GHz. With an average of 10 dB of QCNR clearance, one can extract 14.11 bits out of 16 bits (Table 5.3). Putting these values into Eq. (5.22), with a fast enough ADC, we can potentially extract up to 70 Gbit/s random bits out of our detectors.

The maximum bitrate is ultimately upper bounded by the photon number within a given detection time window. In our setup, a 1550-nm fibre-coupled laser with a power

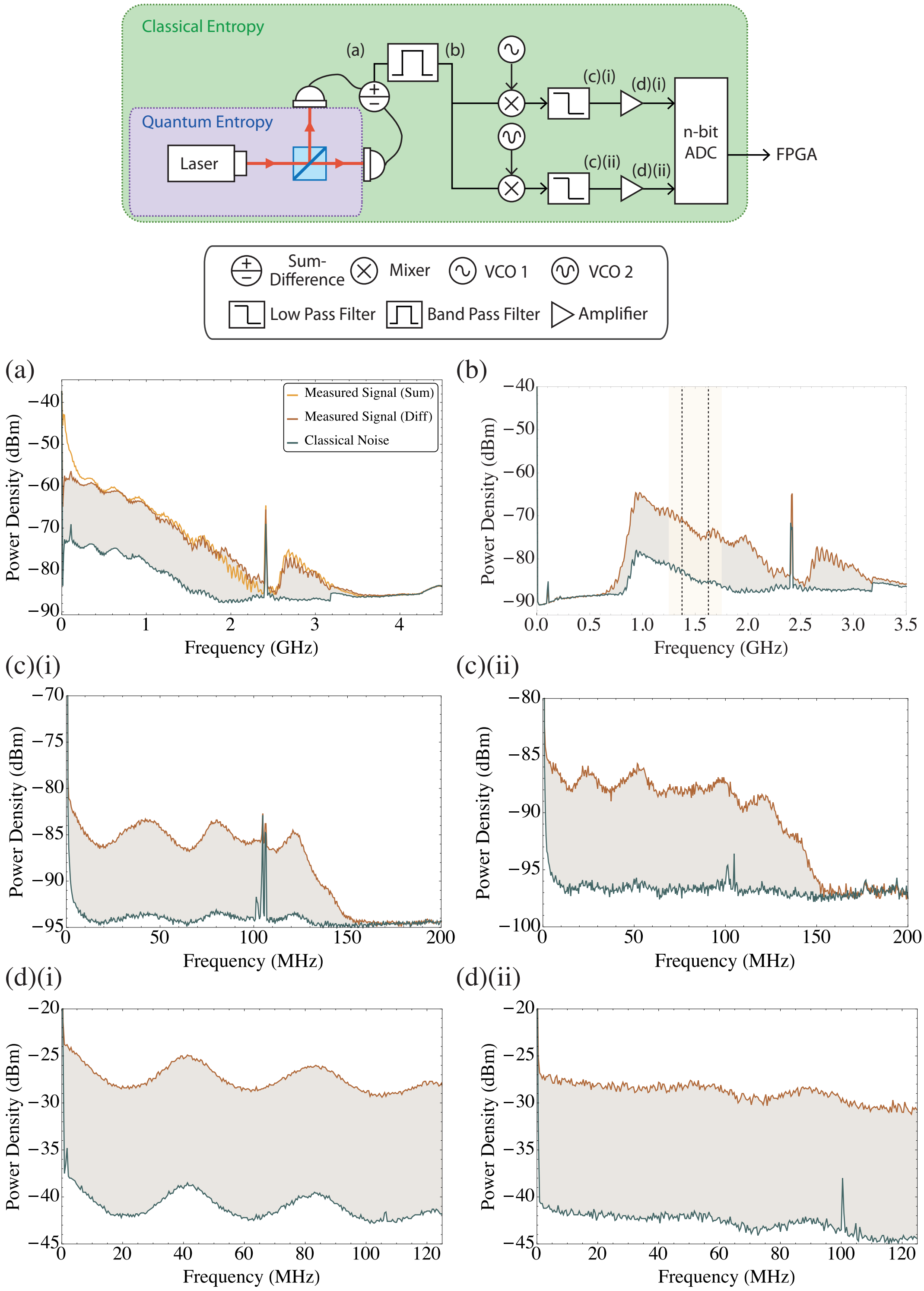


Figure 5.8: Spectral power density from the CV-QRNG at various physical stages. The resolution and video bandwidth are both 1 MHz.

of 60 mW and detection bandwidth of 3 GHz is used. This corresponds to a mean of 1.6×10^8 photons per sampling. Given a perfect photon-number-resolving detector, the maximum min-entropy is given by $-\log_2(1/\sqrt{2\pi \times 1.6 \times 10^8}) \approx 14.9$ bits. In principle,

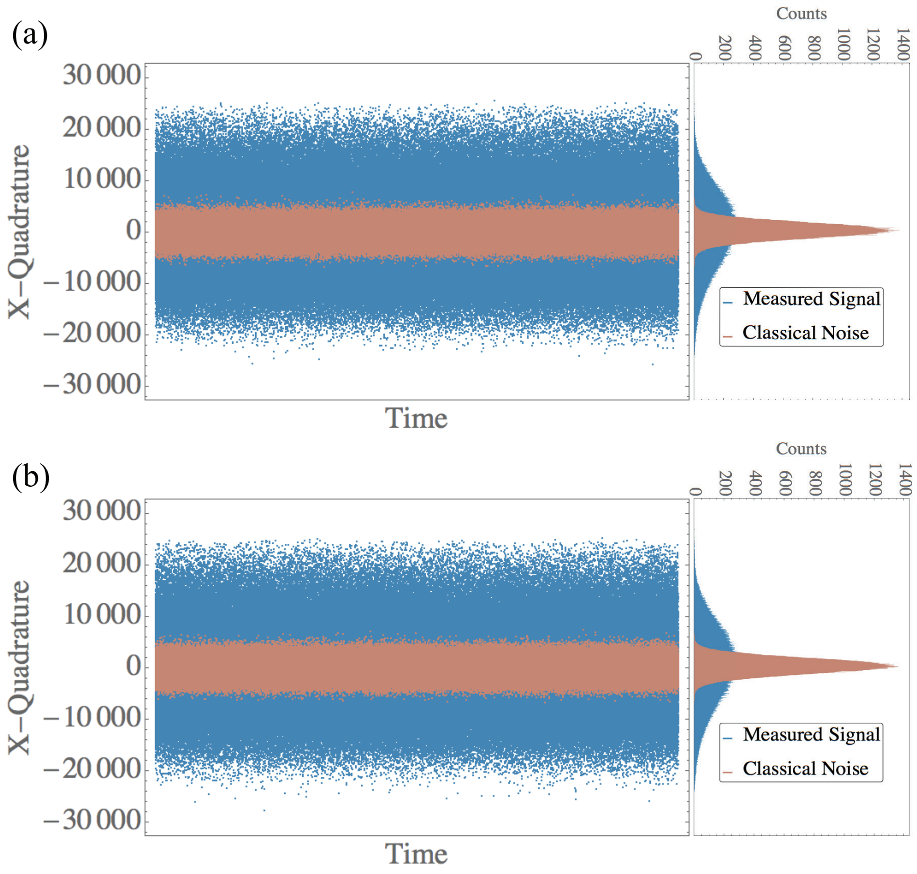


Figure 5.9: Noise measurements of (a) channel 0 and (b) channel 1 for a typical record of 5×10^5 consecutive samples. The quasi-continuous measurement outcomes of the local oscillator (blue) and electronic noise (red). Right: the resulting histograms of the LO and the electronic noise.

one can send more power to extract more random bits, however, this bound can increase only logarithmically with laser intensity.

For a finite coherent state $|\alpha\rangle$, the maximum value of $H_{\text{min}}(M_{\text{dis}}|E)$ is bounded by the number of photons available in $|\alpha\rangle$. This limit is attained when the ADC discretization is fine enough such that events between n and $n+1$ photons at the homodyne output can be distinguished (regardless of the amount of classical noise). The probability density function $p_{M|E}(m|e=0)$ is then a probability mass function having support $(n_1 - n_2)\delta_0$ where n_1 and n_2 are non-negative integers with a Poissonian distribution with mean $|\alpha|^2/2$. The normalization constant $\delta_0 = 1/|\alpha|$ sets the variance to 1. For large $|\alpha|$, the distribution $p_{M|E}(m|e=0)$ tends to a discretized Gaussian distribution with zero mean and unit variance,

$$P_{M_{\text{dis}}|E}(m|e=0) = \frac{\delta_0}{\sqrt{2\pi}} \exp\left(-m^2\right) \ , \tag{5.23}$$

for $m \in \{0, \pm\delta_0, \pm 2\delta_0, \ldots\}$. This function has a maximum value of $\delta_0/\sqrt{2\pi}$ at $m = 0$.

For an ADC discretization with bin size δ less than δ_0 and with range large enough such that the probabilities of the two end bins given e, $P_{M_{\text{dis}|E}}(m_{\text{min}}|e)$, and $P_{M_{\text{dis}|E}}(m_{\text{max}}|e)$ are less than $\delta_0/\sqrt{2\pi}$, the most likely bin given e will have a probability of $\delta_0/\sqrt{2\pi}$. The min-entropy of this distribution is then

$$\begin{aligned} H_{\min}(M_{\text{dis}}|e) &= -\log_2 \left[\max_{m \in M_{\text{dis}}} P_{M_{\text{dis}}|E}(m|e) \right] \\ &= -\log_2 \left(\frac{\delta_0}{\sqrt{2\pi}} \right) \\ &= -\log_2 \left(\frac{1}{\sqrt{2\pi}|\alpha|} \right) . \end{aligned} \tag{5.24}$$

Averaging over e, this gives the bound to the average conditional entropy as $\bar{H}_{\min}(M_{\text{dis}}|E) \leq -\log_2\left(1/\sqrt{2\pi}|\alpha|\right)$. Hence, the maximum amount randomness for a homodyning CV-QRNG is subjected to the power of the local oscillator.

5.4 Randomness Extraction with AES

Here, we demonstrate randomness extraction with the Advanced Encryption Standard (AES) [105] cryptographic hashing algorithm of 128 bits. In our QRNG, randomness extraction is performed with an AES [105] cryptographic hashing algorithm of 128 bits seeded with a 128-bit secret initialization vector. Four most significant bits of the 16-bit samples are discarded before randomness extraction to ensure low autocorrelation among consecutive samples (Fig. 5.10) before hashing. The resulting output is concatenated with partial raw data from the previous run, forming a 128-bit block for cryptographic hashing. The hashing implementation was done by Dr. Syed Assad. Since a complete cryptoanalysis of the cryptographic hashing is intricate and is out of the scope of our work, we simply discard half of the output to ensure uniformity of the generated random sequence [80]. We further strengthen our security by renewing the seed of our AES extractor with these discarded bits.

After post-processing, the final real-time guaranteed-secure random number generation rate of our CV QRNG is 3.55 Gbps. If all the available bandwidth from our detector (approximately 2.5 GHz) can be sampled, with sufficient resources, we can achieve up to 35 Gbit/s (cf. Sec. 5.3.2). This corresponds to a rate of 14 Mbps/MHz in term of bits per bandwidth. Our random numbers consistently pass the standard statistical tests (NIST [106], DieHard [81]) and the results are available on the Australian National University Quantum Random Number Server [107].

5.4.1 Summary

In this work, we propose a generic framework for secure random-number generation, taking into account the existence of classical side information, which, in principle could be manipulated or predicted by an adversary. If the adversary is assumed to have access to the classical noise, for example, the detectors' noise can be originating from pre-established values, the worst-case conditional min-entropy should be used to quantify the available secure randomness. Meanwhile, if we restrict the third party to passive eavesdropping, one can use the average conditional min-entropy instead to quantify extractable randomness. By treating the dynamical ADC range as a free parameter, we show that QCNR is not the sole decisive factor in generating secure random bits. Surprisingly, one can still extract a nonzero amount of secure randomness even when the classical noise is comparable to the quantum noise. This is done simply by optimizing the dynamical ADC range via conditional min-entropies. Such an approach not only provides a rigorous justification for choosing the suitable ADC parameter, but also largely increases the range of QCNR for which true randomness can be extracted, thus relaxing the condition of high QCNR clearance in conventional CV QRNGs. We also notice that we can increase the min-entropy per bit simply by increasing the number of digitization bits. We apply these observations to analyze the amount of randomness produced by our CV QRNG setup. Efficient cryptographic hashing functions are then deployed to extract randomness quantified by average conditional min-entropy.

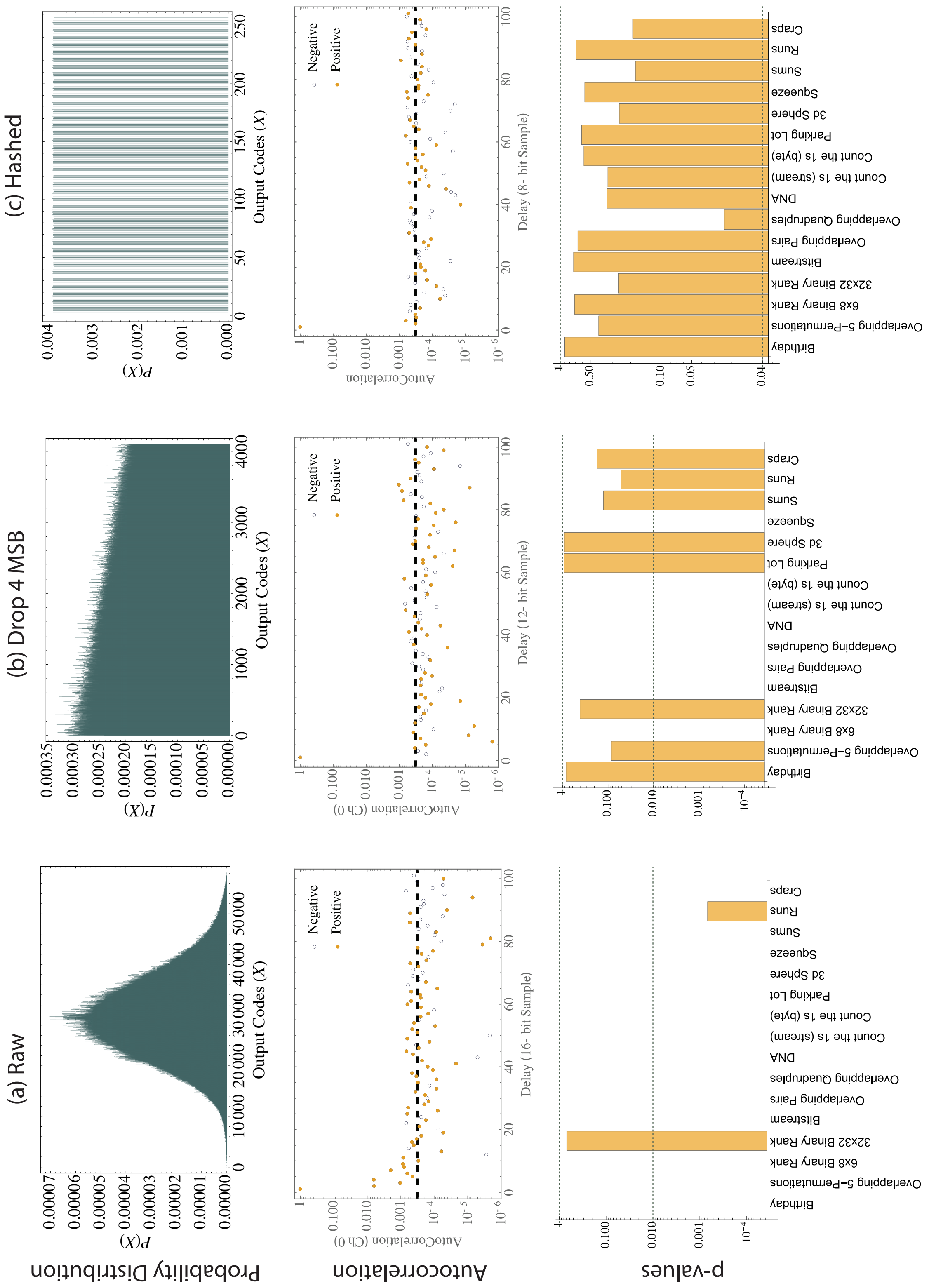


Figure 5.10: Probaility distribution, autocorrelation and p-values of the Diehard test suite for (a) raw data, (b) data with 4 MSB dropped, and (c) final hashed data, respectively for 10^7 samples. Dashed lines show the theoretical standard deviation of truly random 10^7 points. For each test in Diehard, the p-values are the result of a Kolmogorov–Smirnov test of 100 p-values. Dashed lines indicate the threshold to pass the test ($0.01 \leq p \leq 0.99$.)

Chapter 6

Experimental One-sided Device-Independent CV-QKD with Coherent States

"To live effectively is to live with adequate information."

– Norbert Wiener, *The Human Use of Human Beings*

Overview

In the context of continuous-variable (CV) QKD schemes utilizing Gaussian states and measurements, here we present a one-sided device independent protocol that requires only coherent states. A direct link between the relevant EPR steering inequality and the secret key rate is established, further strengthening the relationship between these asymmetric notions of nonlocality and device independence. We experimentally implement a coherent-state prepare-and-measured protocol, and measure the correlations necessary for 1sDI key distribution up to an applied loss equivalent to 3.5 km of optical fiber transmission. The new protocols we uncover apply the cheap and efficient hardware of CVQKD systems in a significantly more secure setting. The construction and operation of this experiment was a joint work between Sara Hosseini, Syed Assad, Jiao Geng and myself. The theoretical part was developed by Nathan Walk and Timothy Ralph from the University of Queensland and Howard Wiseman from Griffith University. The work in this chapter has resulted in the following paper:

- N. Walk, S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janousek, T. C. Ralph, T. Symul, H. Wiseman, and P. K. Lam.
  "Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution."
  Optica, 3(6), 634–642 (2016).

6.1 Introduction

Quantum mechanics promises many new opportunities for the design of communication networks, providing highly correlated resources such as entangled or even nonlocal states as well as stringent restrictions on the possible knowledge of observables, as exemplified by Heisenberg's uncertainty principle. By considering entropic versions of these uncertainty relations [108, 109] the intimate connection between entanglement and uncertainty, first uncovered in the seminal work of Einstein, Podolsky and Rosen (EPR) [110], has since begun to be formalised and quantified [111].

Both these features are of value to the would-be cryptographer as they enable protocols in which security is grounded in the laws of quantum physics, instead of the algorithmic complexity, with the most celebrated example being quantum key distribution (QKD) [112]. The earliest, and most conceptually simple, QKD schemes encode a discrete variable (DV) key in a 2-dimensional Hilbert space, as exemplified by the BB84 and Ekert 91 protocols [113, 114]. Since efficient optical implementation of these protocols involves sophisticated techniques such as the generation and detection of single photons, considerable attention has also been devoted to schemes that instead utilise the quadratures of the optical field [115, 116, 117, 118, 119] where one has access to deterministic, high-efficiency broadband sources and detectors. However, this approach is more theoretically involved, as the secret key is now a continuous variable (CV) that is encoded in states living in an infinite dimensional Hilbert space.

The challenge of realising the full promise of QKD - physically guaranteed security with minimal additional assumptions - has crystallised into two fronts. In one camp, we desire a lower bound on the extractable secret key length that allows for an arbitrarily powerful eavesdropper (Eve), with the goal of including the effects of a finite number of transmitted symbols, [120, 121, 122, 123]. In the second place, we would like to close any gaps that may exist between a theoretical QKD protocol and its practical realisation. This can equally be cast into the problem of whether or not the honest parties (Alice and Bob) have correctly characterised their experimental devices. One might expect that these gaps can only be closed on a case-by-case basis. Indeed, as various loopholes due to mischaracterised devices have been pointed out, they have usually been followed by straightforward methods for their closure. Remarkably, however, it is in principle possible to rigorously surmount even this challenge by harnessing non-local quantum correlations, and it is this second problem we tackle for the entire Gaussian family of CVQKD protocols. We have identified all protocols which can be proven secure in a one-sided device-independent (1sDI) setting, i.e. independent of the devices of either Alice or Bob (but not both), and provide a proof-of-principle experimental demonstration several protocols. Here, we will focus on one of the most practical protocols - a coherent state prepare-and-measure scheme.

6.2 Entropic uncertainty relations

Entropic relations have received a great deal of attention as a convenient and powerful information theoretic tool for investigating uncertainty in quantum systems. Originally, entropic uncertainty relations were derived assuming one starts without any additional information or at most only classical information describing the system in question, i.e. the density matrix [108, 109]. In either case, since classical information can be shared perfectly amongst arbitrarily many parties, there is little sense in thinking about these relations as applying from the perspective of one observer or another. Conversely, if observers were to share quantum correlations with the measured system, one expects the uncertainty relations to be strongly observer dependent and potentially exhibit reduced levels of uncertainty.

A generalised relation, allowing for this so-called quantum side information, was derived in [111] although only for finite dimensional Hilbert spaces and observables with a discrete spectrum. Consider a pair of observables $\{\hat{X}_A, \hat{P}_A\}$ with a complementarity $c = \max_{p_A, x_A} | \langle x_A | p_A \rangle |^2$ where $\{|x_A\rangle, |p_A\rangle\}$ are the eigenvectors of the observables. These observables are to be measured on a state A which is potentially entangled with another state, B, leading to the the following relation for the uncertainty in the pair of observables given access to B [111],

$$S(X_A|B) + S(P_A|B) \geq \log \frac{1}{c} + S(A|B). \tag{6.1}$$

Here $S(X)$ and $S(A|B)$ are the von-Neumann entropy and conditional entropies defined in Eq. (2.55) and Eq. (2.57), respectively. $S(X_A|B)$ is the conditional von Neumann entropy of the random variable, X_A upon the measurement of the *observable* $\hat{X}_A$ given knowledge of system B. This is defined as

$$S(X_A|B) = H(X_A) + \sum_{x_A} p(x_A) S(\rho_B^{x_A}) - S(B), \tag{6.2}$$

with $H(X_A)$ the Shannon entropy (Eq. (2.46)) and $\rho_B^{x_A}$ describing Bob's state conditional on Alice obtaining outcome x_A. The presence of the conditional entropy $S(A|B)$ in Eq. (6.1), which is negative for entangled states, demonstrates both the observer dependence and effect of entanglement in reducing uncertainty, as discussed briefly in Sec. 2.6.2.

Preempting applications to quantum key distribution (QKD), one can also consider that a bipartite state ρ_{AB} could have suffered some decoherence, which may be purified by an environment, or eavesdropper, such that $\rho_{AB} = \mathrm{tr}_E (|ABE\rangle \langle ABE|)$. Using the purity of the overall state ρ_{ABE}, we have $S(AB) = S(E)$, since $S(ABE) = 0$ [23]. We can recast Eq. (6.1) to find [111],

$$S(X_A|B) + S(P_A|E) \geq \log \frac{1}{c}. \tag{6.3}$$

However, these results are only valid for measurements with a finite number of discrete outcomes made on states living in a finite-dimensional Hilbert space. For the purposes of continuous variable (CV) QKD, we will require an uncertainty relation valid for infinite-dimensional Hilbert spaces and continuous-valued measurements. In particular, we are interested in homodyne measurements of the canonically conjugate quadratures $\hat{X}$ and $\hat{P}$. Just such a relation has been recently developed, building on an earlier result for discrete and finite measurements on infinite dimensional Hilbert spaces [124]. This was first extended to countably infinite measurements which could then be applied to a discretised version of a homodyne detection [125]. This lead to the following entropic uncertainty relation for homodyne detection upon infinite dimensional Hilbert spaces

$$S(X_A|B) + S(P_A|E) \geq \log 2\pi\hbar. \tag{6.4}$$

We refer our reader to Refs. [126, 125, 127] for detailed derivation.

6.3 Continuous variable quantum key distribution

The goal of quantum key distribution (QKD) is to allow two communicating parties, Alice and Bob to generate unconditionally secure secret keys. These keys can often be used in conjunction with cryptographic protocols, such as the one time pad. Unlike conventional cryptography, the secrecy of the protocol is guaranteed by the law of quantum physics, rather than algorithmic complexity. Before we move on, let us have a small digression on QKD.

6.3.1 A generic QKD protocol

A typical QKD protocol can be divided into two stages:

1. Quantum communication
   The goal of this stage for Alice and Bob is to exchange a large number of quantum states over a quantum channel. In each round, Alice encodes a classical random variable α onto a quantum system, which is sent to Bob. Bob then performs a quantum measurement on the received quantum state, thus extracting another random variable β, which is correlated with α. At the end of the quantum phase, Alice and Bob end up with a set of correlated raw data, or *raw keys*.

2. Classical post-processing
   The objective of this phase is to map the raw keys into shared key known only to Alice and Bob. This phase is further divided into several steps: parameter estimation, information reconciliation and privacy amplification. First, in parameter estimation, the quantum channel is characterized by having Alice and Bob publicly declare and compare a random subset of their data. This in turn allows them to bound the advantage any potential eavesdropper has. The second phase of

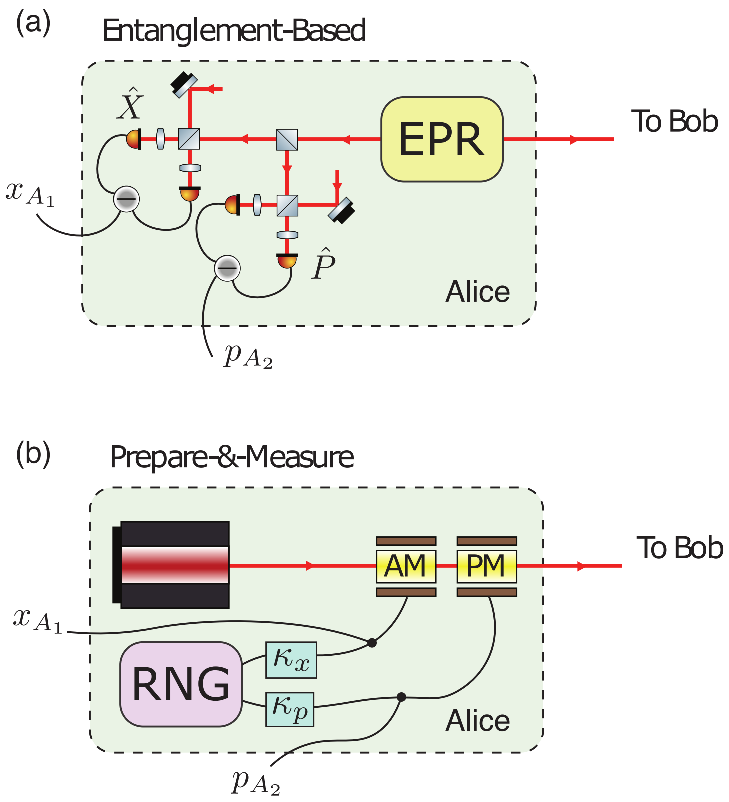


Figure 6.1: An entanglement-based scheme (with heterodyning) is equivalent to a prepare-and-measure scheme (with coherent states).

information reconciliation is essentially error correction. By having either Alice or Bob sending corrections to the other party, the communicating parties can establish bit strings with an arbitrarily high correlation. However, such a bit string might still be known partially by Eve. Therefore, in the last step, Alice and Bob perform privacy amplification, which is based on universal hashing functions to distil the final secret key, which is shorter in length, but has the advantage that Eve now knows almost nothing about the key.

6.3.2 CV-QKD protocols

The most common CV-QKD protocols are Gaussian protocols which encode information in the quadratures of the optical field. In a prepare-and-measure scheme (P&M), one can prepare squeezed [115, 116] or coherent [119] states, and measure with either homodyne detection (switching between quadratures) or heterodyne detection [128] (where both quadratures are measured simultaneously). Alternatively, one could also use entanglement-based (EB) schemes where two squeezed beams are used to create Gaussian EPR-correlated states (EPR states) [117]. An equivalence between these EB schemes and the P&M approaches has been established in a device-dependent scenario [129]. Here, we now discuss briefly such a case for coherent state.

For the entanglement-based scheme, consider a two mode EPR state with symmetric noise variance $V_x = V_p$ in Alice's station (Fig. 6.1 (a)). By measuring the conjugate quadratures $\hat{X}$ and $\hat{P}$ simultaneously on one arm with heterodyne detection (Sec. 3.3.2), Alice projects the state over the other arm into a Gaussian state with a conditional covariance matrix [24]

$$\gamma_{B|x_{A_1},p_{A_2}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{6.5}$$

and mean vector

$$d_{B|x_{A_1},p_{A_2}} = d_B = \begin{pmatrix} \frac{x_{A_1}}{\kappa_x} \\ \frac{p_{A_2}}{\kappa_p} \end{pmatrix}. \tag{6.6}$$

Here, $\kappa_x = \sqrt{\frac{V_x+1}{2(V_x-1)}}$ and $\kappa_x = -\kappa_p$. We thus see that upon Alice's measurement, the quantum state to be sent to Bob is projected into a coherent state. This is equivalent to a P&M scheme in Fig. 6.1(b), where Alice modulates a pair of electro-optical modulators by picking up the pair $(x_{A_1}/\kappa_x, p_{A_2}/\kappa_p)$ from a bivariate Gaussian distribution of variance $V_S = V_x - 1$. Alice further rescales her data by multiplying the modulating signal $\kappa_{x(p)}$, thus keeping a set of (x_{A_1}, p_{A_2}) as record. The variance of the mean of the coherent state d_B is

$$\langle \Delta^2 d \rangle = V_x - 1 = V_S, \tag{6.7}$$

which is indeed the variance of the modulation signal for the P&M protocol. A similar analysis can be done for squeezed state by having a homodyne detection for the EB scheme. Since the EB representation is a powerful theoretical tool to study many other QKD protocols, while the P&M protocol is easy to implement, the equivalence between them is extremely convenient.

In CV-QKD, for the information reconciliation phase, Alice and Bob can use either a direct reconciliation (DR) scheme where Alice sends corrections to Bob; or a reverse reconciliation (RR) [118], where Bob sends corrections to Alice. However, only the RR protocols allow for losses above 50%, although one can also achieve this loss-tolerance via post-selection, which discards some of the keys in order to retain a more correlated subset [130].

6.4 CV-QKD using entropic uncertainty relations

Previous works have proved the security of Gaussian CV-QKD in the asymptotic limit up to the level of collective attacks, via the Gaussian extremality of relevant quantities [131, 132]. The proofs were eventually raised to the level of the most general coherent attacks by use of the de Finetti theorem adapted to infinite dimensions [133], which shows that collective attacks are in fact optimal. Consequently, one can asymptotically lower bound the secret key rate by considering only Gaussian collective attacks.

In the following, we conduct our analysis in the EB picture, and the variances appearing are those that would be directly measured in an EB implementation. We will calculate the key rate encoded in the $\hat{x}$ basis on a particular run. Overall, the total key rate will be the average of the quantities derived here and the analogous expression for encoding in the $\hat{p}$ basis.

We consider a DR for coherent state protocol discussed in Sec X, which in the EB picture involves Alice making a heterodyne detection upon her arm of an EPR pair. Thus she first mixes her mode with vacuum resulting in two modes A_1 and A_2 upon which she measured $\hat{x}$ and $\hat{p}$ respectively. Bob then makes a homodyne detection, randomly switching between the quadratures. We will consider the case where Bob measures $\hat{X}$, with the other case following straightforwardly. The DR key rate is then bounded by [131, 132],

$$K^{\triangleright} \geq I(X_{A_1} : X_B) - \chi(X_{A_1} : E), \tag{6.8}$$

where $I(X_{A_1} : X_B) = h(X_{A_1}) - h(X_{A_1}|X_B)$ denotes the classical mutual information between Alice and Bob (Eq. (2.54)), with $h(X) = -\int \mathrm{d}x \;\, p(x) \log p(x)$ being the continuous Shannon entropy of the measurement strings and

$$\chi(X_{A_1} : E) = S(E) - \int \mathrm{d}x_{A_1} \;\, p(x_{A_1}) S(E|x_{A_1}) \tag{6.9}$$

is the continuous Holevo bound (Eq. 2.62).

Expanding Eq. 6.8 and comparing with the continuous conditional von Neumann entropy

$$S(X_{A_1}|B) = h(X_{A_1}) + \int \mathrm{d}x_{A_1} p(x_{A_1}) S(\rho_B^{x_{A_1}}) - S(B), \tag{6.10}$$

we have

$$\begin{aligned} K^{\triangleright} &\geq h(X_{A_1}) + \int \mathrm{d}x_{A_1} \;\, p(x_{A_1}) \;\, S(\rho_E^{x_{A_1}}) - S(E) - h(X_{A_1}|X_B) \\ &= S(X_{A_1}|E) - h(X_{A_1}|X_B), \end{aligned} \tag{6.11}$$

which is what one would expect from the Devetak-Winter relations [134]. The entropic uncertainty relation derived in Sec. 6.2 now comes to play. Using Eq. (6.4), we can bound the eavesdropper's information on the relevant observable as follows:

$$S(X_{A_1}|E) \geq \log 2\pi\hbar - S(P_{A_1}|E). \tag{6.12}$$

It can be shown that $S(P_{A_1}|B) \leq S(P_{A_1}|P_B) = h(P_B|P_{A_1})$. We thus can write

$$S(X_{A_1}|E) \geq \log 2\pi\hbar - h(P_{A_1}|E). \tag{6.13}$$

Substituting Eq. (6.13) into Eq. (6.11), and setting $\hbar = 2$, we can write

$$K^{\triangleright} \geq \log 4\pi - h(X_{A_1}|X_B) - h(P_{A_1}|P_B). \tag{6.14}$$

Now this formula might pose a problem, in that we do not measure $\hat{P}$ upon mode A_1.

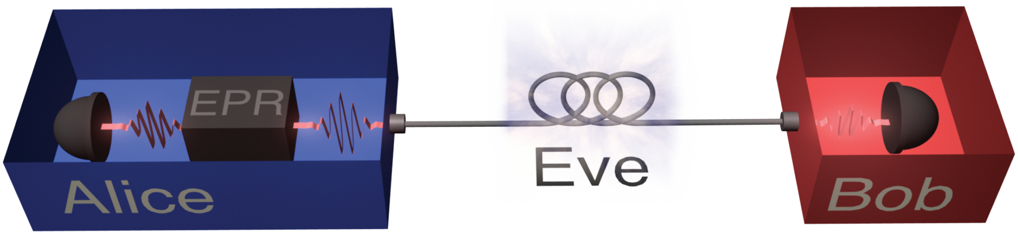


Figure 6.2: Conceptual picture of a 1sDI-CVQKD protocol. From the perspective of Alice (Bob) the local devices are known and allow a secret key to be extracted from a direct (reverse) reconciliation protocol, even though the other party exists only as an unknown red (blue) box.

Nevertheless, this can be circumvented if we can trust the devices, specifically the beam splitter in Alice's station, i.e. Alice is performing a true dual-homodyning. Furthermore, one can show via a variational calculation that for any probability distribution $p(x)$, the corresponding Shannon entropy is maximised for a Gaussian distribution of the same variance. In other words, Alice and Bob can bound their secret key rate for this protocol by measuring Bob's conditional variances. Thus, we can substitute the Shannon entropy for a Gaussian distribution, i.e. $h_G(X_B|X_{A_1}) = \log\sqrt{2\pi e V_{X_B|X_{A_1}}}$, where $V_{X_B|X_{A_1}} = V_{X_B} - \langle X_{A_1} X_B \rangle^2 / V_{X_{A_1}}$ is Bob's variance conditional on Alice's measurement. By trusting Alice's beam splitter, we have $V_{P_{A_1}|P_B} = V_{P_{A_2}|P_B}$, hence $h_G(P_{A_1}|P_B) = h_G(P_{A_2}|P_B)$ which is directly measured. We therefore have,

$$\begin{aligned} K^{\triangleright} &\geq \log 4\pi - \log\sqrt{2\pi e V_{P_{A_2}|P_B}} - \log\sqrt{2\pi e V_{X_{A_1}|X_B}} \\ &= \log\frac{2}{e\sqrt{V_{X_{A_1}|X_B} V_{P_{A_2}|P_B}}}, \end{aligned} \tag{6.15}$$

where the key rate is now bounded only by the conditional variances. Note that for positive key we now require the condition $V_{X_{A_1}|X_B} V_{P_{A_2}|P_B} \leq 0.55$. Equation (6.15) can be generalised to include imperfect reconciliation efficiency β (Appendix B), giving

$$K^{\triangleright} \geq \beta \log\sqrt{\frac{V_{X_{A_1}}}{V_{X_{A_1}|X_B}}} + \log\frac{2}{e\sqrt{V_{X_{A_1}} V_{P_{A_2}|P_B}}}. \tag{6.16}$$

6.5 One-sided DI CV-QKD protocol for P&M scheme

An important benefit of utilising entropic uncertainty relations in QKD proofs is that they lend themselves towards one-sided device-independent (1sDI) protocols [135, 136]. These are relaxed versions of fully the DI schemes [137, 138, 139] in which all devices are untrusted and the security is guaranteed via a detection-loophole-free Bell violation. In the following, we will discuss briefly the notion of device independence in QKD, and its connection to EPR steering, an asymmetric form of non-locality.

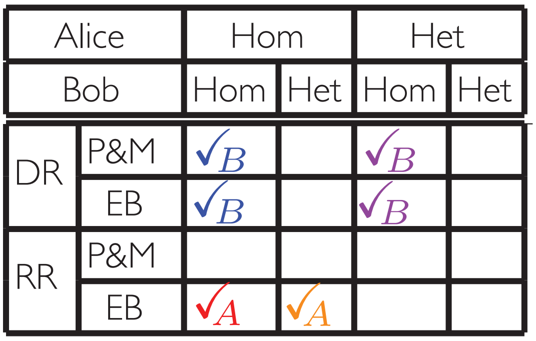
6.5.1 One-sided device-independent QKD

A fully device-independent (DI) protocol operates under the assumption that an eavesdropper, Eve, has full access over all the experimental devices. The security of such protocol is guaranteed by the concept of Bell non-locality and the exclusion of local hidden variable (LHV) models [140, 137, 138, 139, 141, 142]. While a tamper-proof protocol is desirable, these schemes are extremely experimentally challenging as they require the implementation of a detection-loophole-free Bell test [143, 144, 14, 12]. This implies that they are also beyond the reach of purely Gaussian protocols as it is impossible to violate a Bell inequality utilising only Gaussian resources [145].

More recently, an intermediate, asymmetric form of non-locality quantifier known as *EPR-steering* has been identified. This which allows Alice or Bob to exclude an LHV explanation of their correlated measurement outcomes [146]. A natural question to ask is whether there exist analogous cryptographic results, where only one party's devices are untrusted. This possibility, first noted in Ref. [135] was subsequently developed to prove the security of experimentally difficult, but feasible, proposals for one-sided device-independent (1sDI) DVQKD protocols which were explicitly linked to the corresponding EPR steering inequality [136].We note that this should not be confused with the distinct concepts of measurement-device-independent QKD, in which both Alice and Bob use trusted sources to generate a key via an untrusted measurement in the middle [147, 148, 149, 150, 151].

For 1sDI-QKD protocols only one side, Alice or Bob, is untrusted and regarded as a black box while the other is assumed to involve a particular set of quantum operations (Fig. 6.2). The 1sDI nature of these entropic proofs is manifested in the secure key rate (Eq. (6.15)), in that it depends only upon measuring a known observable upon one side. For instance, in deriving Eq. (6.15), only the knowledge of Bob's measurement ($\hat{X}_B$ or $\hat{P}_B$) is required in order to apply the entropic uncertainty relation. Even though we have the conditional expressions such as $V_{X_B|X_A}$ in the key rate equation Eq. (6.15), Alice could be making any measurement and the aforementioned bound will still holds.

As such, in the EB picture, any positive key predicted via the entropic uncertainty relation involving homodyning of EPR states is by definition 1sDI, independent of Alice for RR and Bob for DR [122, 123]. However this device-independence does not necessarily extend to the protocols involving heterodyne detection as that would amount to the characterisation of the devices used in the detection. Therefore, employing a heterodyne detection on the supposedly untrusted side immediately invalidates the device-independence. Nonetheless the remaining protocols, with the heterodyne detection taking place in the trusted station, are still implementable with high-efficiency sources and detection opening the way to several 1sDI-CVQKD protocols with current technology. This means that for EB protocols both DR and RR may be 1sDI provided all parties are homodyning, while Bob may safely heterodyne for an RR protocol and Alice may heterodyne for a DR protocol. Finally, for DR protocols where Alice (who controls the source) is trusted, we may also safely make the equivalence between P&M and EB schemes. Remarkably, this means that for direct reconciliation it is possible to generate 1sDI key using only coherent states. We summarise which of the 16 possible Gaussian protocols are potentially 1sDI in Table inset in Fig. 6.3.



Alice		Hom		Het	
Bob		Hom	Het	Hom	Het
DR	P&M	✓B		✓B	
	EB	✓B		✓B	
RR	P&M				
	EB	✓A	✓A		

Figure 6.3: Summary of 1sDI-CVQKD protocols where subscript A (B) indicates independence of Alice's (Bob's) devices.

6.5.2 Connection to EPR steering

In the earlier discrete variable work, a clear conceptual link was made between DI DV protocols and Bell non-locality [137]. Our intuition that the 1sDI DV protocols should be analogously related to the corresponding asymmetric form of non-locality, EPR steering, was confirmed by Branciard et al.Ṫhey showed that the condition for their protocol achieving a positive key was indeed equivalent to a steering inequality [136].

For continuous variable, where Gaussian states and Gaussian measurements are involved, steering is traditionally demonstrated by a violation of a condition on the conditional variances. In particular, we must violate the so called EPR paradox criteria proposed by Reid [152]

$$\mathcal{E}_{\blacktriangleright} := V_{X_B|X_A} V_{P_B|P_A} \geq 1, \tag{6.17}$$

for Alice to provably steer Bob as indicated by the right black triangle and similarly with A and B interchanged [146] and the arrow reversed. Comparison with Eq. (6.15) shows that we can write the key directly in terms of the steering parameter,

$$K^{\triangleright} \geq \log\left(\frac{2}{e\sqrt{\mathcal{E}_{\blacktriangleleft}}}\right), \tag{6.18}$$

where $\mathcal{E}_{\blacktriangleleft} = V_{X_{A_1}|X_B} V_{P_{A_2}|P_B}$ for our DR key rate with Alice heterodyning and Bob homodyning. We see that $K^{\triangleright} > 0$ if and only if $\mathcal{E}_{\blacktriangleleft} < \left(\frac{2}{e}\right)^2 \approx 0.55$, with the identical relation between the DR key rate and $\mathcal{E}_{\blacktriangleleft}$ following straightforwardly. In other words, the condition for a positive one-sided device-independent key is more stringent than the violation of EPR steering $\mathcal{E}_{\blacktriangleleft} \geq 1$, similarly to the case for 1sDI-DVQKD [136].

Remarkably, this connection hence gives us an operational interpretation for the Reid product of conditional variances [152] as being directly related to the number of secure 1sDI bits extractable from Gaussian states with Gaussian measurements. This is a particularly pragmatic cryptographic interpretation, in addition to previous work highlighting the links between steering and one-sided device independence in quantum teleportation [153] and secret sharing [154].

6.5.3 Experimental implementation

In this section, we discuss the experimental details, imperfections and modelling of the experiment with coherent states and homodyne measurements.

Experimental setup

A quantum noise limited 1064 nm laser was used in the experiment. A small portion of it was passed through a pair of phase and amplitude electro-optic modulators (EOMs). EOMs were used to provide a Gaussian distributed modulation on both amplitude and phase quadrature. Each EOM was driven by an independent function generator, providing a broadband white noise signal up to 10 MHz. The magnitude of white noise was set to provide almost the same displacement on each quadrature, i.e. the noise variance $V_x = V_p$. Outputs of function generators were divided into two. One part was sent to drive the EOMs and the other was recorded. This modulation record, after calibration, was Alice's data since she had control over the source [1].

The modulated beam was then sent through a lossy channel to Bob. To model the lossy channel, a vacuum state was introduced to the system and was mixed with the Bob's mode on a beam splitter of transmission T (Eq. (3.18)). Upon receiving his mode, Bob performed a homodyne measurement, alternating between conjugate quadratures. An electronic delay was introduced to Alice's and Bob's data to gain the maximum correlation between them at 3.5-4.5 MHz.

When the homodyne detector was locked to the phase (amplitude) quadrature, there was 30 (37) dB suppression of cross correlation between orthogonal quadratures, indicating that our modulators were well aligned. Our pair of detectors, both with dark noise clearance of 18 dB, were balanced electronically, providing 30 dB of common mode rejection. Our homodyne efficiency was around 95% with fringe visibility of 98%, limited by the mode distortions introduced by the EOMs. The photodiode's quantum efficiency was estimated to be around 98.5%. 4×10^6 data points were sampled at 25×10^6 samples per second utilizing a digital data acquisition system. The process was repeated

[1] Here, calibration means determining the relationship between the function generator output and the phase space displacement as measured before transmission.

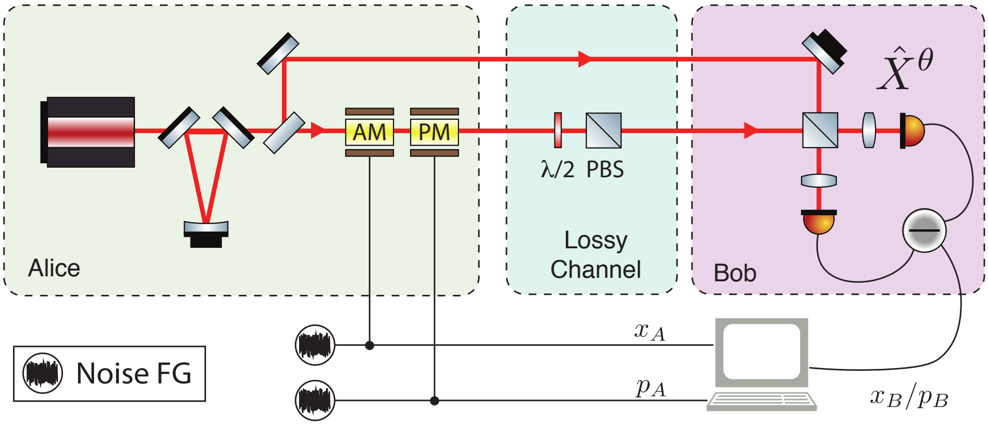


Figure 6.4: Schematic diagram of P&M coherent state experiment: AM and PM are electro-optic modulators (EOMs) driven by function generators (FG), which in turn provided a Gaussian distributed displacement of the vacuum state in amplitude and phase quadratures. The resulting coherent states were then sent to Bob through a lossy channel (simulated by a half waveplate followed by a polarising beam splitter) where he performed a homodyne measurement $\hat{X}^\theta$.

five times in order to provide sufficient statistics for each data points. These data were then digitally filtered to 3.5-4.5 MHz.

In order to find the maximum range over which the protocol provides secure communication, the optimal modulation variance for each value of the channel transmission has to be identified. This is done by scanning the modulation variance over a range of 2 to 19 times the shot noise. As discussed in Sec. 6.3.2, by rescaling Alice's recorded signal, the key rates can be calculated using Eq. (6.16) with reconciliation coefficient set to 0.95.

Modelling

To highlight the relative advantages of the coherent state source, consider the covariance matrix of the equivalent two mode EPR state:

$$\mathrm{EPR}(s) = \begin{pmatrix} \cosh(2s) & 0 & \sinh(2s) & 0 \\ 0 & \cosh(2s) & 0 & -\sinh(2s) \\ \sinh(2s) & 0 & \cosh(2s) & 0 \\ 0 & -\sinh(2s) & 0 & \cosh(2s) \end{pmatrix}, \tag{6.19}$$

where s is the squeezing parameter which is related to the modulation variance via $\cosh(2s) = V_S + 1$. To model the prepare & measure experiment, we remain in the equivalent EB picture and begin with $\gamma_{\text{in}} = \mathrm{EPR(s)}$. We recall that this equivalent picture consists of Alice heterodyning a part of the EPR state, and send the other part to Bob through a lossy channel (Sec. 6.3.2). Although being more robust, the coherent state P&M setup naturally still suffers from imperfections, which in turn effect the optimum modulation. These imperfect correlations arise partly from the cross correlation between orthogonal quadratures and partly from our limited ability to maximize the correlation between Alice and Bob's modes using electronic delay. Both phenomena can be regarded as an unknown rotation in the system. To model these deviations from ideal case, a rotation operator with small angles is applied to the $\hat{X}$ and $\hat{P}$ quadratures of the second mode (Bob's mode).

The channel transmission, T, can be determined directly by taking the ratio of the correlation at a particular setting with the correlation at full transmission. Technically, the experimental channel would also introduce a small amount of excess noise, however this is negligible compared to the excess noise coming from the effects described above. The final simulated covariance matrix hence is

$$\gamma_{\text{out}} = S[\gamma_{\text{in}} \oplus V_{\chi}(B) \oplus \text{diag}(1,1)]S^T, \tag{6.20}$$

where S is given by

$$S = R_2(\theta_x, \theta_p)B_{1,4}(1/2)B_{2,3}(T). \tag{6.21}$$

Here, $V_{\chi} = \text{diag}(1 + \chi_x, 1 + \chi_p)$, where $\chi_{x(p)}$ is the excess noise in $\hat{X}(\hat{P})$ quadrature. $B_{i,i}$ is the beam splitter matrix defined in Sec. 2.3 that acts on mode i and j. The rotation matrix on Bob,

$$R_2(\theta_x, \theta_p) = \begin{pmatrix} \cos\theta_x & \sin\theta_x \\ -\sin\theta_p & \cos\theta_p \end{pmatrix}, \tag{6.22}$$

serves as the fitting parameter to model the unknown rotation due to aforementioned experimental imperfection.

6.5.4 Results

In each protocol, Alice and Bob are connected by a lossy channel of transmission T. The lossy channel is constructed using a half wave plate and a polarizing beam splitter as detailed in Fig. 6.4. We express the applied loss as the equivalent transmission distance through a standard telecom optical fibre with a loss of 0.2dB/km. Ideally, the secret key rate could be computed directly from the expressions in Supplement 1. However, in practice we must modify these expression, multiplying Alice and Bob's mutual information by a factor $\beta < 1$ to account for finite information reconciliation efficiency (see Supplement 1 for explicit calculations). Reconciliation efficiencies for CVQKD have increased substantially in the last few years [155, 156], with efficiencies of between 94 and 95.5 percent recently reported [157]. Here, we choose $\beta = 0.95$. The inclusion of $\beta < 1$ will reduce the final calculated key rate. This makes the condition $\mathcal{E}_{\blacktriangleleft} < 0.55$ necessary but no longer sufficient for a positive key when β is included.

To evaluate the key rate Eq. (6.16), we neglect the excess noise in the channel by setting $\chi_{x(p)} = 0$. The variation of key rates versus the equivalent modulation squeezing parameter for 5 different transmissions is shown in Fig. 6.5(a). As the modulation is

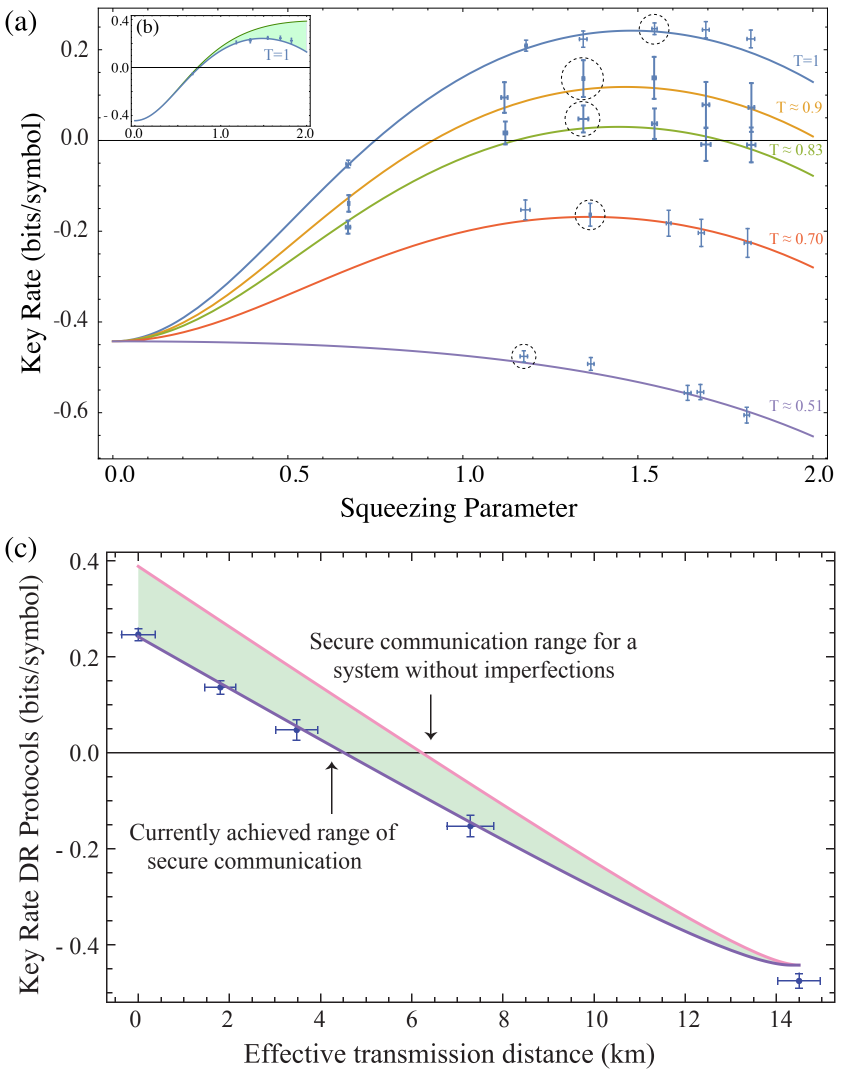


Figure 6.5: (a) Variation of key rates versus effective modulation squeezing parameter for 5 different transmissions. A theory line with the average transmission of the channel is fitted on the experimental data points with 1 s.d. error bars. Data points surrounded by dashed circles correspond to the optimum modulation squeezing parameters which result in the highest key rate for each transmission. The key rates resulting from these optimum modulation variances are shown separately in (c). Inset (b) demonstrates the gap between the theoretical cross-talk free model and the realistic model which captures the experimental imperfections. (c) Predicted improvement of secure transmission distance through the optical fibre for the coherent state protocol with an improved experimental setup (red curve). The model for the current system (blue curve) is plotted along with experimental data (blue points) for comparison. In the actual experiment, the optimal modulation variance is reduced due to unwanted cross-quadrature correlations. In the improved setup, the cross-talk has been eliminated and the optimal modulation variance is now determined by the reconciliation efficiency, which is chosen to be 0.95 for both cases.

increased, so too is the detrimental effect on the correlations, leading to a smaller value for the optimal modulation parameter. Meanwhile, for an ideal experiment, this optimal modulation depends only upon β and the channel loss. In inset (Fig. 6.5(b)) the gap between the ideal case without cross correlation and the realistic case is shown for the case of perfect transmission. For each transmission value, the modulation squeezing parameters that provide the highest key rate are chosen and plotted in Fig. 6.5(c). The theoretical lines in the plot are produced using the model described in section 6.5.3 and Eq. (6.16). The value of the unknown rotation, (θ_x, θ_p), was estimated to be about $\approx (6\pi/180, 3\pi/180)$. We show that secure key remains possible after an equivalent transmission distance of 3.47±0.46 km (approximately 15% applied loss). This is in good agreement with our theoretical model, which predicts our current setup would be secure up to a maximum of 4.5 km.

As is clear from Fig. 6.5(a), using coherent states provides a much greater range over which to tune the equivalent squeezing. Our model also predicts that if the cross correlation between Alice and Bob's modes was zero, the range of secure communication for this protocol would extend from 4.5 km to 6.5 km as depicted in Fig. 6.5(c).

6.6 Summary

To summarise, we have shown that it is possible to achieve a 1sDI CVQKD using only coherent states. That such an exotic quantum communication protocol is possible with these relatively mundane quantum states is a surprising result in itself. Under ideal condition, our model shows that the asymptotic range of the coherent state scheme could be increased to around 4.5 km. This, together with the fact that such states are readily available, makes them an especially attractive candidate for short range metropolitan networks.

Part III

Enhancing the Quantum Amplifier

Chapter 7

Measurement-Based Noiseless Linear Amplification

> *"We must become more comfortable with probability and uncertainty."*
>
> – Nate Silver, *The Signal and the Noise: The Art of Science and Prediction*

Overview

In this chapter, we describe several different approaches in amplifying a continuous variable (CV) quantum state: a deterministic noisy amplifier, a probabilistic noiseless amplifier and a measurement-based implementation of such noiseless amplifier. We compare and contrast the performance of a heralded measurement-based noiseless linear amplifier (MB-NLA) with its physical counterpart through the Husimi Q distribution and its working probability. Relevant publication to the work in this chapter are:

- H. Chrzanowski, N. Walk, J. Y. Haw, O. Thearle, S. Assad, J. Janousek, S. Hosseini, T. C. Ralph, T. Symul, and P. K. Lam.
"Measurement-based noiseless linear amplification for quantum communication."
SPIE/COS Photonics Asia, pages 926902-926902. International Society for Optics and Photonics. (2014)

- J. Zhao, J. Y. Haw, S. M. Assad, T. Symul, and P. K. Lam,
"Characterisation of measurement-based noiseless linear amplifier and its applications."
Physical Review A 96 (1), 012319. (2017).

7.1 Introduction

Signal amplification is a procedure in communication which aims to preserve the signal-to-noise ratio. It is desirable for a signal to be first amplified before entering a lossy or noisy channel. Classically, there is no fundamental limit to the amplification process, since the amplitude and phase of the signal could in principle be determined exactly. In the quantum domain, the incompatibility of the conjugate quadrature not only forbids such a perfect amplification, but also imposes a noise penalty of 3 dB at large power gain limit. The impossibility of such a deterministic noise-free amplification of an arbitrary state was first realised by Haus and Mullen [158] in 1962. It was further developed and clarified by Caves [159], where the ultimate limits imposed by quantum mechanics on amplifiers was pointed out. Although this serves as the crucial basis for secure quantum communication, it imposes unavoidable limits on signal processing and quantum metrology.

The first ingenious idea to evade this noise penalty was proposed by Lund and Ralph [160] and, independently, by Fiurasek [161]. By renouncing the need for a deterministic amplification outcome, they identified a device which can amplify the amplitude of an input state while preserves its noise characteristics, known as *noiseless linear amplifier* (NLA). Of course, even should one sacrifice some events, a perfect implementation of such transformation for any state would still necessitate a vanishing success probability. Nevertheless, practical benefits of noiseless amplification can be retained with high fidelity and reasonable success probability, if one further abandons the exactness of the NLA implementation, or restrict the set of input states [162].

Proposals and physical implementations of such *approximate* NLA includes methods such as quantum scissors [160, 163, 164, 165, 166], photon addition-subtraction [167, 168, 169] and noise addition [170]. We designate these realisations as *physical NLAs* (P-NLA), for they take an input state and transform it into an amplified propagating output. P-NLAs have been studied theoretically in several aspects, with a large focus on the optimality of its architecture [171, 172]. These developments open up many promising applications in quantum computing and communication, such as quantum key distribution [173, 174, 175, 176, 177, 178], quantum cloning [179], entanglement distillation [164, 180], the construction of quantum repeaters [181], phase estimation [170] and error correction [182]. However, most of these experiments are not only challenging to perform, but also suboptimal in terms of the success probability [172, 171].

If one does not require access to an output quantum state that is an amplified version of the input state, which is the case for point-to-point QKD, technical complexities can be alleviated. Refs. [183, 184] proposed the possibility of implementing a non-deterministic measurement-based NLA (MB-NLA) that allows one to transfer the difficulty of hardware implementation to a software-based protocol. This measurement-based protocol has recently been realised by Chrzanowski et. al. in an entanglement distillation experiment. Given a non-maximally entangled resource transmitted through a lossy channel, the authors have demonstrated distilled entanglement using the MB-NLA. Subsequent to the distillation, the entanglement level is beyond that achievable by a maximally entangled resource subjected to the same conditions of loss. The result was further applied to secret key extraction from an otherwise insecure regime.

In this chapter, we will first briefly review deterministic linear amplification, and show that by adopting a probabilistic approach, a physical NLA that circumvents the constraint set by HUP is possible. We then introduce the MB-NLA, which is the post-selective version of NLA. While it has been shown in [183, 185] that MB-NLA is equivalent to an ideal NLA as long as the amplification directly precedes an informational-complete (IC) POVM, it is unclear to what extent they are interchangeable. We will thus examine the relationship between P-NLA and MB-NLA from the perspective of Q-function and success probability.

7.2 Deterministic noisy linear amplifier

7.2.1 The impossibility of deterministic noiseless amplification

The origin of the limitation in quantum amplification is that adding extra noise is inevitable for the output field to obey Heisenberg's uncertainty relation. For a phase insensitive, or phase preserving amplification, it is necessary to extract the information of the conjugate quadratures, amplitude X and phase P. As elucidated in Sec. 3.3.2, a simultaneous measurement of both quadratures would incur a degradation of signal-to-noise ratio, i.e. mean squared $\hat{X}^\theta$ divided by variance $\Delta^2\hat{X}$ due to the coupling of vacuum in the unused port of a heterodyne detection. As we shall illustrate, it is also connected to the impossibility of realizing perfect copies of an unknown quantum signal [5], which is the consequence of quantum mechanical systems evolving according to linear and unitary operations.

Noiseless amplification is typically defined as the ability to increase the amplitude of an arbitrary coherent state without adding any noise, i.e.

$$|\alpha\rangle \xrightarrow{\text{amplification}} |g\alpha\rangle\,, \tag{7.1}$$

with real amplification gain $g > 1$. For such a phase-insensitive transformation, one requires $\hat{a}_{\text{out}} = g\hat{a}_{\text{in}}$ and $\hat{a}^\dagger_{\text{out}} = g\hat{a}^\dagger_{\text{in}}$. By considering the annihilation and creation operators describing a boson mode, it becomes obvious that such transformation does not preserve the canonical commutation relations (Eq. (2.2)), since $[\hat{a}_{\text{out}}, \hat{a}^\dagger_{\text{out}}] = g^2$ [159].

7.2.2 No-cloning theorem

The prohibition of deterministic noiseless amplification can also be illustrated in a more intuitive manner through the no-cloning theorem [5]. This theorem states that it is impossible to *deterministically* clone an *unknown* quantum state. It can be simply proven by linearity and unitarity of quantum mechanics, which we will briefly sketch below.

No cloning theorem: It is impossible to copy an unknown quantum state perfectly. Let us assume that such a unitary transformation exists

$$|\psi\rangle\,|\phi\rangle \xrightarrow{U_c} |\psi\rangle\,|\psi\rangle\,, \tag{7.2}$$

where a blank state $|\phi\rangle$ copies the target state $|\psi\rangle$. For a simple qubit sytem, this implies that under U_c, $|0\rangle|\phi\rangle \to |0\rangle|0\rangle$ and $|1\rangle|\phi\rangle \to |1\rangle|1\rangle$. For a linear combination of $|0\rangle+|1\rangle$, one would expect an outcome of $(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)$ under the cloning operation U_c. However, the linearity in QM requires the output to be $|0\rangle|0\rangle+|1\rangle|1\rangle$, which is not the desired copy. Hence by *reductio ad absurdum*, there exists no such unitary transformation. An alternative proof based on the invariance of inner products under unitary transformations also leads to the conclusion that non-orthogonal states cannot be cloned.

It is straightforward to show that if perfect cloning is prohibited, deterministic amplification is also prohibited [186]. For example, if one is allowed to deterministically amplify an unknown coherent state, a perfect clone could be obtained simply by adjusting their noiseless amplifier to a gain of $g=\sqrt{2}$, and then splitting the output on a 50:50 beam splitter:

$$|\alpha\rangle|0\rangle \xrightarrow{\text{amplification}} \left|\sqrt{2}\alpha\right\rangle|0\rangle \xrightarrow{\text{beam}-\text{splitter}} |\alpha\rangle|\alpha\rangle\,. \tag{7.3}$$

Hence for an ideal quantum limited amplifier, additional noise is unavoidably demanded by the laws of quantum mechanics. Next we will examine what is the best limit allowed by quantum mechanics.

7.2.3 Phase insensitive ideal linear amplifier

The theoretical description of an ideal deterministic linear amplifier (DLA) operating at quantum limit was originally discussed by Haus and Mullen [158], further reformulated in terms of fundamental theorems by Caves [159]. As mentioned in the previous section, in order to preserve the commutator relations Eq. (2.2), we require

$$\hat{a}_{\text{out}} = g_{\text{DLA}}\hat{a}_{\text{in}} + \hat{\mathbb{F}}. \tag{7.4}$$

Here, g_{DLA} is a real-value gain of the ideal DLA, while $\hat{\mathbb{F}}$ is an operator associated with the internal modes of the amplifier, which contribute to the additional quantum noise. Depending on the underlying physical processes, This noise will have different origins. Since the noise are uncorrelated with the input, i.e. $[\hat{\mathbb{F}},\hat{a}_{\text{in}}] = [\hat{\mathbb{F}},\hat{a}^{\dagger}_{\text{in}}] = 0$, insisting $[\hat{a}_{\text{out}},\hat{a}^{\dagger}_{\text{out}}]=1$ yields

$$[\hat{\mathbb{F}},\hat{\mathbb{F}}^{\dagger}] = 1 - g^2_{\text{DLA}}. \tag{7.5}$$

We note that for amplification, where $g^2_{\text{DLA}} > 1$, the RHS of Eq. 7.5 is negative. Hence the simplest form for $\hat{\mathbb{F}}$ is

$$\hat{\mathbb{F}} = \sqrt{g^2_{\text{DLA}}-1}\hat{b}^{\dagger}_{\text{int}}, \quad \hat{\mathbb{F}}^{\dagger} = \sqrt{g^2_{\text{DLA}}-1}\hat{b}_{\text{int}}, \tag{7.6}$$

where $\hat{b}_{\rm int}(\hat{b}^\dagger_{\rm int})$ represents the additional bosonic internal mode. Putting all these together, we end up with the well known formula for a phase-insensitive amplifier working at the quantum noise limit:

$$\hat{a}_{\rm out} = g_{\rm DLA}\hat{a}_{\rm in} + \sqrt{g^2_{\rm DLA} - 1}\hat{b}^\dagger_{\rm int}. \tag{7.7}$$

Numerous proposals show, in principle, ideal phase-insensitive amplification is feasible [187, 188]. Such amplification at the quantum limit was partially demonstrated using optical parametric amplifier [189, 190], limited chiefly by the coupling efficiency.

A recent demonstration [191], using only linear optics and homodyne detection, approaches the quantum noise limit. Consider the setup depicted in Fig. 7.1. After the beam splitter, the X quadrature of a coherent state generated by a pair of modulators at the transmitted and reflected modes are given by

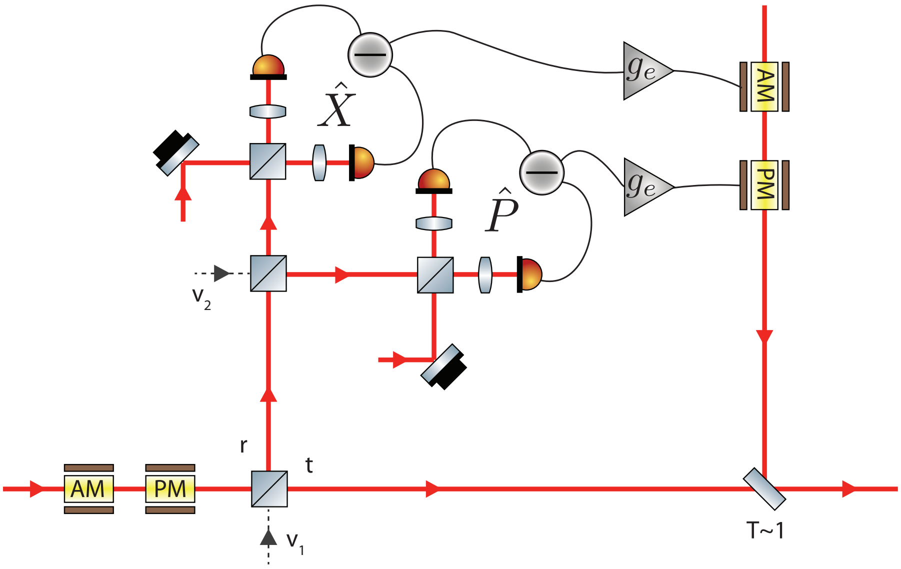


Figure 7.1: Optical implementation of an ideal deterministic linear amplifier via feedforwarding. AM and PM: Amplitude modulation and Phase modulation, t (r): transmitted (reflected) mode, $g_{\rm e}$: electronic gain.

$$\hat{X}_{\rm t} = \sqrt{T}\hat{X}_{\rm in} + \sqrt{1-T}\hat{X}_{\rm v_1}, \tag{7.8}$$
$$\hat{X}_{\rm r} = \sqrt{1-T}\hat{X}_{\rm in} - \sqrt{T}\hat{X}_{\rm v_1}, \tag{7.9}$$

where we have used Eq. (3.17) to describe the coupling of the vacuum mode v_1. At the measurement stage, the reflected modes is detected together with a vacuum input by a heterodyne detector

$$\hat{X}_{\rm m} = \frac{1}{\sqrt{2}}\left(\sqrt{1-T}\hat{X}_{\rm in} - \sqrt{T}\hat{X}_{\rm v_1} + \hat{X}_{\rm v_2}\right). \tag{7.10}$$

The feedforward is completed by amplifying $\hat{X}_{\rm m}$ by electronic gain $g_{\rm e}$ before interfering it with the transmitted mode $\hat{X}_\mathrm{t}$ over a highly reflective beam splitter. This results in

$$\begin{aligned}\hat{X}_\mathrm{out} &= \hat{X}_\mathrm{t} + g_\mathrm{e}\hat{X}_\mathrm{m} \\ &= \left(g_\mathrm{e}\sqrt{\frac{1-T}{2}} + \sqrt{T}\right)\hat{X}_\mathrm{in} + \left(\sqrt{1-T} - g_\mathrm{e}\sqrt{\frac{T}{2}}\right)\hat{X}_{\mathrm{v}_1} + \frac{g_\mathrm{e}}{\sqrt{2}}\hat{X}_{\mathrm{v}_2}. \qquad (7.11)\end{aligned}$$

By setting $g_\mathrm{e} = \sqrt{\frac{2(1-T)}{T}}$, the vacuum mode contribution v_1 is cancelled out. The equation further simplifies into

$$\hat{X}_\mathrm{out} = \frac{1}{\sqrt{T}}\hat{X}_\mathrm{in} + \sqrt{\frac{1}{T} - 1}\hat{X}_{\mathrm{v}_2}. \qquad (7.12)$$

By identifying g_DLA as $1/\sqrt{T}$, and using the fact that $\hat{X}_\mathrm{out} = \hat{a}_\mathrm{out} + \hat{a}^\dagger_\mathrm{out}$, we recover Eq. (7.7) with the vacuum introduced at at the dual-homodyne measurement as the additional internal bosonic mode. We thus see that such an amplification indeed pays only the noise penalty of measuring the quadratures simultaneously. The mean and the variance of the output are given by

$$\langle\hat{X}_\mathrm{out}\rangle = g_\mathrm{DLA}\,\langle\hat{X}_\mathrm{in}\rangle\,, \qquad (7.13)$$

$$\Delta^2\hat{X}_\mathrm{out} = g^2_\mathrm{DLA}\Delta^2\hat{X}_\mathrm{in} + (g^2_\mathrm{DLA} - 1), \qquad (7.14)$$

where we have used $\Delta^2\hat{X}_{\mathrm{v}_2} = 1$. If the input is a coherent state (Sec. 2.2.3), $\Delta^2\hat{X}_\mathrm{in} = 1$, thus the variance becomes $2g^2_\mathrm{DLA} - 1$. The performance of the amplifier can be determined in terms of the signal transfer coefficient, which is defined as

$$T_s = \mathrm{SNR}_\mathrm{out}/\mathrm{SNR}_\mathrm{in}. \qquad (7.15)$$

For the DLA, this is equal to

$$T_s = \frac{g^2_\mathrm{DLA}}{2g^2_\mathrm{DLA} - 1}, \qquad (7.16)$$

which we see that, at large gain limit, $T_s \to 1/2$, implying that the noise will be doubled upon amplification (and hence the 3dB SNR reduction). We refer our reader to the review [192] for more details on other applications of quantum feed-forward control.

7.3 Probabilistic noiseless linear amplifier

While it is impossible to amplify noiselessly in a deterministic fashion, one can forgo determinism in favour of a probabilistic transformation [160],

$$|\alpha\rangle\,\langle\alpha| \to P\,|g\alpha\rangle\!\langle g\alpha| + (1-P)\,|0\rangle\!\langle 0|\,, \qquad (7.17)$$

in which amplification succeeds with probability P, and fails otherwise. If the success is heralded, one can then enjoy the benefits of noiseless amplification at least for some of the time [172]. As discussed in Refs. [160, 167], this transformation is carried out by the operator $g^{\hat{n}}$, where $\hat{n} = \hat{a}^\dagger \hat{a}$ is the number operator. In the amplification regime ($g > 1$), the operation $g^{\hat{n}}$ is unbounded, and as such could only be implemented exactly with a success probability equal to zero. However, for any particular input state and gain, one can always devise an approximation of $g^{\hat{n}}$ by truncating it, thus allowing amplification with a fidelity that is nearly indistinguishable from a perfect NLA [172, 171] (See Sec. 7.5.1).

We first recall that an ideal NLA is a device that amplifies the coherent state without amplifying its quantum noise [160, 161]. The ideal (unbounded) NLA operation can be represented by the operator $g^{\hat{n}}$ with $g > 1$, which transform a coherent state $|\alpha\rangle$ to an amplified state $|g\alpha\rangle$ via the following operation [160, 167]:

$$g^{\hat{n}} |\alpha\rangle = e^{\frac{1}{2}(g^2-1)|\alpha|^2} |g\alpha\rangle \,, \tag{7.18}$$

where $\hat{n}$ is the photon number operator. As discussed in [175, 185], the statistics of a positive-valued operator measurement (POVM) (Sec. 2.4.1) set upon the transformed state can be obtained by instead considering a transformed POVM set acting on the original state. This is permissible provided the POVM set is informationally complete (IC). A dual-homodyne measurement, which is essentially a coherent state projection, is in fact IC-POVM [185]. The ideal unnormalised probability distribution, or Q-distribution (Sec. 2.5.3), of this measurement upon an input state ρ_{in} is given by [175]:

$$\begin{aligned} p_{\text{ideal}}(\alpha) &= \frac{1}{\pi} \langle \alpha | g^n \rho_{\text{in}} g^n | \alpha \rangle \\ &= \exp\left[\left(g^2 - 1\right)|\alpha|^2\right] \frac{1}{\pi} \langle g\alpha | \rho_{\text{in}} | g\alpha \rangle \ . \end{aligned} \tag{7.19}$$

Performing a change of variable, $\alpha = \alpha_m / g$, we get

$$p_{\text{ideal}}(\alpha_m) = \exp\left[\left(1 - \frac{1}{g^2}\right)|\alpha_m|^2\right] \frac{1}{\pi} \langle \alpha_m | \rho_{\text{in}} | \alpha_m \rangle \ . \tag{7.20}$$

As a prelude to a measurement-based approach, this equation allows us to determine the particular probabilistic filter and the necessary rescaling to be applied after the dual-homodyning to emulate the measurement statistics of an NLA (Fig. (7.2).

7.4 Measurement-based noiseless linear amplifier

For the case where the amplification directly precedes the measurement, for example in quantum key distribution, probabilistic NLA can be emulated by conditioning upon the measurement records via a classical filter function [175, 185, 176]. This post-selection scheme, which we term as *measurement-based* NLA (MB-NLA), is shown to be equiva-

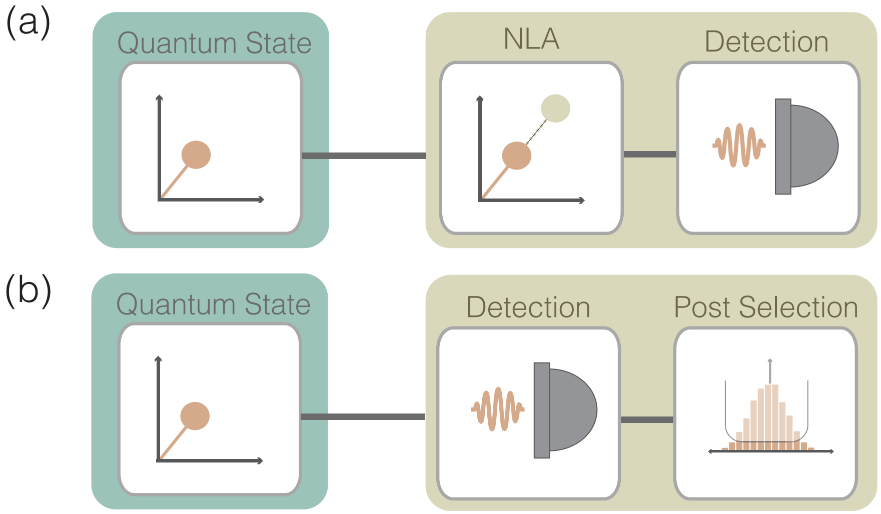


Figure 7.2: (a) When a ideal NLA is immediately followed by an informationally complete POVM, such as a heterodyne measurement, it can be faithfully emulated (b) by applying Gaussian post-selection of the classical data.

lent to its physical counterpart as long as the measurement that follows the amplification is informationally complete [185]. It is demonstrated experimentally that such post-selection scheme permits distillation of entanglement beyond that accessible with a perfect entangled resource experiencing the losses up to an equivalent of 100km [185]. In the same work, it was shown that that secret key extraction from an otherwise insecure regime is possible via MB-NLA. Recently, it is also proposed that MB-NLA can be integrated into a CV quantum teleportation scheme [193] for channel purification. Compared to its physical counterpart, MB-NLA has the advantage of easy implementation, but also allows one to achieve near optimal probability of success.

In ref. [175, 176], it was shown how noiseless amplification can be achieved *virtually* through a Gaussian post-selection. Comparison of Eq. (7.19) and (7.20) provides a three-step recipe for emulating an ideal NLA with gain g via a measurement-based algorithm:

1. First, an input state ρ_{in} is directly measured via a dual homodyne detection to get a probability distribution

$$p\left(\alpha_m\right) = \frac{1}{\pi}\left\langle \alpha_m \middle| \rho_{\text{in}} \middle| \alpha_m \right\rangle \ . \tag{7.21}$$

2. Second, the pre-factor $\exp\left[\left(1-\frac{1}{g^2}\right)\left|\alpha_m\right|^2\right]$ in Eq. (7.20) can be realised by a probabilistic filter. In order to ensure the convergence of the filter probability, this pre-factor is approximated by a probabilistic filter function

$$p_{\text{F}}\left(\alpha_m\right) = \begin{cases} \frac{1}{M}\exp\left[\left|\alpha_m\right|^2\left(1-\frac{1}{g^2}\right)\right] & \text{if } |\alpha_m| < \alpha_{\text{c}}, \\ 1 & \text{otherwise,} \end{cases} \tag{7.22}$$

where $M = \exp\left[\alpha_{\mathrm{c}}^2\left(1-1/g^2\right)\right]$ is the normalisation term that ensures the filter probability $p_{\mathrm{F}} \leq 1$. We note that this filter has an inverse Gaussian profile and is parametrized by the NLA gain g and a real cut-off $\alpha_{\mathrm{c}} \geq 0$. All data points with magnitude less than α_{c} are selected with probability specified by the filter function while all data points with magnitude greater than the cut-off α_{c} are kept. Due to this finite cut-off, the resulting distribution of MB-NLA will differ from that of an ideal NLA. In practice, the emulation can be deployed with high fidelity provided a large enough cut-off value α_{c} is chosen. However, choosing an overly large α_{c} will lead to a vanishing probability of success. Hence, a compromise between the fidelity of the MB-NLA and the probability of success has to be made for each application. The data points that passes through the filter will exhibit a distribution

$$\tilde{p}\left(\alpha_m\right) = \frac{1}{p_S^{(\mathrm{mb})}} p\left(\alpha_m\right) p_{\mathrm{F}}\left(\alpha_m\right), \tag{7.23}$$

where $p_S^{(\mathrm{mb})}$, the probability of success is given by

$$p_S^{(\mathrm{mb})} = \iint \mathrm{d}^2\alpha_m \, p\left(\alpha_m\right) p_{\mathrm{F}}\left(\alpha_m\right) \ . \tag{7.24}$$

3. The third step in emulating an ideal NLA is a linear rescaling that maps α_m to $g\alpha$. The output after this step will be distributed according to $Q^{(\mathrm{mb})}(\alpha)$, where

$$Q^{(\mathrm{mb})}(\alpha) = \tilde{p}\left(g\alpha\right) g^2 \ , \tag{7.25}$$

by requiring $Q^{(\mathrm{mb})}(\alpha)\mathrm{d}^2\alpha = \tilde{p}\left(\alpha_m\right)\mathrm{d}^2\alpha_m$. As we shall illustrate in the next section, this last step ensures that the variance of the vacuum is preserved.

7.5 Comparing the physical and measurement-based amplifiers

While an MB-NLA can approximately emulate a noiseless amplification process, it is not apparent when one concerns with the limits on effective parameters of MB-NLA when it is substituted for a P-NLA. For instance, analogous to the truncation of operating regime of P-NLA, we see that an MB-NLA also require a cutoff on the quantum filter to enact an approximate NLA. Since increasing this cutoff will deteriorate the probability of success, one might conclude that it resembles the truncation of the amplification operator in P-NLA. However, as we shall demonstrate, the truncation and the cutoff actually act in a different manner. In fact, only when one takes into account all of the relevant effective parameters (input amplitude, NLA gain, cut-off), such equivalence between the measurement-based emulation and the physical implementation can be drawn.

In the following sections, we provide a more detailed analysis on the MB-NLA and study its effect on arbitrary coherent input states. We compare the performance of MB-

NLA with a P-NLA scheme based on an optimal POVM implementation [171, 172] that maximizes the probability of success and the fidelity.

7.5.1 Physical NLA

To investigate the equivalence between P-NLA and MB-NLA, it is instructive to look at how well they can be realised physically from a general theoretical framework. For P-NLA, we look particularly at a theoretical model that realizes the NLA optimally with both working probability and fidelity saturating the theoretical bound [171, 172]. Amplification with a gain of g in this architecture is realised by a two-outcomes POVM, where the successful outcome is specified by the operator [172]

$$M_S = \underbrace{\frac{1}{g^{N_\mathrm{c}}} \sum_{n=0}^{\lfloor N_\mathrm{c} \rfloor} g^n \left| n \right\rangle \left\langle n \right|}_{M_{S,1}} + \underbrace{\sum_{n=\lceil N_\mathrm{c} \rceil}^{\infty} \left| n \right\rangle \left\langle n \right|}_{M_{S,2}} \ . \tag{7.26}$$

Here, the photon number cut-off N_c specifies the maximum photon number Fock state that will be amplified. This cut-off amounts to the truncation on the ideal but unbounded amplification operator Eq. (7.18). For an input state ρ_in, we can calculate the probability of success

$$p_S^{(\mathrm{phy})} = \mathrm{Tr}\left(M_S \rho_\mathrm{in} M_S^\dagger \right) , \tag{7.27}$$

and the resultant output state of the NLA will be

$$\rho_S = \frac{M_S \rho_\mathrm{in} M_S^\dagger}{p_S^{(\mathrm{phy})}} \ . \tag{7.28}$$

Performing a dual homodyne measurement on ρ_S reveals its Husimi Q distribution (Eq. (2.43))

$$Q^{(\mathrm{phy})}(\alpha) = \frac{1}{\pi} \left\langle \alpha | \rho_S | \alpha \right\rangle . \tag{7.29}$$

7.5.2 Q distributions

To compare the NLAs, we consider coherent input states, since they have symmetric minimum-uncertainty noise. To elucidate the action of MB-NLA upon the coherent state, we shall elaborate the three steps involved in the amplification. First, a input state $|\alpha_0\rangle$ is directly measured with a dual homodyne measurement to get a distribution

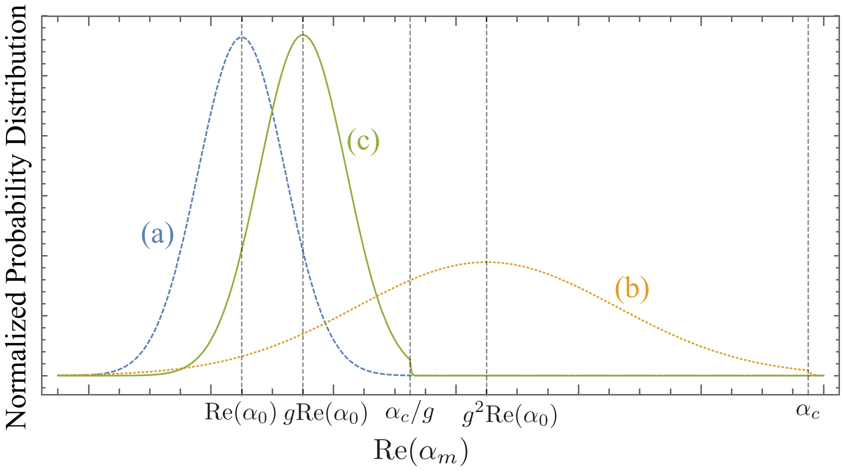


Figure 7.3: Probability distributions of $\mathrm{Re}[\alpha_\mathrm{m}]$ involved in MB-NLA action upon the input coherent state $|\alpha_0\rangle$. (a) Direct measurement with dual-homodyne detection, resulting in a Gaussian distribution with mean $\mathrm{Re}[\alpha_\mathrm{m}]$. (b) With an appropriate cut-off α_c, the probabilistic filter (Eq. (8.14)) shifts the mean to $\approx g^2\mathrm{Re}[\alpha_\mathrm{m}]$. (c) The final rescaling leads to the target distribution with mean of increased by a factor of g.

(Eq. (7.21))

$$p\left(\alpha_m\right) = \frac{1}{\pi}\exp\left(-\left|\alpha_m - \alpha_0\right|^2\right) \,. \tag{7.30}$$

The real part of this distribution is centred at $\mathrm{Re}(\alpha_0)$ and has variance $\mathrm{Var}[\mathrm{Re}(\alpha_m)] = \mathrm{Var}[\mathrm{Im}(\alpha_m)] = 0.5$. The real part of the distribution is plotted in Fig. 7.3(a). In the second step, we apply the filter function Eq. 7.22. As a result, the mean and the variance of the distribution is amplified by a factor of g^2 (Fig. 7.3(b)). Lastly, we rescale the α_m by a factor of $1/g$ to obtain Eq. (7.25). This procedure reduces the mean to $g\alpha_0$ while the variance is reverted back to original. The net effect on the statistics of a coherent input state of the MB-NLA is hence to increase the mean approximately by g while keeping the variance unchanged (Fig. 7.3(c)). The effect of finite cut-off α_c can be observed in Fig. 7.3(b) and (c), where a discontinuity of the distribution occurs at the cut-off value.

Explicitly, the Q distribution of MB-NLA for a coherent state is

$$Q^{(\mathrm{mb})}(\alpha) = \frac{1}{p_S^{(\mathrm{mb})}} \begin{cases} \frac{g^2}{\pi}\exp\left(-\left|\alpha - g\alpha_0\right|^2\right)\exp\left[\left(g^2-1\right)\left(\left|\alpha_0\right|^2 - \frac{\alpha_\mathrm{c}^2}{g^2}\right)\right] & \text{if } |\alpha| < \frac{\alpha_\mathrm{c}}{g}, \\ \frac{g^2}{\pi}\exp\left(-\left|g\alpha - \alpha_0\right|^2\right) & \text{otherwise,} \end{cases} \tag{7.31}$$

which is a concatenation of two Gaussian distributions joined at the circle $|\alpha| = \alpha_\mathrm{c}/g$. The probability of success $p_S^{(\mathrm{mb})}$ will be discussed in the section 7.5.3. This distribution is plotted in Fig. 7.4 for a coherent input state with amplitude $\alpha_0 = 0.5$ and filter cut-off of $\alpha_\mathrm{c} = 4$, 6 and 8. The performance of the MB-NLA is examined with respect to the ideal NLA when varying gains are set. In these figures, only (e), (i) and (j) resembles the output of an ideal NLA. As the gain increases, a larger cut-off is needed for the output to remain close to the ideal output. In the limit $g \to \infty$, the output distribution tends to a Dirac delta function centred at the origin.

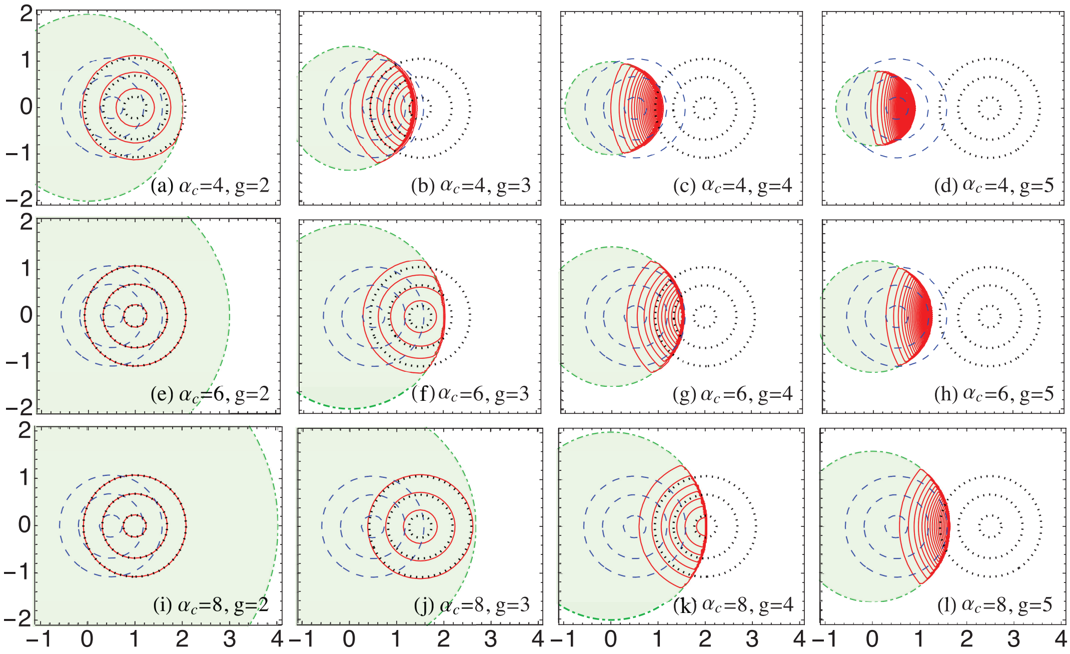


Figure 7.4: Output distribution of a measurement based NLA. Blue dashed line gives the distribution of the coherent state input with amplitude $\alpha_0 = 0.5$. Black dotted line gives the output distribution of an unbounded ideal NLA. Red solid line is the distribution of the outcome of measurement-based NLA with different cut-off and amplification gain. The output distribution consists of two Gaussian distribution joined at the green circle with radius $|\alpha| = \alpha_c/g$. The spacing of contour levels is 0.1.

For comparison, in Fig. 7.5, we plot $Q^{(\mathrm{phy})}(\alpha)$ with same input amplitude $\alpha_0 = 0.5$ and truncation in the photon number $N_c = 1, 3$ and 5. Just as the case in MB-NLA, we see that P-NLA implements the ideal NLA faithfully only when the truncation point N_c properly accommodates $|\alpha_0|$ and g (Fig. 7.5 (e), (i) and (j)). However, we do notice that the cut-offs α_c and N_c do have a different effect on the distribution of the amplified coherent state. We also note that for MB-NLA, its output distribution does not necessarily represent a valid Husimi Q-distribution of a physical quantum state, in particularly when the cut-off is not sufficiently large. Lastly, We emphasize that the MB-NLA is not an emulation of the P-NLA, but rather the measurement statistic of an ideal NLA (Eq. 7.20).

7.5.3 Probability of success

In a MB-NLA setup, the probability of success is given by Eq. (7.24) which is a function of the NLA gain g, cut-off α_c and the amplitude of the input states. For a coherent state

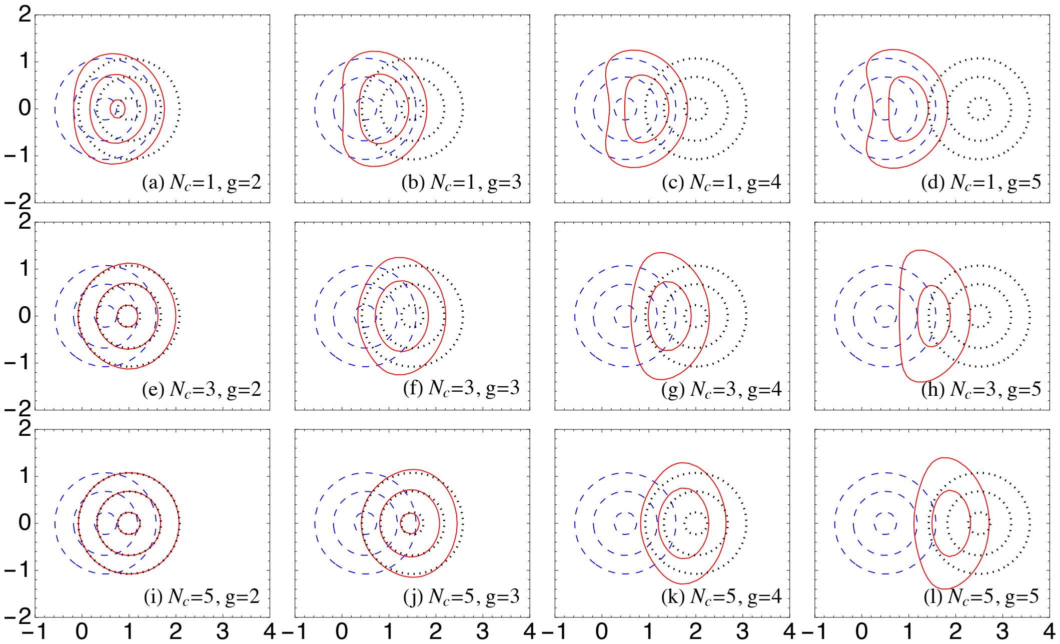


Figure 7.5: Output distribution of a physical NLA. The blue, dashed line gives the distribution of the coherent state input with amplitude $\alpha_0 = 0.5$. The black, dotted line gives the output distribution of an ideal NLA with infinite photon number cut-off. Red solid line is the distribution of the outcome of physical NLA with different photon number cut-offs and amplification gains. The spacing contour levels is 0.1.

input with amplitude α_0, this is given by

$$p_S^{(\mathrm{mb})} = \underbrace{\frac{g^2}{\pi} \exp\left[\left(g^2-1\right)\left(|\alpha_0|^2 - \frac{\alpha_{\mathrm{c}}^2}{g^2}\right)\right] \iint\limits_{|\alpha|<\frac{\alpha_{\mathrm{c}}}{g}} \exp\left(-\left|\alpha - g\alpha_0\right|^2\right) \mathrm{d}^2\alpha}_{p_{S,\mathrm{in}}^{(\mathrm{mb})}}$$

$$+ \underbrace{\frac{g^2}{\pi} \iint\limits_{|\alpha|\geq\frac{\alpha_{\mathrm{c}}}{g}} \exp\left(-\left|\alpha-\alpha_0\right|^2\right) \mathrm{d}^2\alpha}_{p_{S,\mathrm{out}}^{(\mathrm{mb})}} \ . \tag{7.32}$$

The first term $p_{S,\mathrm{in}}^{(\mathrm{mb})}$ involves an integration within the circle of radius α_{c}/g of a two-dimensional Gaussian centred at $g\alpha_0$. The second term, $p_{S,\mathrm{out}}^{(\mathrm{mb})}$, is independent of g (upon a change of variable $\beta = g\alpha$). Although both terms contribute to the total probability of success, only the fraction $p_{S,\mathrm{in}}^{(\mathrm{mb})}$ are properly amplified. The $p_{S,\mathrm{out}}^{(\mathrm{mb})}$ fraction are the remnant from the input distribution that lies beyond the filter cut-off. The probability of success are plotted in Fig. 7.6(a) as a function of the NLA gain for different cut-offs. We see that the probability of success decreases rapidly as gain and cut-off increases. For example, at NLA gain $g = 2$, the probability of success drops from 10^{-4} to 10^{-11} when the cut-off increases from $\alpha_{\mathrm{c}} = 4$ to $\alpha_{\mathrm{c}} = 6$. Meanwhile, for P-NLA, the probability of

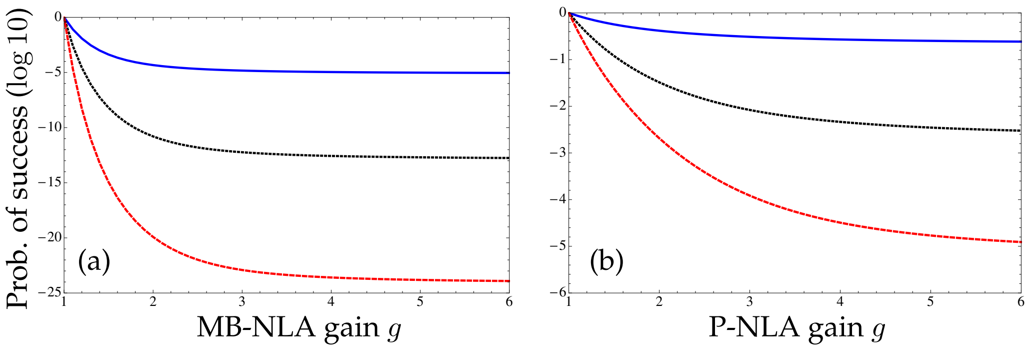


Figure 7.6: (a) MB-NLA with versus gain g for $\alpha_{\mathrm{c}} = 4$, 6 and 8 (blue, black and red) curves. (b) P-NLA versus gain g for cut-off $N_{\mathrm{c}} = 1$, 3 and 5 (blue, black and red). For all plots, the input state has an amplitude of $\alpha_0 = 0.5$.

success (Eq. (7.27)) can be written as a sum of two terms

$$p_S^{(\mathrm{phy})} = \underbrace{\mathrm{Tr}\left(M_{S,1}\rho_{\mathrm{in}}M_{S,1}\right)}_{p_{S,1}^{(\mathrm{phy})}} + \underbrace{\mathrm{Tr}\left(M_{S,2}\rho_{\mathrm{in}}M_{S,2}\right)}_{p_{S,2}^{(\mathrm{phy})}} , \tag{7.33}$$

where $p_{S,2}^{(\mathrm{phy})}$ is independent of g. Similarly to MB-NLA (Eq. (7.32), the first term contributes to a proper amplification while the second term accounts for the events lies beyond the truncation point. For a coherent input state, this expression can be written analytically as [172]

$$\begin{aligned} p_S^{(\mathrm{phy})} =& 1 - Q\left(N_{\mathrm{c}}+1, |\alpha_0|^2\right) + \\ & g^{-2N_{\mathrm{c}}} \exp\left[\left(g^2-1\right)|\alpha_0|^2\right] Q\left(N_{\mathrm{c}}+1, |g\alpha_0|^2\right) \ , \end{aligned}$$

where $Q(N,\lambda)$ is the regularised incomplete gamma function defined as

$$Q\left(N,\lambda\right) = \Gamma\left(N,\lambda\right)/\Gamma\left(N\right) \ ,$$

where $\Gamma\left(N,\lambda\right)$ and $\Gamma\left(N\right)$ are the incomplete and complete gamma function, respectively. Similarly to the MB-NLA, the probability of success is plotted as a function of the NLA gain for different photon number cut-off values (Fig. 7.6(b)). The trend is similar to that of the MB-NLA, that is the higher the cut-off N_{c}, the lower the probability of success due to a better approximation of the ideal NLA. While the link between the MB-NLA cut-off α_{c} and P-NLA photon number cut-off N_{c} is not immediate due to different implementation mechanism, comparison of the plots suggests that that the probability of success of the former is less optimistic. For example, with the gain of 2, the output Q-distributions of the amplifiers at cut-off values of $\alpha_{\mathrm{c}} = 4$ and $N_{\mathrm{c}} = 3$ exhibit similar features (Fig. 7.4(e) and 7.5(i)). However, the probability of success differs by more than 2 orders of magnitude. Of course, it is reminded that the P-NLA in comparison is an optimal theoretical bound [172], and the practical realisation would have lower success probability due to experimental imperfection such as detection efficiency [171].

7.5.4 Discussion and summary

We have shown that our MB-NLA is equivalent to its physical counterpart for entanglement distillation protocol when considering the situation where the amplification directly precedes the measurement. This equivalence allows us to extend this technique to CV-QKD, where the potential benefits have been explored in Refs. [174, 183, 184]. Such interchangeability with measurement-based implementation is also of great practical advantage because it avoids the complications arise from physical implementation, such as restriction to small input states due to inefficiencies of source and measurements [194, 164, 165, 195].Although a deterministic phase-insensitive amplifier [191] inevitably incurs noise to its output, one can get the best of both worlds by considering the possibility of a hybrid system to perform operations such as enhancement of the signal-to-noise ratio and universal cloning [196], which we shall discuss in the next chapter.

Chapter 8

Heralded Hybrid Linear Amplifier for Quantum Cloning

> *"If people reach perfection they vanish, you know."*
>
> – T.H. White, *The Once and Future King*

Overview

The no-cloning theorem states that an unknown quantum state cannot be cloned exactly and deterministically due to the linearity of quantum mechanics. Associated with this theorem is the quantitative no-cloning limit that sets an upper bound to the quality of the generated clones. However, this limit can be circumvented by abandoning determinism and using probabilistic methods. Here, we report an experimental demonstration of probabilistic cloning of arbitrary coherent states that clearly surpasses the no-cloning limit. Our scheme is based on a hybrid linear amplifier that combines an ideal deterministic linear amplifier with a heralded measurement-based noiseless amplifier. We demonstrate the production of up to five clones with the fidelity of each clone clearly exceeding the corresponding no-cloning limit. This work is a collaborative work between University of Queensland (UQ) and the Australian National University (ANU), where the theory is conceived in UQ and the experiment is conducted in ANU. Most of the contents in this chapter have been published in the following articles:

- J. Y. Haw, J. Zhao, J. Dias, S. M. Assad, M. Bradshaw, R. Blandino, T. Symul, T. C. Ralph, and P. K. Lam,
  "Surpassing the no-cloning limit with a heralded hybrid linear amplifier for coherent states," Nature Communications, 7: 13222. (2016).

- J. Zhao, J. Dias, J. Y. Haw, T. Symul, M. Bradshaw, R. Blandino, T. Ralph, S. M. Assad, P. K. Lam.
  "Quantum enhancement of signal-to-noise ratio with a heralded linear amplifier," Optica 4 (11), 1421-1428. (2017)

8.1 Introduction

The impossibility to perfectly duplicate an unknown quantum state deterministically, known as the no-cloning theorem [5], lies at the heart of quantum information theory and guarantees the security of quantum cryptography [197, 198]. This no-go theorem, however, does not rule out the possibility of imperfect cloning. The idea of generating approximate copies of an arbitrary quantum state was conceived by Buzek and Hillery in their seminal work [199] with the proposal of universal quantum cloning machine. This discovery has since sparked intense research in both discrete [200, 201, 202, 203] and continuous variable [204, 205, 206, 207, 208] systems to explore the fundamental limit of cloning fidelity allowed by quantum mechanics, known as the no-cloning limit. Several quantum cloning experiments approaching the optimal fidelity enforced by this limit have since been demonstrated for single photons [209], polarisation states [210] and coherent states [196].

By forgoing determinism, perfect cloning is not entirely forbidden by the law of quantum physics. In fact, if the quantum states to be cloned are chosen from a discrete, linearly independent set, then the unitarity of quantum evolution does allow probabilistic exact cloning [211, 212, 162, 171, 213]. Non-deterministic high-fidelity cloning of linearly dependent input states can also be performed if the cloning operation is only arbitrarily close to the ideal case [186, 171]. Recently, the invention of probabilistic noiseless linear amplifier (NLA) [160], and its subsequent theoretical studies [168, 167, 163, 214, 215] and implementations [164, 165, 169, 216, 217] in principle provided a method for cloning arbitrary distributions of coherent states with high fidelity via an amplify-and-split approach [164]. In practice, however, implementing NLA for coherent states with amplitude $|\alpha| \geq 1$ remains a technical challenge. This is because the resources required scales exponentially with the coherent state size.

In this chapter, we follow a different path by adopting a method that interpolates between exact-probabilistic and approximate-deterministic cloning [218]. We show that a hybrid linear amplifier, comprising of a probabilistic NLA and an optimal deterministic linear amplifier (DLA) [196, 192], followed by an N-port beam splitter is an effective quantum cloner. Previously, Müller *et al.* [179] demonstrated probabilistic cloning of coherent states which outperformed the best deterministic scheme for input alphabet with random phases but fixed mean photon number. Here, we propose a high fidelity heralded cloning for arbitrary distributions of coherent states and experimentally demonstrate the production of N clones with fidelity that surpasses the Gaussian no-cloning limit $F_N = N/(2N-1)$ [207, 208].

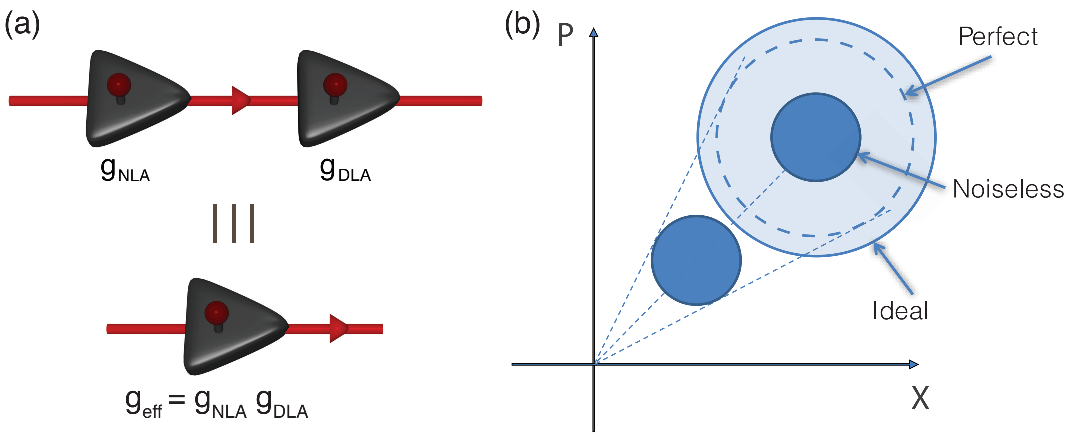


Figure 8.1: (a) Concatenation of a noiseless linear amplifier (NLA) and an ideal deterministic linear amplifier (DLA). (b) Ideal (outer circle), perfect (dashed circle) and noiseless linear amplification (inner circle). By concatenating a DLA with a NLA, we have access to the region between the two amplifiers (light blue), and are able to preserve or even enhance the input SNR.

8.2 Hybrid linear amplifier

8.2.1 Reduced-noise amplifier

In the previous chapter, we have introduced the deterministic and probabilistic linear amplifier. The former, though produces an outcome always, suffers from the degradation in signal-to-noise ratio (SNR). Meanwhile, although an NLA in principle can amplify a quantum state without paying the noise penalty, the success probability can turn out to be infeasible when the demand for input amplitude and gain increases. In turns out that it is actually possible to merge them together into one entity, which we termed a reduced-noise amplifier [219]. As depicted in Fig. 8.1(a), a reduced-noise setup can be formed by a concatenation of DLA and NLA. Such setup can be interpreted as two linear amplifiers with distinct features, complementing each other by sharing the burden of amplification. Lower noise can be achieved at the expense of the probability of success by increasing the NLA gain. Conversely, a higher probability of success, though with an increased noise, can be obtained by increasing the DLA gain. Hence, by tailoring both gains appropriately, one can achieve the desired enhancement of SNR, with vanishing probability of success as the amplification approaches truly noiseless.

One of the figure of merit for an amplifier is the signal transfer coefficient, $\mathcal{T}_s$ defined in Eq (7.15). By considering the action of NLA with gain $g_{\rm NLA}$ in phase space representation [220], a single mode Gaussian state with mean $\mathbf{d} = (\langle\hat{x}\rangle\,,\,\langle\hat{p}\rangle)^T$ and covariance matrices $\mathbf{\Sigma} = \mathrm{diag}(V_x, V_p)$ transforms according to

$$\mathbf{d}_{\mathrm{NLA}} = \begin{pmatrix} \frac{2g_{\mathrm{NLA}}\langle\hat{x}\rangle}{V_x+1-g^2_{\mathrm{NLA}}(V_x-1)} \\ \frac{2g\langle\hat{p}\rangle}{V_p+1-g^2_{\mathrm{NLA}}(V_p-1)} \end{pmatrix}, \tag{8.1}$$

$$\mathbf{\Sigma}_{\mathrm{NLA}} = \begin{pmatrix} \frac{V_x+1+g^2_{\mathrm{NLA}}(V_x-1)}{V_x+1-g^2_{\mathrm{NLA}}(V_x-1)} & 0 \\ 0 & \frac{V_p+1+g^2_{\mathrm{NLA}}(V_p-1)}{V_p+1-g^2_{\mathrm{NLA}}(V_p-1)} \end{pmatrix}. \tag{8.2}$$

For the coherent states with ($V_x = V_p = 1$), Eq. (8.1) reduces to $\mathbf{d}_{\mathrm{NLA}} = g_{\mathrm{NLA}}\mathbf{d}$, i.e. the amplification of the mean is independent of the variance. The signal transfer coefficient for an ideal NLA upon a coherent state is thus in principle is unbounded, $\mathcal{T}_{\mathrm{s}}^{\mathrm{NLA}} = g^2_{\mathrm{NLA}}$. Combining this with the signal transfer coefficient for a DLA (Eq. (7.16)), in which $\mathcal{T}_{\mathrm{s}}^{\mathrm{DLA}} = g^2_{\mathrm{DLA}}/(2g^2_{\mathrm{DLA}} - 1)$, the effective $\mathcal{T}_{\mathrm{s}}$ is given by

$$\begin{aligned} \mathcal{T}_{\mathrm{s}}^{\mathrm{eff}} &= \mathcal{T}_{\mathrm{s}}^{\mathrm{NLA}} \times \mathcal{T}_{\mathrm{s}}^{\mathrm{DLA}} && (8.3) \\ &= \frac{g^2_{\mathrm{NLA}} g^2_{\mathrm{DLA}}}{2g^2_{\mathrm{DLA}} - 1}. && (8.4) \end{aligned}$$

Remarkably, a $\mathcal{T}_{\mathrm{s}}$ of 1, i.e. SNR preserving *perfect* amplification is achievable by setting the $g^2_{\mathrm{NLA}} = 2 - 1/g^2_{\mathrm{DLA}}$. We can also define this in terms of the effective gain $g_{\mathrm{eff}} = g_{\mathrm{DLA}}g_{\mathrm{NLA}}$, giving $g^2_{\mathrm{NLA}} = 2g^2_{\mathrm{eff}}/(g^2_{\mathrm{eff}} + 1)$. We note that in this perfect amplification regime, the gain of the noiseless linear amplifier is upper bounded by 2. Since the probability of success decreases rapidly as a function of gain (See Fig. 7.6), this bound on the NLA gain implies that good probability of success can be attained even for high total effective gain g_{eff}. Beyond the perfect amplification regime, we observe that a reduced-noise amplifier in fact allows us to explore the amplification continuum between the DLA and NLA (Fig. 8.1(b).)

8.2.2 Heralded hybrid linear amplifier

A reduced-noise probabilistic amplifier, though attractive in terms of flexibility in gain and noise level, might be difficult to be realised in practise. As discussed in Sec. 7.1, it is generally technically challenging in the implementation of a P-NLA, let alone the requirement of tunability in gain power to meet the required SNR. Although a direct application of MB-NLA is conceivable, the approach of measurement-based would imply the loss of the propagating quantum state.

This predicament can be mitigated with the observation that when the probabilistic gain is less than the deterministic gain, $g_{\mathrm{NLA}} < g_{\mathrm{DLA}}$, the reduced-noise amplifier can be translated to a linear optical setup [192] with an embedded measurement-based NLA (MB-NLA) (Fig. 8.5b). Since the measurement outcome of such a composite device is heralded, we termed it as a heralded hybrid linear amplifier (HLA).

We now show how concatenating an NLA and a DLA (Fig. 8.2a) can be transformed

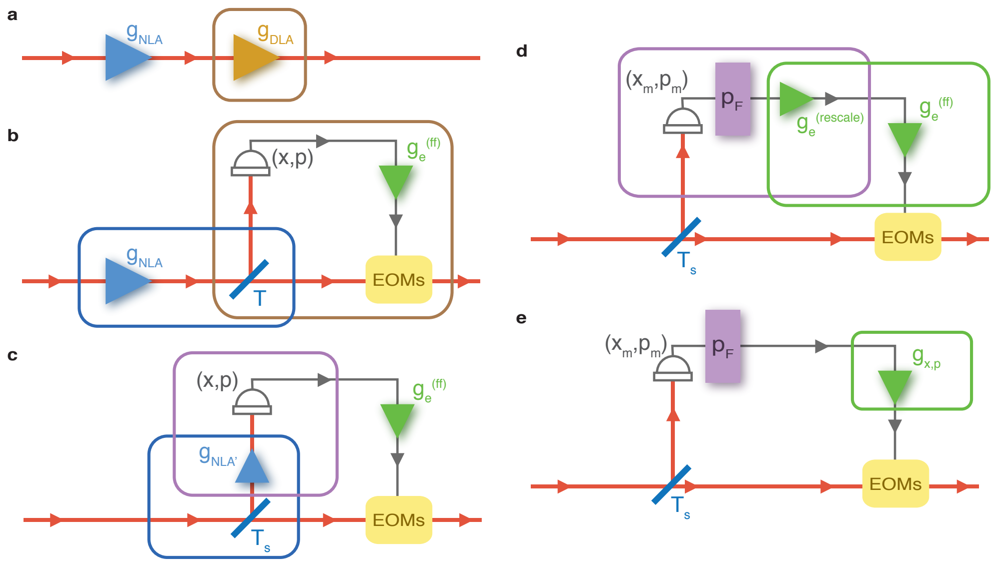


Figure 8.2: Hybrid Linear Amplifier. (**a**) The general concatenated amplifier, consisting a noiseless linear amplifier (NLA) followed by a deterministic linear amplifier (DLA). (**b**) An optical implementation of the DLA with a beam splitter of transmission T and electronic gain $g_{\mathrm{e}}^{(\mathrm{ff})}$. (**c**) When $g_{\mathrm{NLA}} < g_{\mathrm{DLA}}$, the NLA and beam splitter T can be substituted by an effective NLA (NLA′) at the reflection port of a beam splitter T_{s}. (**d**) The NLA′ followed by a dual-homodyne detection with outcomes (x, p) is replaced by a heralding function p_{F} with an electronic rescaling $g_{\mathrm{e}}^{(\mathrm{rescale})}$ acting upon measurement outcomes $(x_{\mathrm{m}}, p_{\mathrm{m}})$. (**e**) The two electronic gains are combined into $g_{\mathrm{x,p}}$. EOMs, electro-optical modulators.

to a probabilistic linear optical setup (Fig. 8.2(e)). In our scheme, the deterministic amplification can be implemented by a linear optical feed-forwarding circuit discussed in Sec. 7.2.3, which is shown in Fig. 8.2b. A beam splitter with transmission

$$T = \frac{1}{g_{\mathrm{DLA}}^2}, \tag{8.5}$$

is used to tap off the noiselessly amplified state. The reflected beam is subjected to a dual homodyne measurement whose outcome $d = (x, p)$ is electronically amplified with gain

$$g_{\mathrm{e}}^{(\mathrm{ff})} = \sqrt{2\left(g_{\mathrm{DLA}}^2 - 1\right)}. \tag{8.6}$$

This amplified signal is feed-forwarded to the transmitted beam to displace it by $g_{\mathrm{e}}^{(\mathrm{ff})} d$ via electro-optical modulators (EOMs).

As described in [174], this same output state can be obtained by a different setup (Fig. 8.2c) where the NLA is moved from the input to the reflected port with a modified gain

$$g_{\mathrm{NLA}'} = \sqrt{\frac{1 - T}{1 - T g_{\mathrm{NLA}}^2}}\, g_{\mathrm{NLA}}, \tag{8.7}$$

and the beam splitter is replaced by a beam splitter with transmission

$$T_{\rm s} = T g_{\rm NLA}^2 = g_{\rm NLA}^2 / g_{\rm DLA}^2. \tag{8.8}$$

These setups are equivalent provided $g_{\rm NLA} < g_{\rm DLA}$. The reason for going to this alternate setup is that now we have a situation where the NLA is followed by a dual-homodyne detection which can be implemented by a measurement-based NLA (MB-NLA) [175, 185]. The MB-NLA consists of a Gaussian heralding function $p_{\rm F}$, followed by a rescaling factor

$$g_{\rm e}^{(\rm rescale)} = \frac{1}{g_{\rm NLA'}}. \tag{8.9}$$

This rescaling factor is combined with $g_{\rm e}^{(\rm ff)}$ to give a net electronic gain of

$$\begin{aligned} g_{\rm x,p} &= g_{\rm e}^{(\rm rescale)} g_{\rm e}^{(\rm ff)} \\ &= \sqrt{2\left(\frac{1}{T_{\rm s}} - 1\right)}, \end{aligned} \tag{8.10}$$

as shown in Fig. 8.2e.

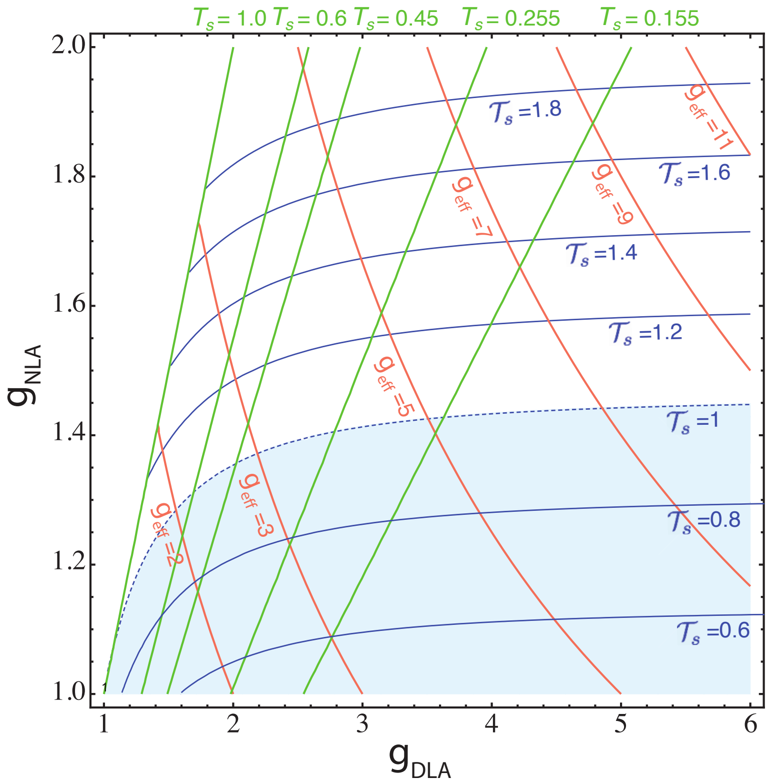


Figure 8.3: Tunability of the amplifier. Signal transfer coefficient (blue contours), various effective gains (red contours), and T' (green lines) as the function of $g_{\rm NLA}$ and $g_{\rm DLA}$. The blue-dotted line denotes SNR preserving amplification ($\mathcal{T}_{\rm s} = 1$) while the enclosed shaded area refers to the region where additional noise is introduced.

Figure 8.3 illustrates the operational degrees of freedom of our noise-reduced linear amplifier. The amount of noise reduction depends on both the product and the ratio of $g_{\rm NLA}$ and $g_{\rm DLA}$, which correspond to, respectively, the values of the effective gain $g_{\rm eff}$ and the transmittivity $T_{\rm s}$ in Fig. 8.2. Intuitively, for a fixed effective gain $g_{\rm eff}$, a higher signal transfer coefficient $\mathcal{T}_{\rm s}$ is achieved with a larger $g_{\rm NLA}$, since the associated noise determined by $g_{\rm DLA}$ decreases while the input amplitude undergoes the same amount of amplification. Hence, under the same effective gain, a higher $T_{\rm s}$ would always lead to a larger signal transfer coefficient.

8.3 Hybrid cloning machine

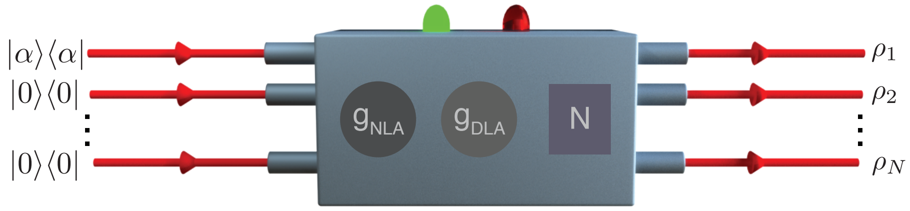


Figure 8.4: Hybrid Cloning Machine. An N-port hybrid cloning machine (HCM), consisting of two control knobs: a probabilistic noiseless linear amplifier (NLA) gain ($g_{\rm NLA}$) and a deterministic linear amplifier (DLA) gain ($g_{\rm DLA}$). Heralded successful events (symbolised by a green light) produce N clones (ρ_i) of coherent state $|\alpha\rangle$ with noise less than the deterministic approach, while unsuccessful events (red light) will be discarded.

As discussed in Sec. 7.2.1 quantum amplification and cloning are closely related concepts, as the no-go of one implies the impossibility of the other. By subjecting the output of a hybrid linear amplifier to an N-port beam splitter, we obtain a total gain of

$$g = g_{\rm NLA} g_{\rm DLA}/\sqrt{N}. \tag{8.11}$$

Quantum cloning can be achieved when the gain is set to unity, i.e. $g = 1$. Upon setting $T_{\rm s}$ and the number of clones N, the corresponding $g_{\rm NLA}$ and $g_{\rm DLA}$ at unity gain can be determined from Eq. (8.8). Combining Eq.s (8.8) and (8.11), we note that as long as $T_{\rm s} > 1/N$, $g_{\rm NLA}$ will always be bigger than 1, enabling the hybrid operation of the cloning machine. Our heralded hybrid cloning machine (HCM) is depicted conceptually in Fig. 8.5a, where an N-copy cloner is parametrised by an NLA amplitude gain ($g_{\rm NLA}$) and an optimal DLA gain ($g_{\rm DLA}$). By introducing an arbitrary input coherent state of $|\alpha\rangle$, and setting the total gain to unity,

$$g = g_{\rm NLA} g_{\rm DLA}/\sqrt{N} = 1, \tag{8.12}$$

HCM will generate N clones with identical mean α and quadrature variance $1+2(g_{\rm DLA}^2 -$

$1)/N$ (where the quantum noise level is 1). Since the probabilistic amplification incurs no noise at all, the variance is a function of g_{DLA} only.

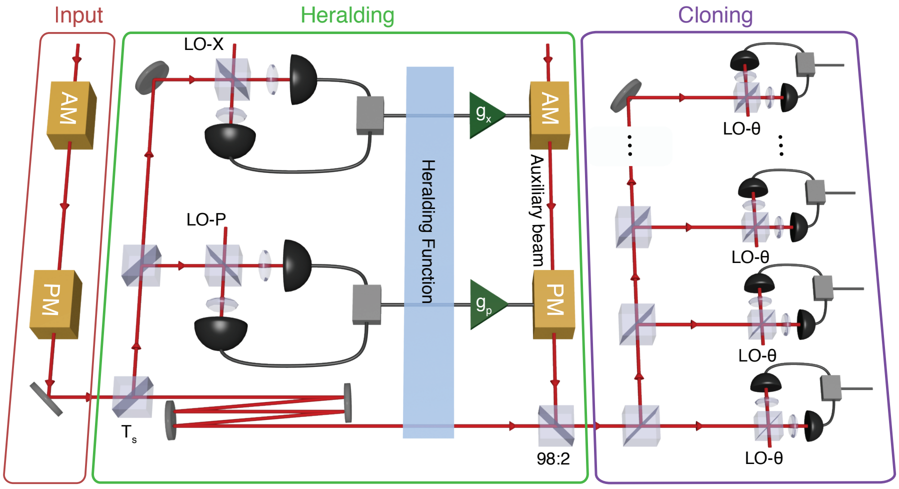


Figure 8.5: Experimental schematic for HCM. When $g_{\mathrm{NLA}} < g_{\mathrm{DLA}}$, the cloning machine can be realised by a feed-forward scheme. The input coherent state passes through a beam splitter with transmitivity T_s, where both conjugate quadratures of the reflected port are measured via a dual-homodyne detection setup. The measurement outcomes pass through a heralding function and the successful events are then amplified with gain $g_{x,p}$ to displace the corresponding transmitted input state via a strong auxiliary beam. An N-port beam splitter finally creates N clones, which are characterised by homodyne measurements on quadratures $\theta = \{X, P\}$. $|0\rangle$, vacuum state; LO, local oscillator; 98:2, 98% transmissive, 2% reflective beam splitter; AM, amplitude modulator; PM, phase modulator.

A key feature in our implementation is the observation that when the probabilistic gain is less than the deterministic gain, $g_{\mathrm{NLA}} < g_{\mathrm{DLA}}$, the hybrid amplifier can be translated to a linear optical setup [192] with an embedded MB-NLA (Fig. 8.5b). This equivalence is illustrated in Fig. 8.2. The MB-NLA is the post-selective version of the physical realisation of NLA that has been proposed [175, 221] and experimentally demonstrated recently [185]. Compared to its physical counterpart, MB-NLA offers the ease of implementation and avoids the predicament of demanding experimental resources. By deploying MB-NLA as the heralding function in a feed-forward control setup [193], HCM preserves the amplified quantum state, extending the use of the MB-NLA beyond point-to-point protocols such as quantum key distribution.

8.3.1 Cloning protocol

To clone an input coherent state, we first tap off part of the light with a beam splitter of transmission

$$T_{\mathrm{s}} = (g_{\mathrm{NLA}}/g_{\mathrm{DLA}})^2, \tag{8.13}$$

which is then detected on a dual-homodyne detector setup locked to measure the amplitude and phase quadratures (X and P). A probabilistic heralding function, which is the probabilistic quantum filter function of a MB-NLA [175, 185], is then applied to the measurement outcome. By post selecting the dual-homodyne data with higher amplitude, the heralding function gives rise to an output distribution with higher overall mean. We will discuss this in more details in Sec. 8.3.2.

The heralded signal is then scaled with gain $g_{\mathrm{x,p}} = \sqrt{2\,(1/T_{\mathrm{s}} - 1)}$ and used to modulate an auxiliary beam. The auxiliary beam is combined with the transmitted beam using a 98:2 highly transmissive beam splitter, which acts as a displacement operator to the transmitted beam [222]. Finally, the combined beam passes through an N-port beam splitter to create N-clones, which is then verified by homodyne measurements.

In our experiment, the dual-homodyne measurement heralds successful operation shot-by-shot. This is then paired up with the corresponding verifying homodyne measurements to select the successful amplification events. The accumulated accepted data points give the distribution of the conjugate quadratures of the successful clones. The processing of the input coherent state at different stages of the HCM is illustrated by Fig. 8.6a.

It is instructive to compare our scheme to that of ref. [179], where probabilistic cloning of fixed-amplitude coherent states was demonstrated. In [179], the amplification is performed by a phase-randomized displacement and phase insensitive photon counting measurement, which have to be optimised according to input amplitude. In our scheme, the amplitude and the phase of the input state is a priori unknown. Moreover, owing to the phase-sensitive dual-homodyne measurement and coherent feed-forward control in DLA [214, 223], the state to be cloned is amplified coherently in the desired quadrature. The integration of MB-NLA in HCM, which emulates a phase-preserving noiseless amplification, further enhances the amplitude of the signal while maintaining its phase.

8.3.2 Implementation of measurement-based noiseless linear amplifier

Here we give a brief summary of the MB-NLA implementation in our protocol. The NLA with gain $g_{\mathrm{NLA}'}$ on the reflected mode followed by a dual-homodyne measurement can be replaced by a direct dual-homodyne measurement on the reflected mode, whose outcomes $\alpha_{\mathrm{m}} = (x_{\mathrm{m}} + ip_{m})/\sqrt{2}$ are used to herald successfully cloned states. These measurement data points α_{m} are accepted with probability

$$p_{\mathrm{F}}\left(\alpha_{\mathrm{m}}\right) = \begin{cases} \frac{1}{M}\exp\left[|\alpha_{\mathrm{m}}|^{2}\left(1-\frac{1}{g_{\mathrm{NLA}'}^{2}}\right)\right] & \text{if } |\alpha_{\mathrm{m}}| < |\alpha_{\mathrm{c}}|, \\ 1 & \text{otherwise.} \end{cases} \tag{8.14}$$

Here $|\alpha_\mathrm{c}|$ is the NLA cut-off and $M = \exp\left[|\alpha_\mathrm{c}|^2\left(1 - 1/g^2_{\mathrm{NLA}'}\right)\right]$ ensures that the output is normalized properly. This heralding function, $p_\mathrm{F}\left(\alpha_\mathrm{m}\right)$, together with the rescaling factor (Eq. (8.9)), can be made arbitrarily close to an ideal NLA operation g^n, where n is the number operator.

Next, we describe how the parameters $g_{\mathrm{NLA}'}$ and $|\alpha_\mathrm{c}|$ are chosen in Eq. (8.14). For both X and P quadratures, the gain $g_{\mathrm{NLA}'}$ is chosen such that the inferred mean of N clones prior to splitting equals to that of the amplified input mean to ensure average unity gain. For the quadrature with zero mean, $g_{\mathrm{NLA}'}$ will be tuned such that the variance matches the value given by the experimental model with imperfect dual-homodyne detection efficiency. In all cloning protocols, only two clones are directly measured. Based on the N-port splitting ratios, the mean and the variance of the remaining clones for $N > 2$ can be evaluated either from rescaled data from different cloning runs or from an estimation of the remaining transmission power.

The cut-off parameter $|\alpha_\mathrm{c}| > 0$ determines how closely the MB-NLA approximates an ideal NLA. A larger cut-off parameter implements the ideal NLA more accurately at the cost of a lower probability of success. The accuracy and the success probability also depend on the $g_{\mathrm{NLA}'}$ and the amplitude of the coherent state. The probability distribution of a dual-homodyne measurement on $\rho = |\alpha_0\rangle\langle\alpha_0|$ is given by

$$\begin{aligned} Q(\alpha_\mathrm{m}) &= \frac{1}{\pi}\langle\alpha_\mathrm{m}|\rho|\alpha_\mathrm{m}\rangle \\ &= \frac{1}{\pi}\exp\bigl(-|\alpha_\mathrm{m} - \alpha_0|^2\bigr), \end{aligned} \tag{8.15}$$

which is centred around α_0 with the variances Var(Re(α_m)) $=$ Var(Im(α_m)) $= 0.5$. Applying the probabilistic filter Eq. (8.14) on the distribution $Q(\alpha_\mathrm{m})$ results in a two-dimensional Gaussian distribution with amplified mean and variance of $g^2_{\mathrm{NLA}'}\alpha_0$ and $0.5g^2_{\mathrm{NLA}'}$, respectively. To implement the NLA with high fidelity, we propose the following cut-off value for the distribution:

$$\mathrm{Re}(\alpha_\mathrm{c}) = g^2_{\mathrm{NLA}'}\mathrm{Re}(\alpha_0^{\mathrm{max}}) + \beta(\sqrt{0.5}g_{\mathrm{NLA}'}), \tag{8.16}$$

and similarly for Im(α_c). Here, α_0^{max} is the expected maximum input amplitude involved in the cloning protocols. In our experiment, β is chosen to ensure more than 98% of the data are within the cut-off value for both the two-clone and multi-clone protocols.

Finally, the probability of success for input state $|\alpha_0\rangle$ can be obtained by integrating the function $p_\mathrm{F}\left(\alpha_\mathrm{m}\right)$ (Eq. (8.14)) with the dual-homodyne distribution $Q(\alpha_\mathrm{m})$.

8.4 Experimental details

Our hybrid cloning machine is shown in Fig. 8.5b. The coherent state is created by modulating the sidebands of a $1064\,\mathrm{nm}$ laser at $4\,\mathrm{MHz}$ with a pair of phase and amplitude modulators. The mean of the coherent state is set by the modulation strength.

In the cloning stage, the input mode is split by a variable beam splitter consisting of a half-wave plate and a polarising beam splitter with transmitivity $T_{\mathrm{s}} = (g_{\mathrm{NLA}}/g_{\mathrm{DLA}})^2$. An optical dual-homodyne measurement is performed on the reflected beam, where the measurement outcome is further split into two parts. The first part is used to extract the $4\,\mathrm{MHz}$ modulation by mixing it with an electronic local oscillator, before being low pass filtered at $100\,\mathrm{kHz}$ and oversampled on a 12-bit analog-to-digital converter at $625\,\mathrm{kSamples}$ per second. The data is used to provide the heralding signal. The second part of the output is amplified electronically with a gain $g_{\mathrm{x,p}}$ and sent to a pair of phase and amplitude modulators, modulating a bright auxiliary beam. This beam is used to provide the displacement operation by interfering it in phase with the delayed transmitted beam on a 98:2 beam splitter. The delay on the transmitted beam ensures that it is synchronised to the auxiliary beam at the beam splitter. The combined beam is then split by an N-port splitter to generate clones. The clones are then verified individually by the same homodyne detector. Two conjugate quadratures X and P are recorded and used to characterise the Gaussian output. For each separate homodyne detection at least 5×10^7 data points are saved. We note that in evaluating the fidelities, we take into account the detection efficiency and losses to avoid an overestimation of the fidelity (See Sec. 8.7).

8.5 Two clones

To benchmark the performance of the HCM, Fig. 8.6b demonstrates the universality of the cloning machine by showing the cloning results of four coherent input states with different complex amplitudes $|x/2 + ip/2\rangle$, where $(x, p) = (-0.71, 0.72)$, $(-0.01, -1.51)$, $(2.23, 2.19)$ and $(-5.26, -0.02)$. The figure of merit we use is the fidelity $F = \langle\alpha|\rho_i|\alpha\rangle$, which quantifies the overlap between the input state $|\alpha\rangle$ and the i-th clone ρ_i. Using a setting of $T_{\mathrm{s}} \approx 0.6$, our device clones the four input states with average fidelities of 0.695 ± 0.001, 0.676 ± 0.005, 0.697 ± 0.001 and 0.681 ± 0.008, respectively. All of the experimental fidelities are significantly higher than that of a classical measure-and-prepare (M&P) cloner ($F_{\mathrm{M\&P}} = 0.5$), where the clones are prepared from a dual-homodyne measurement of an input state [224]. More importantly, all the clones also surpass the no-cloning limit of $F_2 = 2/3$, which is impossible even with a perfect deterministic cloning machine.

To further analyse the HCM, we examine in detail the cloning of an input state $(x, p) = (2.23, 2.19)$ ($|\alpha| = 1.56$). This experiment is repeated 5×10^7 times, from which about 5.9×10^5 runs produced successfully heralded clones. The electronic gain $g_{\mathrm{x,p}}$ and the splitting ratio of the beam splitter are carefully tuned to ensure that the two clones produced are nearly identical. The probabilistic heralding function was chosen to ensure that the output clones have exactly unity gain. This is done to prevent any overestimation of the fidelity (see Sec. 8.7 and Fig. 8.10). As can be seen in Fig. 8.7c, the produced clones have noise significantly lower than the M&P cloning protocol.

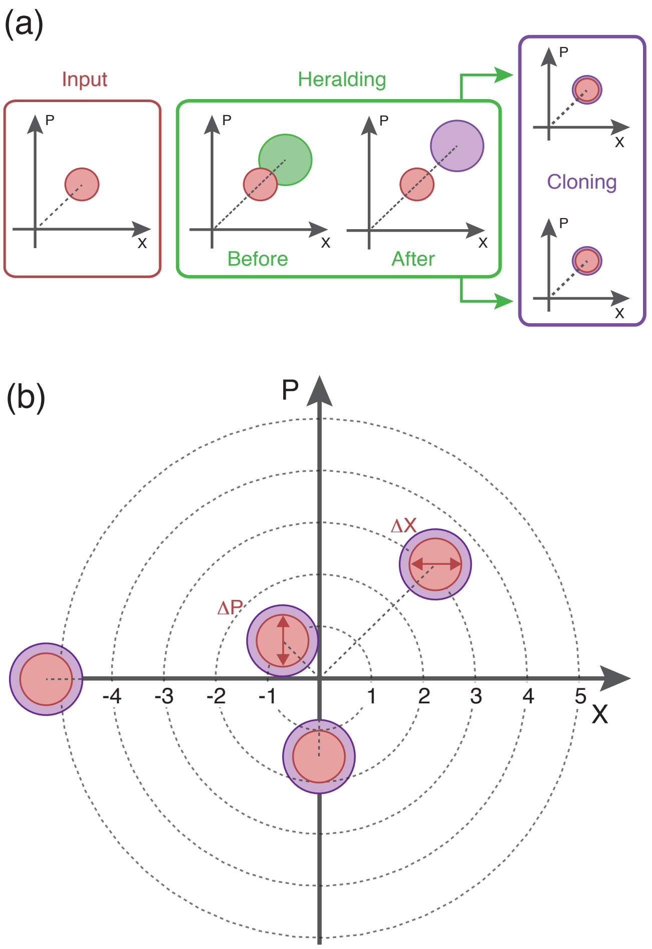


Figure 8.6: (a) Phase space representation of the deterministic-probabilistic hybrid cloning approach. The input state is first deterministically amplified before being heralded to produce a target state which is split into two clones. (b) Cloning of distinct input states. Since both the deterministic and noiseless linear amplifiers are invariant to the input state, any unknown coherent state can be cloned in the same way.

Since the noise variance is only affected by the deterministic amplification, setting $g_{\text{NLA}} > 1$ will reduce the required DLA gain while still achieving unity gain. As a result, the clones produced by our HCM will have less noise compared to its deterministic counterpart. The data points also show that the heralded events (purple region of Fig. 8.7c right) have Gaussian distributions with mean equal to that of the input state. We experimentally obtained a fidelity of 0.698 ± 0.002 and 0.697 ± 0.002 for the two clones. The fidelity plot in Fig. 8.7d clearly demonstrates that the fidelities of both clones exceed not only the M&P limit but also lie beyond the no-cloning limit by more than 15 standard deviations.

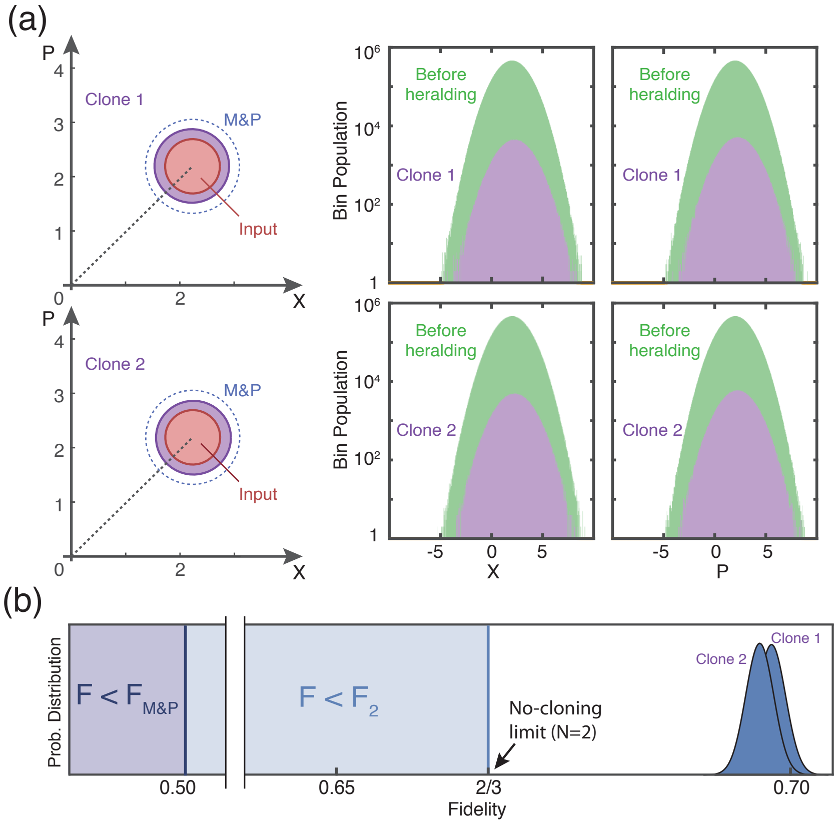


Figure 8.7: (a) Cloning of coherent state $(x, p) = (2.23, 2.19)$. Left, noise contours (1 standard deviation width) of the Wigner functions of the input state (red circle) and the clones from a measure-and-prepare (M&P) cloning machine (dashed blue) and an hybrid cloning machine (purple circle). Right, Quadrature measurement histograms constructed from 5×10^7 homodyne measurements before (green) and 5.9×10^5 measurements after heralding (purple). (b) Probability distributions of the fidelity of the clones. Both clones surpass the fidelity limits imposed by the M&P cloner ($F_{\text{M\&P}} = 0.5$) and the deterministic cloner ($F_2 = 2/3$).

8.6 Multiple clones

We operate our HCM at higher gains to enable the production of more than two clones. In order to have $g_{\text{NLA}} > 1$, from equations (8.12) and (8.13), we require $g_{\text{DLA}} < \sqrt{N}$, which leads to $T_{\text{s}} > 1/N$. Hence, by tailoring T_{s} for each N, HCM can produce N clones with fidelity beating the deterministic bound F_N with the desired probability of success. Fig. 8.8a shows the fidelity of the multiple clones with an input of $|\alpha| \approx 0.5$. The average fidelities of the clones for $N = 2, 3, 4$ and 5 are 0.695 ± 0.002, 0.634 ± 0.012, 0.600 ± 0.009 and 0.618 ± 0.008, respectively, clearly surpassing the corresponding no-cloning limit. In Fig. 8.8b, we plot the theoretical prediction of the fidelity as a function of the probability of success with the experimental data. The theoretical fidelity is modelled upon the dual-homodyne detection efficiency of $90 \pm 5\%$, which is the main source of imperfection (see Sec. 8.7). We find that our results lie well within the expected fidelities, with the probability of success ranging between 5% to 15%. Remarkably, by keeping 5% of the

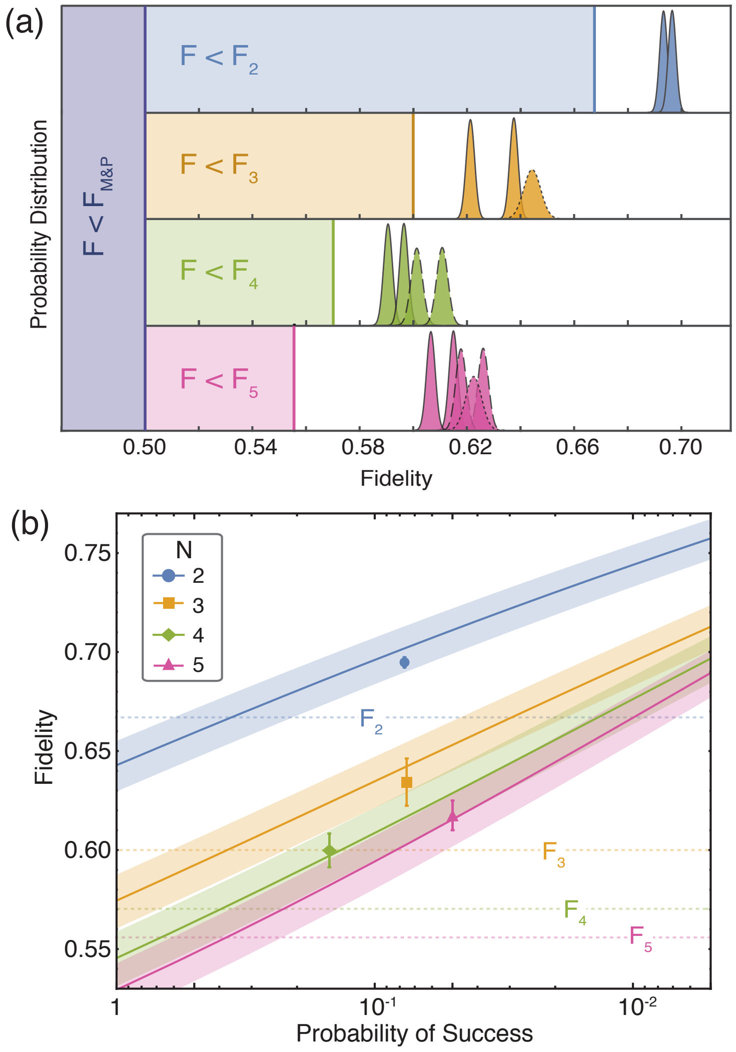


Figure 8.8: (**a**) Fidelity of N clones beyond the no-cloning limit. By applying appropriate deterministic and probabilistic gains on the input $|\alpha| \approx 0.5$, clones with fidelity exceeding their corresponding no-cloning limits $F_N = N/(2N-1)$ are produced. For $N > 2$, only two of the output clones are directly measured (solid lines). The remaining $N-2$ clones' fidelity distributions are obtained either from rescaled data of different runs (dashed) or estimation of the remaining intensities (dotted). A sample size of 5×10^7 data points is used for all N. The spreads in fidelity distributions are predominately due to imperfect splitting. (**b**) Fidelity as a function of heralding probability of success for different N. Theoretical simulations (solid lines) are superimposed with the experimental points (symbols) and the no-cloning limits F_N (dotted lines). Error bars represent 1 standard deviation of clones' fidelities and the shaded regions are theoretically expected fidelities from 1 standard deviation of the dual-homodyne detection efficiency.

data points, the average cloning fidelity for $N = 5$ can be enhanced by more than 15%, and hence exceeding the no-cloning limit F_5 by 11.2%. For deterministic unity gain cloners, as long as N clones are produced each with fidelity $F > F_{N+1}$ [208, 207], one may conclude that there are no other clones with equal or higher fidelity. Here we show

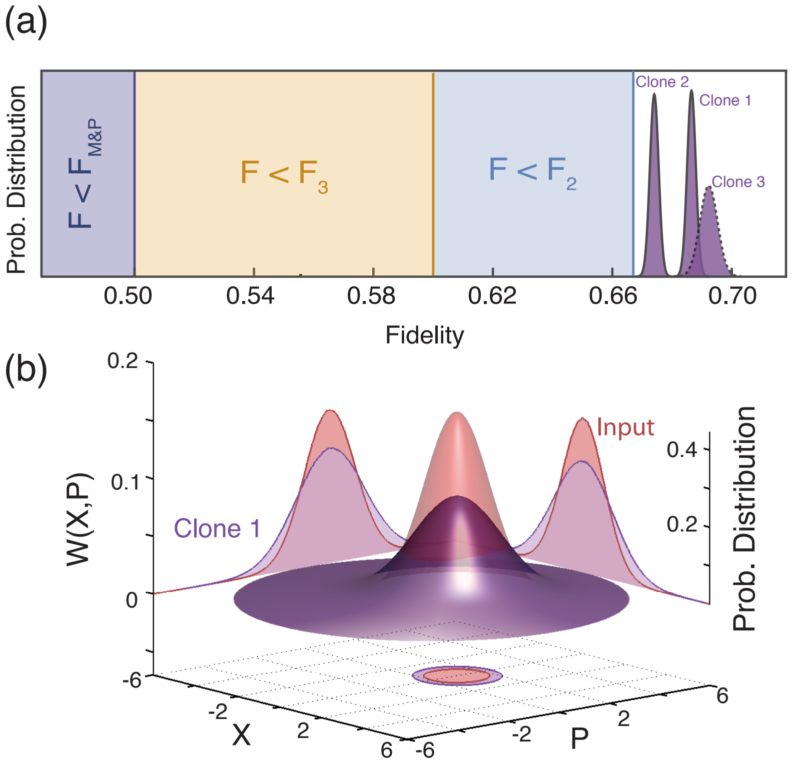


Figure 8.9: Three clones with fidelity $F > F_2$ and F_3. The experimentally reconstructed Wigner functions of the input (red) and clone 1 (purple) together with their normalized probability distributions for both X and P quadratures.

that this is not necessarily the case for probabilistic cloning. By further increasing NLA gain, we successfully produce three clones, each with fidelity $F > F_2$ (Fig. 8.9c), and the average fidelity is 0.684 ± 0.009. Given only fidelity, it is impossible for a receiver with only two clones to determine whether the clones originate from a 2-clone or 3-clone probabilistic protocol (Fig. 8.8a and 8.9c). The resulting probability distribution from 7.2×10^6 successful three-clone states out of 5×10^8 inputs and the corresponding experimental reconstructed Wigner function are shown in Fig. 8.9d together with the input state.

The theoretical fidelity for the HCM's clones at unity gain can be shown to be $F_{\text{HCM}} = 1/(1 + (g^2_{\text{DLA}} - 1)/N)$, which is only a function of the deterministic gain and the number of clones. We note that maximum fidelity for a given N can be achieved in the limit of $T_\text{s} \to 1$, giving $F_{\text{max}}(N) = 1/(1 + (\sqrt{N} - 1)/N)$ (See Sec. 8.7). $F_{\text{max}}(N)$ converges to 1 in the limit of an infinite number of clones. However, since this also requires an infinitely large nondeterministic gain, and thus an unbounded truncation in post-selection, the probability of success will be essentially zero.

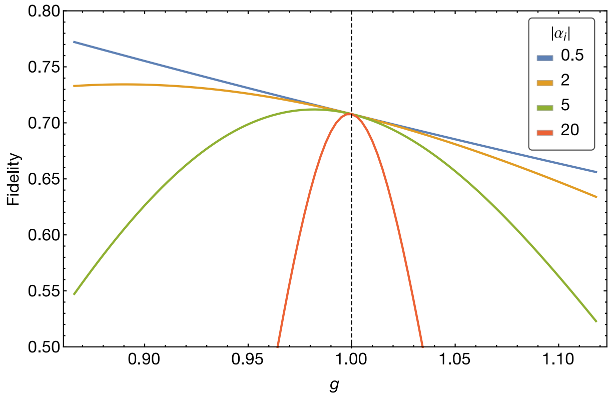


Figure 8.10: Fidelity of two-clone protocol with different input states. Deviation from unity gain (dashed line) can lead to overestimation of fidelity when the amplitude of the input state $|\alpha_{\rm i}|$ is small.

8.7 Fidelity evaluation

The fidelity which quantifies the overlap between the clones and the input state is calculated as a criterion for examining the performance of our HCM. We consider single-mode Gaussian input $\rho_{\rm i}\,(\mathbf{d}_{\rm i}, \mathbf{V}_{\rm i})$ and output $\rho_{\rm o}\,(\mathbf{d}_{\rm o}, \mathbf{V}_{\rm o})$, where $\mathbf{d}_j = (x_j, p_j)$ is the mean of the amplitude and the phase of the state ρ_j while $\mathbf{V}_j = \text{diag}(\sigma_{x_j}, \sigma_{p_j})$ is the corresponding covariance matrix. The fidelity between $\rho_{\rm i}$ and $\rho_{\rm o}$ is given by [24]

$$F(\rho_{\rm i}, \rho_{\rm o}) = \frac{2}{\sqrt{\Delta\ +\delta} - \sqrt{\delta}}\exp\left[-\frac{1}{2}\mathbf{d}^T(\mathbf{V}_{\rm i} + \mathbf{V}_{\rm o})^{-1}\mathbf{d}\right]\ , \tag{8.17}$$

where $\Delta := \det(\mathbf{V}_{\rm i} + \mathbf{V_o})$, $\delta := (\det\mathbf{V}_{\rm i} - 1)(\det\mathbf{V}_{\rm o} - 1)$, and $\mathbf{d} := \mathbf{d}_{\rm o} - \mathbf{d}_{\rm i}$. The fidelity for a coherent state input $\rho_{\rm i}\,(\mathbf{d}_{\rm i}, \mathbf{1})$ is

$$\begin{aligned} F &= \frac{2}{\sqrt{(\sigma_{x_{\rm o}}^2 + 1)(\sigma_{p_{\rm o}}^2 + 1)}} \\ &\quad \exp\left[-\frac{1}{2}\left(\frac{(x_{\rm o} - x_{\rm i})^2}{\sigma_{x_{\rm o}}^2 + 1} + \frac{(p_{\rm o} - p_{\rm i})^2}{\sigma_{p_{\rm o}}^2 + 1}\right)\right]\ . \end{aligned} \tag{8.18}$$

Suppose that the output quadratures are symmetric, and the theoretical output means $\{x_{\rm o}, p_{\rm o}\}$ are given by $\{gx_{\rm i}, gp_{\rm i}\}$ and the variances $\sigma_{x_{\rm o}}^2 = \sigma_{p_{\rm o}}^2 = 1 + 2(g_{\rm DLA}^2 - 1)/N$, respectively. Then, the theoretical fidelity of N clones is thus

$$F(N) = \frac{1}{1 + (g_{\rm DLA}^2 - 1)/N}\exp\left[-\frac{(g-1)^2|\alpha_{\rm i}|^2}{1 + (g_{\rm DLA}^2 - 1)/N}\right]\ .$$

where $\alpha_{\rm i} = (x_{\rm i} + ip_{\rm i})/2$. We emphasize that it is crucial to set the gain of the HCM as close to unity gain as possible. As shown in Fig. 8.10, non-unity gain for small input amplitude may lead to an overestimation of the fidelity. At unity gain, the theoretical fidelity reduces to

$$F(N) = \frac{1}{1 + (g_{\mathrm{DLA}}^2 - 1)/N} , \tag{8.19}$$

which depends only on the deterministic gain and number of clones. The maximum fidelity can be achieved in the limit of $T_\mathrm{s} \to 1$, and from Eq. (8.8) and (8.11), $g_{\mathrm{DLA}}^2 \to \sqrt{N}$, giving

$$F(N) \to F_{\mathrm{max}}(N) = \frac{1}{1 + (\sqrt{N} - 1)/N} . \tag{8.20}$$

Note that although the fidelity goes to 1 as N increases, the probability of success is vanishingly small. This is because at this limit, the cut-off α_c in the heralding function will also scale with the probabilistic gain g_{NLA}^2 to implement the amplification faithfully, thus rejecting essentially most of the data points (c.f. Eq. (8.14)). In practice, the fidelity of HCM is limited by several factors, such as the dual-homodyne efficiency, electronic gain, asymmetry in the quadratures and imperfect N-port splitting ratio. Nevertheless, following [225], a simple model of the imperfection of HCM can be constructed simply by considering the detection efficiencies of the dual-homodyne η_{DH}, which is the dominant source of imperfection. Taking into account the losses and imperfect visibilities, the average dual-homodyne detection efficiency for the amplitude and phase quadratures is $90 \pm 5\%$.

To evaluate the experimental fidelity of the clones, we corrected the homodyne data to ensure proper characterization of both the input state and the clones. This is to avoid overestimation of the fidelity due to underestimation of the clones variances (Fig. 8.10). The total detection efficiency for the input state is typically around 97%, where we have taken into account the quantum efficiency of the photodiodes, mode-matching visibility, and the propagation losses. The detection efficiency of the clones in the verification stage is about 98.5%.

The correct mean can be obtained by rescaling the overall data by $1/\sqrt{\eta_{\mathrm{tot}}}$, where η_{tot} is the total detection efficiency of either the input state or the clones. The corresponding variance can be obtained by subtracting $(1 - \eta_{\mathrm{tot}})/\eta_{\mathrm{tot}}$ from the variance of the rescaled data.

To determine the standard deviation of the fidelity, we take into account the propagation of the uncertainties in the variance of output quadratures. The uncertainty of our fidelity is estimated according to:

$$\mathrm{Var}\left(\sigma_{\tilde{F}}^2\right) = \left(\frac{\partial \tilde{F}}{\partial \sigma_{x_\mathrm{o}}^2}\right)^2 \mathrm{Var}(\sigma_{x_\mathrm{o}}^2) + \left(\frac{\partial \tilde{F}}{\partial \sigma_{p_\mathrm{o}}^2}\right)^2 \mathrm{Var}(\sigma_{p_\mathrm{o}}^2) . \tag{8.21}$$

Here $\tilde{F}$ is

$$\tilde{F} = \frac{2}{\sqrt{(\sigma_{x_\mathrm{o}}^2 + 1)(\sigma_{p_\mathrm{o}}^2 + 1)}}, \tag{8.22}$$

which is obtained by setting $x_\mathrm{o} = x_\mathrm{i}$ and $p_\mathrm{o} = p_\mathrm{i}$ in Eq. (8.18). The variance of the quadrature variances $\mathrm{Var}(\sigma^2_{x_\mathrm{o}})$ and $\mathrm{Var}(\sigma^2_{p_\mathrm{o}})$ are evaluated based on several parameters: number of datapoints, uncertainty of the total detection efficiency and uncertainty of the N-port beam splitter. Finally the standard deviations of the average fidelities are determined from the spread of the fidelity probability distributions.

8.8 Summary

In a nutshell, we have proposed and demonstrated a hybrid cloning machine that combines a deterministic and a probabilistic amplifier to clone unknown coherent states with fidelity beyond the no-cloning limit. Even though an ideal NLA implementation is not possible with our setup, as this would require unity deterministic gain, our hybrid approach does allow the integration of measurement-based NLA in the optimal deterministic amplifier. We showed that our device is capable of high-fidelity cloning of large coherent states and generation of multiple clones beyond the no-cloning limit, limited only by the amount of data collected and the desired probability of success. Our cloner, while only working probabilistically, provides a clear heralding signal for all successful cloning events.

Chapter 9

Conclusion and Future Outlook

9.1 Summary

In this thesis, we have studied two aspects of the continuous variable (CV) quantum communication in detail, namely the security of the quantum devices, and the amplification of quantum state in a communication channel. By carefully redesign and quantify the relevant quantities in the quantum protocols, we have demonstrated novel simple techniques that enhance the security and robustness quantum devices. To summarise:

- **The security of the quantum devices**
  - **CV quantum random number generator (QRNG**)
    We have presented a novel method that leads to the maximization of extractable high-quality randomness without compromising both the integrity and the speed of a QRNG. In fact, within our framework, when the QRNG is appropriately calibrated, the generated random numbers are secure even if the electronic noise is fully known. We showed that depending on the assumption made on the eavesdropper, the ADC range, digitisation bits and the QCNR can be optimised with respect to speed and security. From a practical point of view, our method also relaxes the signal-to-noise ratio requirement on the detector. The final real-time throughput our CV QRNG is 3.55 Gbps, with a potential to achieve up to 70 Gbit/s provided all the available bandwidth and (conditional) min-entropy from our detector (approximately 2.5 GHz) can be harnessed.
  - **One-sided device independent CV quantum key distribution**
    We have proposed and demonstrated that through a recently proved entropic uncertainty principle for the continuous variable, it is possible to establish a one-sided device-independent quantum key distribution (QKD) protocol, where the device of one side of the communicating party needs not be fully trusted. Remarkably, such a coveted protocol could be performed using only coherent states, one of the most readily available resources in the lab. By examining the protocol experimentally, the correlation necessary for 1sDI key distribution up to an applied loss equivalent to 3.5 km of fibre transmission

was measured.

- **Probabilistic linear amplification of quantum state**
  - **Measurement-based quantum amplifier**
    We have studied a hierarchy of quantum amplifiers, and show the interplay between amplification noise and the probability of success in a quantum amplifier. We have reviewed a recent measurement-based noiseless linear amplifier (MB-NLA), and compared it with its physical counterpart. We noted that equivalence between the approaches, and highlighted that care must be taken in choosing the experimental parameters, such as truncation point to ensure a faithful emulation of the NLA.
  - **Heralded hybrid quantum amplifier based cloner**
    By combining an ideal deterministic amplifier with a heralded MB-NLA, we have proposed and demonstrated a hybrid cloning machine that combines a deterministic and a probabilistic amplifier to clone unknown coherent states with fidelity beyond the no-cloning limit. Even though an ideal NLA implementation is not possible with our setup, as this would require zero deterministic gain, our hybrid approach does allow the integration of measurement-based NLA in the optimal deterministic amplifier.

9.2 Future research

For the CV-QRNG, we note several possible extensions of our work. For instance, one can apply entropy smoothing [93, 91] on the worst-case min-entropy to tighten the analysis. Our framework can also be generalized to encapsulate potential quantum side information by considering the analysis described in Ref. [79]. It is also interesting to examine the bound for the accessible entropy without either the description of the source or the measurement device. For example, in [226], the CV entropic uncertainty principle (see Sec. 6.2) in the form of min-max entropies provided a lower bound of the conditional min-entropy without trusting the quantum source. A detailed cryptoanalysis of our framework can also increase the final throughput of the QRNG [101]. Last, a hybrid of an information-theoretic provable and cryptographic randomness extractor is also an interesting avenue to be explored in the construction of a high-speed, side-information (classical and quantum) proof QRNG [104].

In one-sided device independent QKD, an obvious avenue for future work is the investigation of methods to improve long distance performance. One option would be to revisit the restrictions, or lack thereof, made about the eavesdropper including physical assumptions about the quantum memory available to Eve [227, 228, 229], which has already seen applications in DI-DVQKD [230]. Another candidate to further extend the range of these protocols would be the noiseless linear amplifier [194, 164] which has already been proposed for application to fully DI-DVQKD [231]. Even more appealing may be the measurement-based versions of these amplification schemes [184, 183] that have recently been experimentally demonstrated [185] although this could only be applied to RR protocols. In light of these results, it appears that several 1sDI-CVQKD protocols are within the reach of current technology and multiple possibilities exist to extend the secure range of such schemes to long distances.

The notion of noiseless linear amplifier opens up an opportunity for extending the range of a quantum network. Our study on the equivalent measurement-based approach would provide a guideline in determining the best operating parameters while optimising the relevant figure of merit. For example, in NLA-assisted quantum communication protocols [232, 233], one can choose to maximise either the transmission range or the secret key rate. While our analysis here focuses on the emulation of a quantum amplification process, it suggests the possibility of performing other quantum information processing in a measurement-based manner, such as virtual photon subtraction [234] and iterative entanglement distillation [235].

For our heralded hybrid cloning machine (HCM), several comments on the prospects and avenues for future work are in order. An immediate extension is the implementation of HCM in various feed-forward based cloning protocols, such as phase conjugate cloning [236], cloning of Gaussian states [237, 238], telecloning [239], and cloning with prior information [179, 240, 241]. Our tunable probabilistic cloner could further elucidate fundamental concepts of quantum mechanics and quantum measurement, for instance, quantum deleting [242] and quantum state identification [218, 243]. This probabilistic coherent protocol might also play a role in the security analysis of eavesdropping attacks in continuous variable quantum cryptography as well [244, 245]. The implication of HCM in the context of quantum information distributor [246] and quantum computation [247] also demands further investigation.

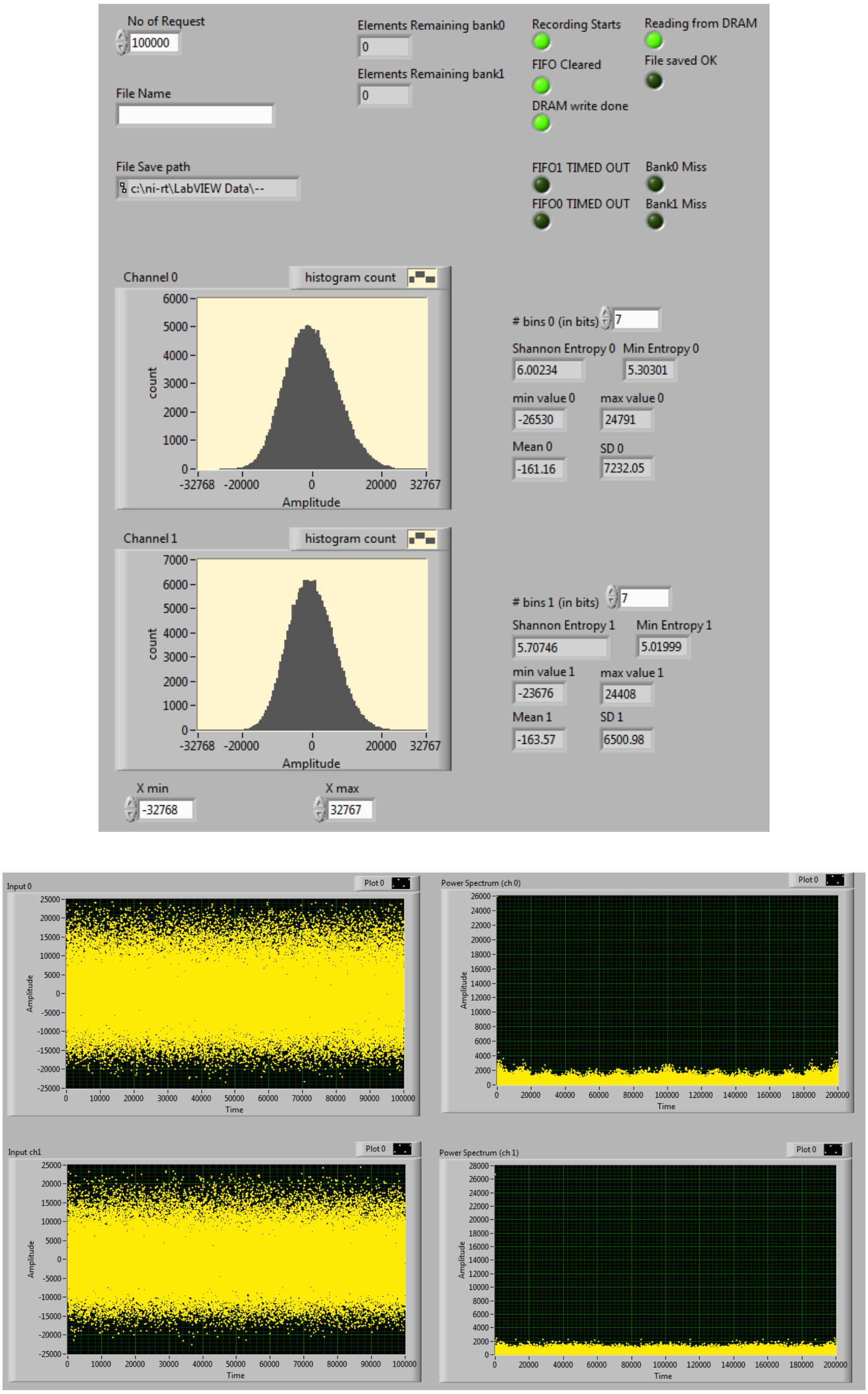
Beyond probabilistic cloning, owing to the composability, tunability, and ease of implementation of this heralded hybrid amplification, it provides several interesting avenues for future research in loss-sensitive quantum information protocols. First, the access to the two variable knobs - deterministic and probabilistic - provides a spectrum of effective gain and success probability. For protocols with high SNR demands, such as long-distance quantum communication [156], the signal transfer coefficient can be enhanced by intensifying the probabilistic gain. When signal transfer speed is the critical requirement, the deterministic amplification can play the leading role while maintaining the same effective gain. An interesting extension of this work would be to study the optimality of these gains for a given channel loss and excess noise in various quantum communication protocols, including quantum key distribution [232], entanglement distillation [164, 178, 185] and quantum repeater [182, 181]. As such, we believe our scheme will be a useful tool in the quest to realise large-scale quantum networks.

Appendix

Appendix A

QRNG LabView Interface

As described in Sec. 5.3.1, National Instrument FPGA is used to collect, analyse and post-process the raw quantum randomness from our continuous variable random number generator. Fig. A.1 shows the Labview interface used to extract consecutive raw data from two independent high-speed analog-to-digital (ADC) channels for analysis.



No of Request 100000

File Name

File Save path c:\ni-rt\LabVIEW Data\--

Elements Remaining bank0 0

Elements Remaining bank1 0

Recording Starts ●

FIFO Cleared ●

DRAM write done ●

Reading from DRAM ●

File saved OK ●

FIFO1 TIMED OUT ●

FIFO0 TIMED OUT ●

Bank0 Miss ●

Bank1 Miss ●

bins 0 (in bits) 7

Shannon Entropy 0 6.00234

Min Entropy 0 5.30301

min value 0 -26530

max value 0 24791

Mean 0 -161.16

SD 0 7232.05

bins 1 (in bits) 7

Shannon Entropy 1 5.70746

Min Entropy 1 5.01999

min value 1 -23676

max value 1 24408

Mean 1 -163.57

SD 1 6500.98

X min -32768

X max 32767

Figure A.1: The LabView interface for the CV-QRNG. (Top) Raw data is stored in RAM before readout to prevent latency issue in collecting the sampled data. The randomness (Shannon entropy and min-entropy) is then estimated from the data histograms. (Bottom) Raw time series and power spectrum from two ADC channels.

Appendix B

1SDI-QKD Secret Key Rate with Imperfect Reconciliation Efficiency

In Sec. 6.4, we derived secret key rates assuming that Alice and Bob achieve the Shannon capacity for their Gaussian encoding, and we recall that the key rate is bounded by Eq. (6.8),

$$K^{\triangleright} \geq I(X_{A_1} : X_B) - \chi(X_{A_1} : E) \tag{B.1}$$

In practise, we will not be able to achieve this ideal capacity and the key rate will instead be bounded by,

$$K^{\triangleright} \geq \beta I(X_{A_1} : X_B) - \chi(X_{A_1} : E) \tag{B.2}$$

where $\beta < 1$ is the information reconciliation efficiency. In this case, instead of using the entropic uncertainty relation to lower bound the secret key rate, we will use it to upper bound Eve's information and then independently measure $\beta I(X_{A_1} : X_B)$ to obtain the actual key rate. Eve's information is upper bounded by the Holevo quantity,

$$\chi(X_{A_1} : E) \leq S(E) - \int \mathrm{d}x_{A_1} \;\; p(x_{A_1}) S(\rho_E^{x_{A_1}}) \tag{B.3}$$

The conditional von Neuman entropy of the observable X_A is given by

$$S(X_{A_1}|E) = h(X_{A_1}) + \int \mathrm{d}x_{A_1} \;\; p(x_{A_1}) S(\rho_E^{x_{A_1}}) - S(E) \tag{B.4}$$

Thus we can rewrite Eve's information as,

$$\chi(X_{A_1} : E) \leq h(X_{A_1}) - S(X_{A_1}|E) \tag{B.5}$$

We now make use of our CV entropic uncertainty relation,

$$S(X_{A_1}|E) + S(P_{A_1}|B) \geq \log 4\pi \tag{B.6}$$

to obtain,

$$\chi(X_{A_1}:E) \leq h(X_{A_1}) + S(P_{A_1}|B) - \log 4\pi \tag{B.7}$$

Using the fact that $S(P_{A_1}|B) \leq S(P_{A_1}|P_B) = h(P_{A_1}|P_B)$ and that the Shannon entropy is maximised by a Gaussian distribution for a fixed variance such that $h_G(X_{A_1}) \leq \log\sqrt{2\pi e V_{X_{A_1}}}$ we finally arrive at,

$$\chi(X_{A_1}:E) \leq \log 2\pi e\sqrt{V_{X_{A_1}} V_{P_{A_1}|P_B}} - \log 4\pi \tag{B.8}$$

Thus the secret key rate for an arbitrary β for the DR protocol where Alice heterodynes (or alternatively prepares coherent states) is given by

$$K^{\triangleright} \geq \beta \log\sqrt{\frac{V_{X_{A_1}}}{V_{X_{A_1}|X_B}}} + \log\frac{2}{e\sqrt{V_{X_{A_1}} V_{P_{A_2}|P_B}}} \tag{B.9}$$

Appendix C

Verification of Quantum Discord

Overview

We introduce and demonstrate experimentally a simple technique to verify quantum discord in Gaussian states and certain class of non Gaussian states prepared by using a beam splitter. We show that quantum discord for Gaussian states can be verified by checking whether the peaks of the conditional marginal distributions corresponding to two different outcomes of homodyne measurement coincide at the same point in the phase space or not. This method is further applied to non-Gaussian states that are statistical mixture of coherent states subjected to a beam splitter. The work in this chapter has appeared in the following publication:

- S. Hosseini, S. Rahimi-Keshari, J. Y. Haw, S. M. Assad, H. M. Chrzanowski, Janousek, J., T. Symul, T. C. Ralph, and P. K. Lam.
"Experimental verification of quantum discord in continuous-variable states."
Journal of Physics B: Atomic, Molecular and Optical Physics, 47(2), p.025503. (2014).

C.1 Introduction

Quantum correlations have been the subject of many studies during the last decades, in particular, as a resource for quantum information processing and quantum communication. Previously, any correlation in the absence of entanglement was thought to be purely classical as they can be prepared with local operations and classical communications. However, there are reasons to believe that this was not the whole story; for example, there are quantum computational models with no or little entanglement, which can efficiently perform tasks that are believed to be classically hard [248, 285]. Quantum discord was introduced as a general measure of quantum correlation that can capture nonclassical correlations beyond entanglement [249]. Discord was suggested as a figure of merit for characterizing the quantum resources in a computational model [250]; it also was introduced as a resource for quantum state merging [286, 287] and for encoding information onto a quantum state [251]. This measure of nonclassical correlation has been extended to continuous-variable systems to study quantum correlations in Gaussian states [252, 253] and certain non-Gaussian states [288].

Considering the importance of quantum discord, of particular interest is to experimentally verify discord for an *unknown* quantum system. Methods have been proposed to test for nonvanishing quantum discord of bipartite discrete-variable quantum states [289, 290, 291, 292, 293, 294, 295], some of which have been experimentally implemented in nuclear-magnetic-resonance systems [296, 297] and in an optical system [298]. Recently a measurement-based method for verifying quantum discord was introduced [299], which can be applied to both discrete- and continuous-variable systems.

Here we introduce and demonstrate a simple and efficient experimental technique for verifying quantum discord in Gaussian states. It was shown that the "if and only if" condition for a bipartite Gaussian state to have zero discord is that there is no correlation between the quadratures of two subsystems, i.e., it is a product state [299]. In our method, we use two homodyne detections to examine the correlations between quadratures of subsystems A and B. For example, if the peaks of the conditional marginal distributions of B's quadrature corresponding to the positive and negative outcomes of homodyne measurements performed on A's quadrature, do not coincide at the same point, those quadratures are correlated. In order to consider all possible correlations, we check the correlations between all four combinations of the amplitude and phase quadratures of A and B. If at least one of them is found to be correlated, quantum discord is nonzero, otherwise it is zero. There is also a simple way to verify quantum discord in bipartite non-Gaussian states prepared by subjecting a statistical mixture of coherent states to one port of a beam splitter while the other port is in the vacuum state. We show that any changes in the conditional marginal distributions observed using our method for this class of bipartite non-Gaussian states indicate nonzero discord. We experimentally demonstrate our technique by preparing Gaussian and non-Gaussian states with no entanglement and verify the presence of quantum discord.

This paper is structured as follows. In Section C.2, we review the theoretical description of quantum discord and introduce our technique to experimentally verify quantum discord in Gaussian states and certain class of non-Gaussian states. In Section C.3, we thoroughly describe the experiments which are performed to examine this method on a Gaussian state and three different non-Gaussian states, and the experimental results are presented in detail. Finally, Section C.4 concludes our main findings.

C.2 Theory

C.2.1 Quantum discord

Quantum discord, is defined as the mismatch between two quantum analogues of classically equivalent expressions of the mutual information [254]. For two classical random variables A and B, the total correlation is given by mutual information, which can be defined by two equivalent expressions $I(A:B){=}H(A){+}H(B){-}H(A,B)$ and $J(A:B){=}H(A){-}H(A|B){\equiv}H(B){-}H(B|A)$, where $H(X)$ is the Shannon entropy and $H(X|Y)$ is the conditional entropy. For a bipartite quantum system, the quantum mutual information is defined by $I(\rho_{AB}){=}S(\rho_A){+}S(\rho_B){-}S(\rho_{AB})$ that is analogous to $I(A:B)$, where $S(\rho){=}-\mathrm{Tr}[\rho\log_2(\rho)]$ is the von Neumann entropy. A measurement-based quantum conditional entropy is $S_{\{\Pi_j\}}(A|B){=}\sum_j p_j S(\rho_{A|j})$, where $p_j{=}\mathrm{Tr}[\rho_{AB}\Pi_j]$ is the probability of obtaining the conditional state $\rho_{A|j}{=}\mathrm{Tr}_B[\rho_{AB}\Pi_j]/p_j$, and the set $\{\Pi_j\}$, with $\sum_j \Pi_j{=}\mathbb{I}$, form a POVM performed on subsystem B. As this quantity is measurement dependent, the quantum version of the expression including conditional entropy is defined as $J^{\leftarrow}(\rho_{AB}){=}S(\rho_A){-}\mathrm{min}_{\{\Pi_j\}}S_{\{\Pi_j\}}(A|B)$, which is known as one way classical correlation.The minimization is performed over all possible measurements. Therefore, the quantum discord from B to A is defined as:

$$\begin{aligned} D^{\leftarrow}(\rho_{AB}) &= I(\rho_{AB}) - J^{\leftarrow}(\rho_{AB}) \\ &= S(\rho_B) - S(\rho_{AB}) + \mathrm{min}_{\{\Pi_j\}}S_{\{\Pi_j\}}(A|B)\ . \end{aligned} \tag{C.1}$$

In general, it is not clear how to perform the minimization for any arbitrary state, unless there are restrictions to certain class of states and POVMs. Gaussian quantum discord is defined as the quantum discord of a bipartite Gaussian state, where the minimization is restricted to generalized Gaussian measurements [252, 253]. This quantity was experimentally estimated and characterized for a two-mode squeezed thermal state [300], two-mode squeezed vacuum state generated by a four-wave mixing process [255], and entangled and separable Gaussian states [256]. Gaussian states with nonzero discord are shown to be used to reveal interference [301]. It was recently shown that Gaussian states with nonzero Gaussian discord have nonzero discord [299].

C.2.2 Verification of quantum discord in Gaussian states

The measurement-based method for verifying quantum discord [299] is based on measuring the conditional states of subsystem B corresponding to the outcomes of an informationally complete POVM [257, 258] performed on subsystem A. If the conditional states commute with one another then quantum discord is zero, otherwise is nonzero. However, if some prior knowledge about the state is available, one may be able to verify discord with only a few measurements. It was shown in ref [299] that in principle for Gaussian states nonvanishing quantum discord can be verified by checking whether the peaks of two conditional Wigner functions corresponding to two different outcomes of heterodyne measurements do not coincide at the same point in the phase space. However, in practice, this is not efficient, as one has to repeat the measurements many times in order to obtain sufficient data for finding the peaks of the conditional Wigner functions. Here we introduce a simple and efficient experimental technique for verifying discord of Gaussian states, which can be also applied to some class of non-Gaussian states.

In general, one can always characterize Gaussian states in terms of the means and covariance matrix of their quadratures x and p [24]. For a bipartite system with modal annihilation operators $\hat{a}=x_1+ip_1$ and $\hat{b}=x_2+ip_2$, we define quadrature vectors for each subsystem, $\mathbf{x}_A=(x_A, p_A)$ and $\mathbf{x}_B=(x_B, p_B)$, and an overall quadrature vector $\mathbf{x}=(\mathbf{x}_A, \mathbf{x}_B)=(x_A, p_A, x_B, p_B)$. The vector $\bar{\mathbf{x}}$ represents the means of the quadratures, and the covariance matrix is

$$\boldsymbol{\sigma} = \langle|\hat{\mathbf{x}}^T\hat{\mathbf{x}}|\rangle - \bar{\mathbf{x}}^T\bar{\mathbf{x}} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}, \tag{C.2}$$

where $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{C}$ are 2×2 matrices. The Wigner function is then given by

$$W_{AB}(\mathbf{x}) = \frac{1}{4\pi^2\sqrt{\det\boldsymbol{\sigma}}} \exp\Big(-\frac{(\mathbf{x}-\bar{\mathbf{x}})\boldsymbol{\sigma}^{-1}(\mathbf{x}-\bar{\mathbf{x}})^T}{2}\Big), \tag{C.3}$$

A bipartite Gaussian state has zero discord if and only if there is no correlation between the quadratures of the two subsystems, i.e., [299]

$$\mathbf{C} = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = 0\,. \tag{C.4}$$

Suppose Alice and Bob are sharing a bipartite Gaussian state. In order to verify quantum discord they use two homodyne detections, one for each subsystem. Without loss of generality, we assume $\mathbf{A}$=diag$(a1, a2)$, $\mathbf{B}$=diag$(b1, b2)$ and $\bar{\mathbf{x}} = 0$, as these can be always accomplished by appropriately choosing the zero reference phase of the local oscillators and shifting the zero reference points of the quadratures being measured. The joint marginal distribution describing the outcomes of two homodyne detections is then given by [25]

$$\begin{aligned} D_{AB}(x_A, \theta_A, x_B, \theta_B) &= \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} dp_A dp_B W(\mathbf{x}\mathbf{U}_{\theta_A,\theta_B}) \\ &= \frac{\pi}{\sqrt{\lambda_{\theta_A}\mu_{\theta_B} - \nu^2_{\theta_A,\theta_B}}} \\ &\times \exp\left(-\lambda_{\theta_A}x_A^2 - \mu_{\theta_B}x_B^2 + 2\nu_{\theta_A,\theta_B}x_Ax_B\right), \end{aligned} \tag{C.5}$$

where

$$\mathbf{U}_{\theta_A,\theta_B} = \begin{pmatrix} \cos\theta_A & \sin\theta_A & 0 & 0 \\ -\sin\theta_A & \cos\theta_A & 0 & 0 \\ 0 & 0 & \cos\theta_B & \sin\theta_B \\ 0 & 0 & -\sin\theta_B & \cos\theta_B \end{pmatrix}.$$

with θ_A and θ_B being the phases of the local oscillators used in Alice's and Bob's homodyne detection, respectively, and λ_{θ_A}, μ_{θ_B}, and ν_{θ_A,θ_B} are some functions of the covariance matrix elements, which depend on θ_A and θ_B. If ν_{θ_A,θ_B} is nonzero, then the quadrature associated with the phase θ_A of subsystem A is correlated to the quadrature associated with the phase θ_B of subsystem B. In order to check this, Bob measures two conditional marginal distributions corresponding to outcomes $x_A > 0$ and $x_A < 0$ of Alice's measurements

$$\begin{aligned} D_{B|\pm}(x_B,\theta_B,\theta_A) &= \int_0^{\pm\infty}(\pm 1)dx_A D_{AB}(x_A,\theta_A,x_B,\theta_B) \\ &= \frac{\sqrt{\pi\lambda_{\theta_A}}\exp\left(\frac{\nu^2_{\theta_A,\theta_B}-\mu_{\theta_B}\lambda_{\theta_A}}{\lambda_{\theta_A}}x_B^2\right)}{\sqrt{\mu_{\theta_B}\lambda_{\theta_A}-\nu^2_{\theta_A,\theta_B}}} \\ &\times\left(1\pm\mathrm{Erf}\left(\frac{\nu_{\theta_A,\theta_B}x_B}{\sqrt{\lambda_{\theta_A}}}\right)\right), \end{aligned} \tag{C.6}$$

where Erf(.) being the error function. If the peaks of the marginal distributions $D_{B|+}(x_B,\theta_B,\theta_A)$ and $D_{B|-}(x_B,\theta_B,\theta_A)$ do not coincide with one another, this implies that $\nu_{\theta_A,\theta_B} \neq 0$.

Using this technique Alice and Bob can now verify quantum discord. As we have

$$\begin{aligned} \nu_{0,0} &= \frac{c_1}{2a_1b_1-2c_1^2}, \\ \nu_{0,\frac{\pi}{2}} &= \frac{c_2}{2a_1b_2-2c_2^2}, \\ \nu_{\frac{\pi}{2},0} &= \frac{c_3}{2a_2b_1-2c_3^2}, \\ \nu_{\frac{\pi}{2},\frac{\pi}{2}} &= \frac{c_4}{2a_2b_2-2c_4^2}, \end{aligned}$$

they only need to choose the phases of their local oscillator to be 0 or $\pi/2$ and measure the conditional marginal distribution $D_{B|\pm}(x_B,\theta_B,\theta_A)$ to check whether the elements of matrix $\mathbf{C}$ are zero or not. If at least one of the elements is found to be nonzero, the state has nonzero quantum discord.

C.2.3 Verification of quantum discord in non-Gaussian states

One way to create quantum states with nonclassical correlation is to use beam splitter. It was shown that nonclassicality of input states to a beam splitter is a necessary condition for generating entanglement at the output of a beam splitter [302, 303]. Here we show that bipartite quantum states that are prepared by subjecting a statistical mixture of coherent states to a beam splitter, while the other port is in the vacuum state, have nonzero discord. We show that quantum discord for this class of non-Gaussian states can be simply verified.

By using the Glauber-Sudarshan representation [26, 27] for an input state ρ_1 to a beam splitter

$$\rho_1 \otimes |0\rangle \langle 0| = \int d^2\alpha P_1(\alpha) |\alpha\rangle \langle \alpha| \otimes |0\rangle \langle 0| , \tag{C.7}$$

the output state is then given by

$$\rho_{\text{out}} = \int d^2\alpha P_1(\alpha) |\eta\alpha\rangle \langle \eta\alpha| \otimes |\tilde{\eta}\alpha\rangle \langle \tilde{\eta}\alpha| , \tag{C.8}$$

where η is the transmissivity of the beam splitter and $\tilde{\eta} = \sqrt{1-\eta^2}$. If $P_1(\alpha)$ is a positive semidefinite Gaussian or non-Gaussian function other than the Dirac delta function, the state ρ_{out} has nonzero discord, as it is a mixture of nonorthogonal states of two subsystems [299].

The Wigner function of the state after the beam splitter is given by [25]

$$\begin{aligned} W_{\text{out}}(x_1,p_1,x_2,p_2) &= W_1(\eta x_1 + \tilde{\eta} x_2, \eta p_1 + \tilde{\eta} p_2) \\ &\times \frac{1}{\pi} \exp\left[-(\eta x_2 - \tilde{\eta} x_1)^2 - (\eta p_2 - \tilde{\eta} p_1)^2\right] . \end{aligned} \tag{C.9}$$

where $W_1(x,p)$ is the Wigner function for the input state ρ_1. Therefore, the necessary and sufficient condition to verify discord in the state (C.8) is to check whether the Wigner function of any of marginal states at the output, for example

$$W_{\text{out},1}(x_1,p_1) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} dx_2 dp_2 W_{\text{out}}(x_1,p_1,x_2,p_2),$$

is the Wigner function of a coherent state or not.

Also by applying our technique developed in the previous subsection, if one observes any changes in the conditional marginal distributions, that indicates correlation between the two quadratures and hence nonzero quantum discord. By measuring x-quadratures of two subsystems using two homodyne detections, the joint marginal distribution is then given by

$$D(x_1,x_2) = \frac{1}{\sqrt{\pi}} D_1(\eta x_1 + \tilde{\eta} x_2) e^{-(\eta x_2 - \tilde{\eta} x_1)^2}, \tag{C.10}$$

where $D_1(x)$ is the marginal distribution of $W_1(x,p)$. If the input state is not a coherent state then ρ_{out} has discord, otherwise zero discord. In the following section, we demonstrate the use of our technique for three different non-Gaussian states.

Notice that our technique has limited use in verifying quantum discord of completely general non-Gaussian states where any peak separation is not necessarily an indication of quantum discord. For example, this state

$$\begin{aligned} \rho_{AB} =& \frac{1}{4}\big(|\alpha\rangle \langle \alpha| \otimes (|0\rangle + |1\rangle)(\langle 0| + \langle 1|) \\ &+ |-\alpha\rangle \langle -\alpha| \otimes (|0\rangle - |1\rangle)(\langle 0| - \langle 1|)\big) \end{aligned}$$

has zero discord from B to A, but by using our method one can see that there is a peak separation in the conditional marginal distributions of B . There are also quantum states with nonzero discord but no peak separation in the conditional marginal distributions; one such state is

$$\rho_{AB} = \rho_{A,1} \otimes \rho_{B,th} + \rho_{A,2} \otimes \rho_{B,S}, \tag{C.11}$$

where $\rho_{B,th}$ and $\rho_{B,S}$ are thermal state and squeezed vacuum state, respectively.

C.3 Experiment

C.3.1 Quantum discord in Gaussian states

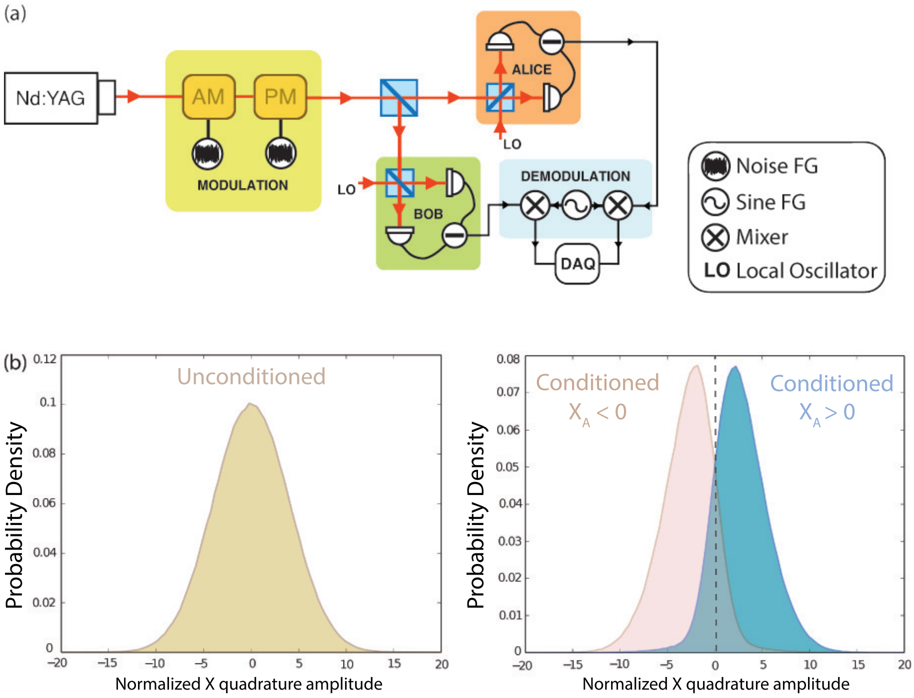


Figure C.1: (a) Schematic diagram of the experimental setup. Here, AM and PM are the electro-optic modulators (EOM) driven by function generators (FG), which in turn provide displacement of the vacuum state in amplitude and phase quadrature with Gaussian distributed noise. Laser light is passed through electro-optic modulators and is split on 50:50 beam splitter. Each part is sent to a homodyne measurement station (Alice and Bob). Collected data points from each homodyne station are demodulated and sampled using a digital data acquisition system (DAQ). (b) The unconditioned (left) and conditioned (right) probability distributions of the bipartite Gaussian state with discord. The state is obtained from a Gaussian distributed modulated beam with modulation depth of 4.5 times the quantum noise. The blue and pink shaded curves show the probability distributions conditioned respectively on $x_A > 0$ and $x_A < 0$, where x_A is the measured amplitude quadrature of subsystem A normalized to quantum noise. The peak separation indicates that the states A and B are discordant.

The experimental setup used to verify the presence of quantum discord is depicted in Figure C.1 (a). The laser light is passed through a mode cleaner cavity to provide a quantum noise limited light source. A large portion of it, is used as the bright source of local oscillator for homodyne detection, and a small portion, is passed through a pair of phase and amplitude elctro-optic modulators (EOM). EOMs are used to provide Gaussian distributed modulation on both quadratures. The modulated beam is then split on a 50:50 beam splitter to generate two separable but correlated bipartite state (A and B). Each part of it, is sent to a homodyne measurement station, which we labelled Alice and Bob.

Following subsection C.2.2, in order to check whether the elements of matrix **C** are zero or not, all possible correlations between two subsystems A and B need to be checked. In order to do that we first lock Bob's station to amplitude quadrature and perform homodyne measurements on both of the stations by locking Alice's station to amplitude quadrature, followed by phase quadrature. The same procedure is repeated for phase quadrature of Bob's station. The marginal distributions of Bob's state conditioned on Alice's outcomes, $x_A > 0$ and $x_A < 0$, are calculated and any possible separation between the peaks of conditional marginal distributions are investigated. In our experiment, the bipartite Gaussian state have correlations in both phase and amplitude quadratures but with very little cross-correlation between the quadratures of two subsystems. Hence when Alice and Bob are both locked to the same quadrature, we observe separation between peaks of conditional marginal distributions, as shown in Figure C.1(b) for amplitude quadrature. Similar result is obtained when both subsystems are locked to phase quadrature. As discussed in subsection C.2.2, for Gaussian state the peak separation in the conditional marginal distributions is a necessary and sufficient condition of non-zero quantum discord. Hence from our result we conclude that we have a discordant bipartite Gaussian state.

In our experiment each pair of detectors are balanced electronically, providing 30 dB of common mode rejection. Typical suppression of cross correlation between orthogonal quadrature is around 25 dB. For each separate homodyne detection, 2.4×10^6 data points are sampled at 14×10^6 samples per second utilizing a digital acquisition system. In order to provide adequate statistics, this procedure is taken over five times for each data point. These data are then down sampled and digitally filtered to 2-5 MHz. Our homodyne efficiency is typically 96.6%, with fringe visibility of 97.6%, generally limited by the mode distortions introduced by the EOMs and the photodiode quantum efficiency of 99%.

We also investigate the effect of variation of modulation depth on the peaks separation of conditional marginal distributions. This is done by changing the variance of Gaussian noise introduced by (EOM) on the desired quadrature. Since we only modulate the phase quadrature, both subsystems are locked to this quadrature. We apply 22 different modulation depths on the phase quadrature, ranging from zero to 5 times the quantum noise. For each homodyne detection, 1.2×10^5 data points are sampled at 200 ksamp per second and then down sampled at 4 MHz sideband. The process is repeated 20 times in order to provide sufficient statistics. For each modulation depth, the con-

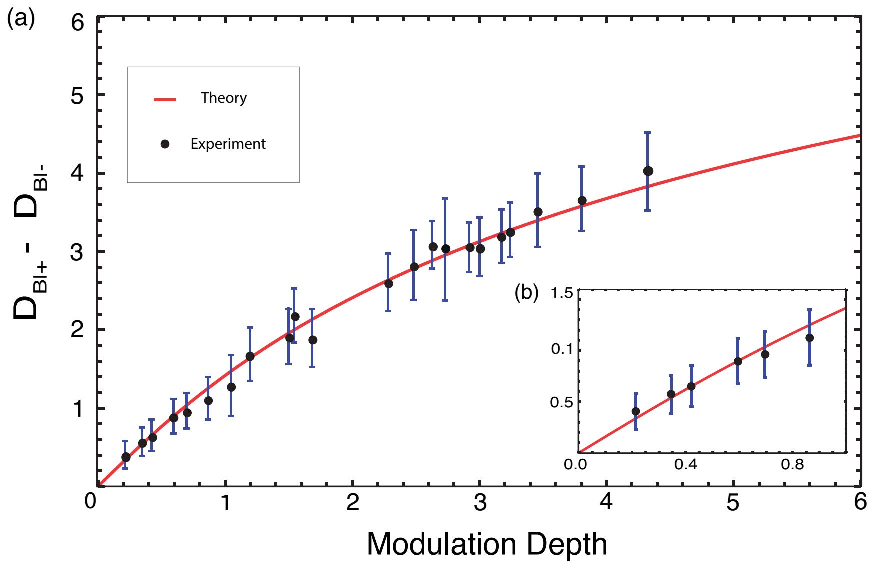


Figure C.2: (a) Variation of peak separations of marginal distributions conditioned on two different homodyne outcomes, $D_{B|+} - D_{B|-}$, versus modulation depth. The theoretical curve is evaluated according to Eq. (C.6). The experimental error bars are estimated using statistical uncertainties. Inset (b) shows the zoom-in for small modulation depth. Even for the smallest modulation depth (0.2 times of quantum noise), our technique is still able to reveal the presence of quantum discord.

ditional marginal distributions are evaluated and the separation between two peaks is measured. As shown in Figure C.2(a), the separation of the peaks increases monotonically with the modulation depth. This is consistent with the theoretical curve plotted by Eq. (C.6). As the modulation depth increases, more noise is applied on the input beam and thus increases the variance of the input beam. This gives rise to output beams with higher correlations, and hence larger elements of matrix **C**. It is remarkable that despite the simplicity of our technique, it is robust enough to verify the presence of discord in weakly correlated bipartite Gaussian states, as indicated in the Fig C.2(b).

C.3.2 Quantum discord in non-Gaussian states

As discussed in subsection C.2.3, our discord verification technique can be applied to bipartite non-Gaussian states obtained by overlapping a statistical mixture of coherent states and vacuum state on a beam splitter. It was previously reported in ref [304] that a mixture of coherent states can be generated by subjecting a laser beam to time varying modulation. Here, we demonstrate our verification technique to examine quantum discord in non-Gaussian states discussed in Section C.2.3. In the following, we describe the preparation of three non-Gaussian states with positive-definite Wigner functions (see Figure C.3) and discuss the corresponding verification results.

1) *Switched Noise Modulation* - The first non-Gaussian state is an equal statistical mixture of vacuum and a thermal state. The thermal state is produced by applying two

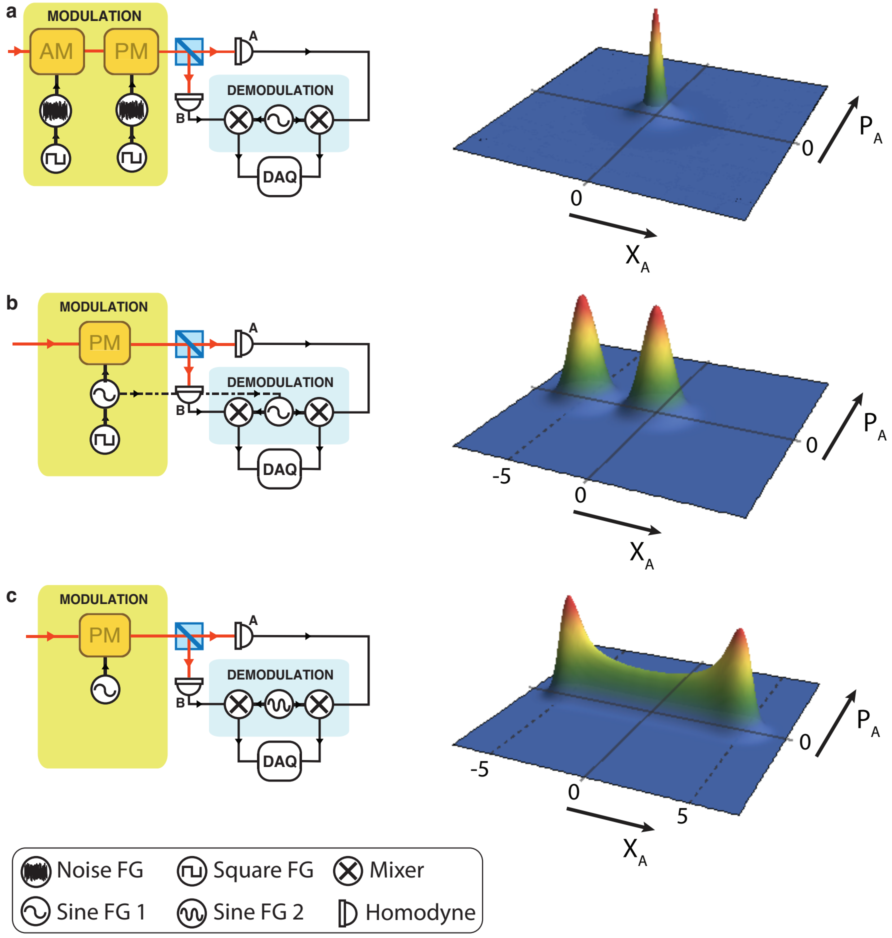


Figure C.3: Schematic diagram of the modulation and demodulation arrangements used in preparation of the non-Gaussian states (left) and their corresponding positive-definite non-Gaussian Wigner functions (right), X_A and P_A are normalized quadrature amplitudes (a) Switched noise modulation (b) switched phase modulation and (c) asynchronous detection.

independent Gaussian distributed noise signals to a phase and amplitude modulator. An external square wave modulation envelope at 12 kHz was then used to gate the two modulators. Square wave modulation turns the Gaussian modulation, on and off periodically. In this way the beam has either Gaussian modulation or no modulation at all. Since the square wave gating frequency is fast compare to the detection time, the net detected statistics seen will consist of an equal contribution from both the vacuum and the thermal state. Modulation and demodulation arrangement and the Wigner function of the produced state are shown schematically in Figure C.3(a). The laser light with this non-Gaussian modulation then splits on a 50:50 beam splitter and each part is sent to a homodyne measurement station. To investigate the correlations between two subsystems, the same measurement procedure is performed as described in Section C.3.1, and the results are presented in Figure C.4 (a).

2) *Switched Phase Modulation* - The second prepared non-Gaussian state is a mixture

of vacuum and a coherent state. As depicted in Figure C.3(b), a sine wave modulation with frequency of 4 MHz is introduced to phase quadrature to create the coherent state. We then add a square wave modulation with frequency of 120 Hz to gate the sine modulation on and off. With this arrangement there is a sine modulation for half of the measurement time and no modulation for the other half. Signal is detected synchronously by using the same demodulation frequency as is used for modulation. Similar procedure is repeated to prepare a correlated bipartite state. In order to verify the presence of discord, the marginal distributions of Bob's state conditioned on two different sets of Alice's outcomes $x_A < -6$ and $x_A > -6$ are calculated and any possible correlation in conditional marginal distributions is investigated[1]. The results are shown in Figure C.4(b).

3) *Asynchronous Detection* - We prepare the third non-Gaussian state by using asynchronous detection. This is experimentally realised by choosing a demodulation signal different in the frequency by an small amount compared to the modulation signal. As displayed in Figure C.3(c), we drive the EOM by sine wave with frequency of 4 MHz and demodulate with frequency of 3.99MHz. The data collected is then digitally filtered to 3.9-4.1 MHz. The prepared state is a two peak probability distribution function along the X-quadrature as shown by Wigner function in Figure C.3(c) right. This is analogous to the stroboscopic measurement of the quadrature of a harmonic oscillator. The marginal probability distribution of the prepared state and the conditional probability distributions are presented in Figure C.4(c).

As can be observed from Figure C.4, it is evident that the conditional probability distributions for all three non-Gaussian states are different from their unconditioned distributions. Neither their peaks nor the mean values of their distributions coincide, which by considering the preparation method, is a sufficient evidence of the presence of discord in the three non-Gaussian states. As the difference between two conditional marginal distributions is the criterion to verify quantum discord, in situations where the conditional distributions are very similar to each other, one can deploy χ^2 test and calculate its probability function. Generally one rejects the *null* hypothesis if the probability function is less than 0.05, which means two distributions are not the same. In our experiment, the calculated probability function is zero for all the states, indicating the two conditional distributions are completely different and the states are discordant.

C.4 Conclusion

We have introduced and experimentally demonstrated a simple and efficient method for verifying quantum discord in unknown bipartite Gaussian states. We have shown that by checking peak separation between the marginal distributions conditioned on two different homodyne measurements outcomes, the correlation of corresponding quadra-

[1] As discussed in Section C.2.3, in order to verify quantum discord in this class of non Gaussian states it is sufficient to calculate marginal distributions conditioned on any two sets of Alice's outcomes.

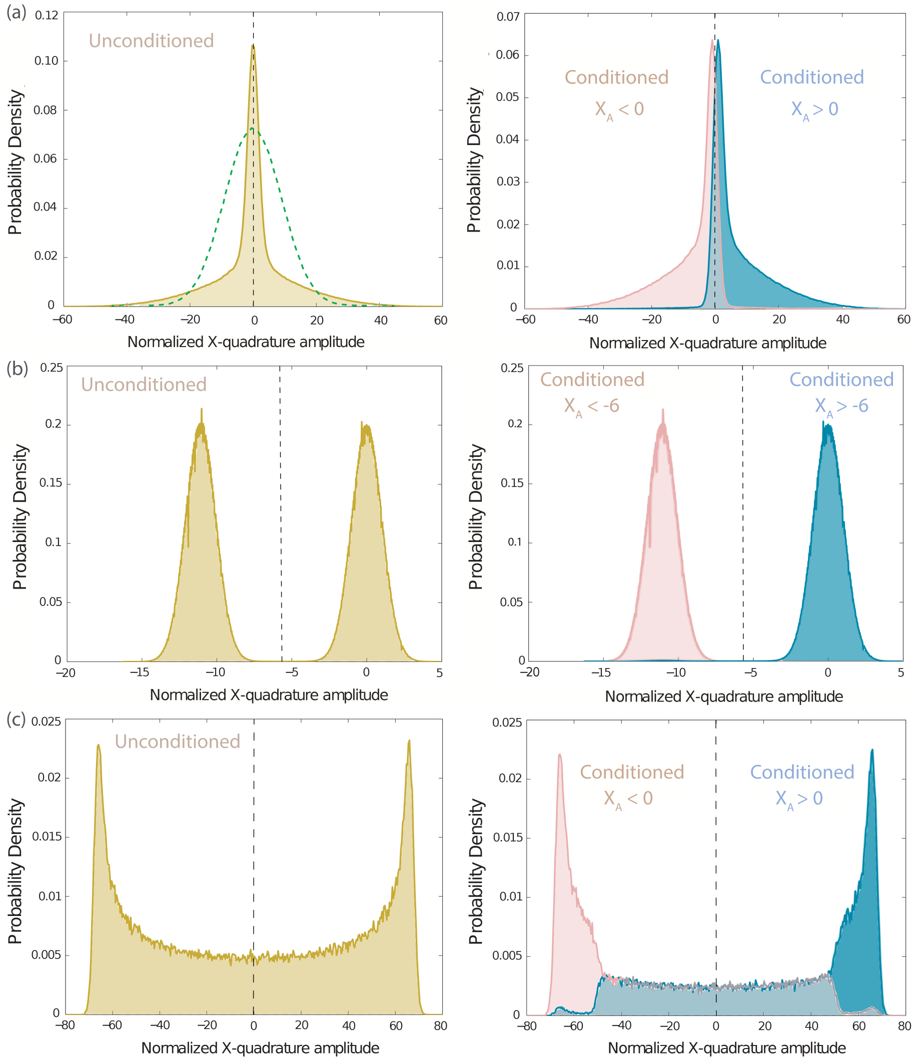


Figure C.4: Unconditional (Brown) and conditional probability distributions of two different outcomes (Pink and Blue) of the non-Gaussian states prepared by (a) Switched Noise Modulation (The green dashed curve corresponds to a Gaussian state with average variance of the two Gaussian distributions); (b) Switched Phase Modulation; and (c) Asynchronous Detection. We observe that the unconditional distributions are non-Gaussian, and also changes in the conditional marginal distributions in all three cases. Hence, according to Section C.2.3, all the three non-Gaussian states have nonzero discord.

ture can be tested. With this technique, quantum discord can be verified by testing correlations between all four combinations of the amplitude and phase quadratures of two subsystems. By varying the modulation depth, we showed that our results are indeed consistent with the theoretical predictions within statistical errors. The robustness of our technique in small modulation depth permits one to detect nonzero discord even when the correlations are small. Moreover, we have discussed that our technique can be used for a certain class of non-Gaussian states. We applied our method to three different bipartite non-Gaussian states, which are prepared by subjecting statistical mixtures of coherent states to one port of beam splitter while the other port is in the vacuum state.

Experimental results for all the non-Gaussian states show that the conditional marginal distributions are significantly different from the unconditional distributions, indicating nonzero quantum discord in each case. Our results show that with some prior knowledge about a quantum state, such as being Gaussian, or about the preparation stage quantum discord can be efficiently verified with a finite number of measurements.

Appendix D

Discord Empowered CV Quantum Illumination

Overview

Here we study the role of discord in continuous variable quantum illumination. I am involved in initiating the research and conducted the preliminary derivation of the mutual information (Holevo and Accessible). The project was took over by Mark Bradshaw, who further explored tighter bound for the information quantities and derived the analytical result.

The work in this chapter has resulted in the following publication:

- M. Bradshaw, S. M. Assad, J. Y. Haw, S. H. Tan, P. K. Lam and M. Gu.
  "The overarching framework between Gaussian quantum discord and Gaussian quantum illumination."
  Physical Review A, 95 (2): 022333 (2017).

D.1 Introduction

Quantum illumination is a simple target detection scheme, first proposed by Lloyd for photonic qubits [259]. It harnesses entanglement in a quantum state of light to better infer the presence or absence of a weakly reflecting object flooded by white noise. The protocol distinguished itself in displaying quantum advantage, even in regimes so noisy that no entanglement survives. It presented a remarkable deviation from the conventional view that quantum technologies are fragile, displaying advantage only in carefully engineered environments which ensure little or no loss of entanglement. Since its original inception, quantum illumination has gained significant scientific interest. Many variants have been proposed, including some that make use of Gaussian states in the continuous variable regime [260, 261, 262] and inspiring a number of different experimental realizations [263, 264, 265, 266]. The phenomenon has also seen applications outside metrology, where quantum illumination has been harnessed to provide security against passive eavesdropping in the setting of secure communication [267].

Quantum illumination challenges the conventional view that entanglement alone can explain all quantum advantage. It joins a particularly surprising class of protocols that appear to thrive in noisy, possibly entanglement-breaking environments [268, 269]. What other quantum resources then, could help us better understand its noisy resilience? Quantum discord [270, 254, 271] which quantifies correlations beyond entanglement is considered a likely candidate. Unlike entanglement, discord is far more robust, and can also survive in highly noisy conditions [250]. In fact, Weedbrook *et al.* have shown such a relation for discrete variables [272]. Specifically, they showed that the performance advantage of quantum illumination – in terms of extra accessible information about whether an object is present – can be directly related to the amount of discord in the illumination protocol that survives after being subjected to entanglement-breaking noise. Does a similar relationship hold for continuous variables?

The aim of this work is to answer this question. We extend the framework relating discord and illumination to the continuous variable regime. This involves understanding how these relations generalize when a number of conditions specific to the discrete scenario no longer hold. The paper is organized as follows. In section D.2 we describe the illumination protocol and the quantifiers of performance. In section D.3 we describe discord and how it relates to quantum illumination. In section D.4 we present and discuss our results, demonstrating that there is a general relationship between discord and the quantum advantage of illumination in the continuous variable regime.

D.2 The illumination framework

D.2.1 Setup

The illumination framework is described as follows: Bob wishes to determine whether an object is located in a noisy environment. He sends a quantum state, referred to as the probe, to the location. If an object is present, part of the probe will be reflected back to Bob, along with some background noise. If the object is not present, Bob receives only the background noise. Bob may have another state called the idler, which was initially correlated with the probe.

If the probe and idler are quantum correlated (have a non-zero quantum discord) the scheme is called *quantum illumination*. If there is no idler, it is called *single-mode illumination*. A diagram of illumination is shown in Fig. D.1(a) and (b). Bob performs a joint measurement on the idler and returning probe, and uses the results of the measurement to determine whether an object was present. For brevity in notation in the rest of the paper, modes A and B will label the probe and idler parts of the state respectively.

We are interested in quantum illumination in the continuous variable setting, where the probe and idler are Gaussian states. For single-mode illumination, Bob uses a coherent state ρ_α, where α is its amplitude. For quantum illumination, Bob uses an EPR state

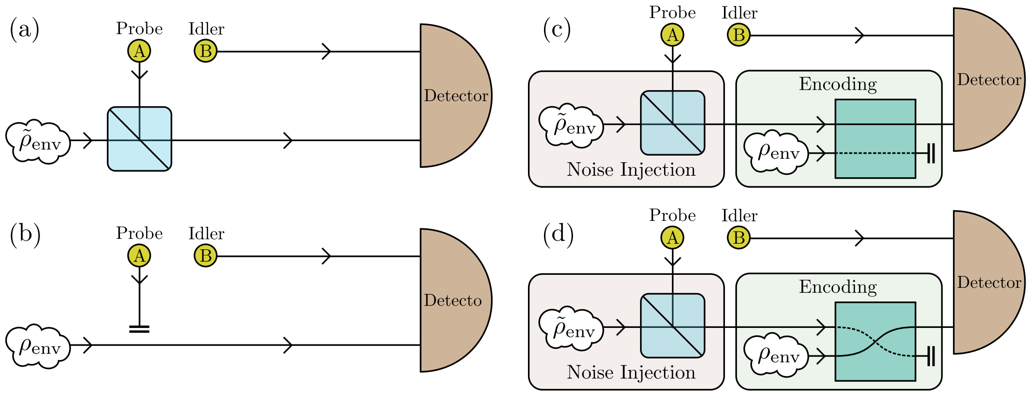


Figure D.1: Diagram of illumination setup. (a) With probability p_0 there is an object located in a noisy environment. The object is partially reflective (modeled as a beam splitter with reflectivity ϵ). A probe is sent towards the object. The probe is mixed with the noisy environment, and reflected to the detector. (b) With probability p_1 an object is not present. In which case there is nothing to reflect the probe to the detector. Hence, only noise is detected. (c) An equivalent description of illumination whereby first noise is injected. Then, encoding is performed on the probe, whereby with a probability p_0, an identity operation is performed on the probe (after noise injection) and the environment noise, and (d) with probability p_1 a swap operation is performed on the probe and environment. In quantum illumination we also have an idler initially entangled with the probe which is used to perform a joint measurement. Single-mode illumination is when there is no idler. ρ_{env} is the noisy environment and $\tilde{\rho}_{\text{env}}$ is the environment with the mean photon number scaled by $1/(1-\epsilon)$.

described by $\rho_{\text{EPR}} = |\psi_{\text{EPR}}\rangle \langle\psi_{\text{EPR}}|$, where

$$|\psi_{\text{EPR}}\rangle = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}(-\lambda)^n |n\rangle_A |n\rangle_B \ . \tag{D.1}$$

where $\lambda = \tanh(r)$, and r is the squeezing parameter.

Illumination can also be recast as a communication protocol. Let us suppose that Alice is in control of the object, and she would like to communicate with Bob. She can do so by encoding a binary alphabet via the control of the object, such as in the Morse code. The message she sends to Bob can be described by realizations of a random variable X, where if $X = 0$ Alice places the object in the noisy environment, and if $X = 1$ Alice removes the object. Let p_x be the prior probability that $X = x$, and let $p_0 = p_1$, i.e. let both hypotheses be equally likely to occur. Let $\rho^{(x)}$ denote the state received by Bob when $X = x$. Noise is injected into the probe state before Alice encodes the value of X. This is shown diagrammatically in Fig. D.1(c) and (d). We model the object as a beam splitter with reflectivity ϵ. The environment noise state ρ_{env} is a thermal state with mean photon number $\bar{n}_{\text{env}}$, where $\rho_{\text{env}}(\bar{n}) = \sum_{n=0}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} |n\rangle \langle n|$. When the object is present, the environment noise is multiplied by a factor of $1/(1-\epsilon)$ such that the mean number of noise photons arriving at the detector is the same as when the object is absent. This approach has been adopted by [273] to avoid a 'shadowing effect' – so that the object is not detected by a reduction in the number of noise photons arriving at the detector. The typical illumination scenario that has greatest quantum advantage is for the regime of low object reflectivity and high noise, i.e. $\epsilon \ll 1$ and $\bar{n} \ll \bar{n}_{\text{env}}$ where $\bar{n}$ is the mean photon number of the probe. We term this as the intense white noise limit.

Consider Fig. D.1(c) and (d). After the noise injection, the entanglement is reduced or lost all together, before any information is encoded within the probe. In fact, for all the settings studied in section D.4, the entanglement after noise injection is strictly zero. Nevertheless we see a quantum advantage. Thus, quantum entanglement itself does not give a complete picture on why illumination thrives in such noise. Our goal here is to see if discord will give us additional insight.

In the next subsection, we will use the communication formalism to study the amount of information that Alice can communicate to Bob under different settings. This provides a measure for assessing the performance of illumination under these settings.

D.2.2 Quantifiers of performance

We consider two quantifiers of performance of illumination: the accessible information and Holevo information.

Let $\mathcal{M} = \{E_k\}$ be a set of positive operator-valued measures (POVMs) (Sec. 2.4.1) that represent mathematically the outcome of a measurement. The subscript k labels the outcome of the measurement. The probability of the measurement outcome k on a state $\rho^{(x)}$ is then given by $q_k^{(x)} = \mathrm{Tr}\big(\rho^{(x)} E_k\big)$. Let this be governed by random variable $K_{\mathcal{M}}$. In the communication setting described in the last subsection, the amount of information obtained by Bob after measurement of the state $\rho^{(x)}$ is given by the mutual information,

$$I_{\text{mut}}(X, K_{\mathcal{M}}) = \sum_k \sum_{x=0}^{1} p_x q_k^{(x)} \log\left(\frac{q_k^{(x)}}{q_k}\right), \tag{D.2}$$

where $q_k = \sum_{x=0}^{1} p_x q_k^{(x)}$. The accessible information is the maximization of the mutual information over all POVMs:

$$A\left(\rho^{(0)}, \rho^{(1)}\right) = \max_{\mathcal{M}} I_{\text{mut}}\left(X, K_{\mathcal{M}}\right). \tag{D.3}$$

The accessible information quantifies Bob's knowledge when each $\rho^{(x)}$ from N trials is measured separately using an optimal POVM. In the context of communication, illumination can be regarded as classical information exchange over a noisy channel. By the Shannon's noisy-channel coding theorem [30], Alice and Bob communicate at a rate equal to the accessible information in the limit of infinite message size N.

There is no known general method for calculating the accessible information exactly. Here we will make use of the upper and lower bounds found by Fuchs and Caves [274].

The lower bound, hereby referred to as the Fuch's lower bound is

$$I_{\text{lower}} = \text{Tr}\left\{p_0\rho^{(0)}\ln\left[\mathcal{L}_{\bar{\rho}}(\rho^{(0)})\right] + p_1\rho^{(1)}\ln\left[\mathcal{L}_{\bar{\rho}}(\rho^{(1)})\right]\right\} \tag{D.4}$$

where $\mathcal{L}$ is the lowering superoperator given by

$$\mathcal{L}_{\bar{\rho}}(\Delta) = \sum_{\{j,k|\lambda_j+\lambda_k\neq 0\}}\left[\frac{2}{\lambda_j(p_1)+\lambda_k(p_1)} \times \langle\psi_j(p_1)|\,\Delta\,|\psi_j(p_1)\rangle\,|\psi_j(p_1)\rangle\,\langle\psi_k(p_1)|\right], \tag{D.5}$$

and where $\Delta = \rho^{(1)} - \rho^{(0)}$. $\lambda_i(p_1)$ and $|\psi_i(p_1)\rangle$ are the eigenvalues and eigenvectors of $\bar{\rho} = (1-p_1)\rho^{(0)} + p_1\rho^{(1)}$. The Fuchs upper bound I_{upper}, is found by numerically solving the differential equation

$$\frac{\mathrm{d}^2 I_{\text{upper}}(p_1)}{\mathrm{d}p_1^2} = \sum_{\{j,k|\lambda_j+\lambda_k\neq 0\}}\left[-\frac{2}{\lambda_j(p_1)+\lambda_k(p_1)} \times |\,\langle\psi_j(p_1)|\,\Delta\,|\psi_k(p_1)\rangle\,|^2\right] \tag{D.6}$$

subject to:

$$I_{\text{upper}}(0) = I_{\text{upper}}(1) = 0. \tag{D.7}$$

The other figure of merit we consider is the Holevo information [31]. It is given by

$$\chi(\rho^{(0)},\rho^{(1)}) = S\left(\sum_{x=0}^{1} p_x\rho^{(x)}\right) - \sum_{x=0}^{1} p_x S(\rho^{(x)}) \tag{D.8}$$

where $S(\rho)$ is the Von Neumann entropy of the quantum state ρ. The Holevo information is the maximum communication rate Bob can obtain, provided he stores all of the N states and then performs a joint measurement upon all of the states. From the Holevo-Schumacher-Westmoreland theorem [275, 276] this information rate is obtainable when $N \to \infty$.

D.2.3 Three cases of illumination and quantum advantage

Three cases, together with three pairs of accessible information and Holevo information are relevant for our assessment of the illumination scheme (Figure D.1(a)) in the communication framework. They are as follows:

Case 1. Quantum illumination with joint measurement: A_q and χ_q are the accessible information and Holevo information, respectively for Bob when two mode EPR states are used as probes and idlers for illumination. Any arbitrary joint measurement over the two modes is allowed.

Case 2. Quantum illumination with local measurements: A_c and χ_c are the average accessible information and Holevo information for Bob with EPR state as the probe and idler, under the restriction that Bob must perform the optimal Gaussian local measurement on mode B, followed by an arbitrary local measurement on mode A. The measurement on mode B is optimal in the sense that it maximizes the amount of accessible information/Holevo information Bob receives. In this case, Bob only takes advantage of the classical correlations of the EPR state. This enables a direct comparison to case 1, when both quantum and classical correlations are utilized.

Case 3. Single-mode illumination: A_s and χ_s are the accessible information and Holevo information, respectively when Bob uses a single mode coherent state with a fixed amplitude α as the illumination probe.

The quantum advantage is defined as the difference between the performance of quantum illumination and single-mode illumination protocol. The protocols are compared for scenarios where the probe states have coinciding energy. This constraint allows for fair comparison, as it is always possible to detect the presence of an object with any fixed accuracy by using a sufficiently energetic probe. The quantum advantage in terms of accessible information is $A_q - A_s$ and the Holevo information quantum advantage is $\chi_q - \chi_s$, where each information quantity is evaluated over the probe with mean photon number $\bar{n}$. As we shall show in this paper, these quantum advantages can be linked to the discord consumed in the illumination protocol.

D.3 Discord and quantum illumination

Quantum discord, as introduced in Sec. C.2.1, is a measure of the nonclassical correlations between two quantum states. It arises from the difference between quantum analogs of two distinct definitions of the classical mutual information [270, 254]:

$$I(\mathrm{A}:\mathrm{B}) = S(\mathrm{A}) + S(\mathrm{B}) - S(\mathrm{AB}) \tag{D.9}$$

$$J(\mathrm{A}|\mathrm{B}) = S(\mathrm{A}) - \min_{\{\Pi_b\}} \sum p_b S(\mathrm{A}|b) \tag{D.10}$$

where Π_b is the positive-operator valued measure (POVM) of the outcome b, p_b is the probability of that outcome, and $S(\mathrm{A}|b)$ is the entropy of the state conditioned on the outcome b. The discord is then

$$\begin{aligned}\delta(\mathrm{A}|\mathrm{B}) &= I(\mathrm{A}:\mathrm{B}) - J(\mathrm{A}|\mathrm{B}) \\ &= S(\mathrm{B}) - S(\mathrm{AB}) + \min_{\{\Pi_b\}} \sum p_b S(\mathrm{A}|b)\ ,\end{aligned} \tag{D.11}$$

where the minimization is done over all possible POVMs on mode B. In the special case that the domain of this minimization is restricted to Gaussian measurements, then the discord is known as the Gaussian discord [253, 252]. It was recently shown that for a large class of Gaussian states, Gaussian quantum discord is equal to quantum discord [277]. Henceforth we denote the Gaussian discord: $\delta^{\mathrm{G}}(\mathrm{A}|\mathrm{B})$ with a superscript

G.

We now consider the evolution of the discord when quantum illumination is described by Fig. D.1(c) and (d). After the noise injection step, Alice is left with state ρ with which she can encode information to send to Bob. We note that this state may have no entanglement due to the noise injection [273]. Alice encodes the value of X on the state by performing the operation O_x on ρ, resulting in a state $\rho^{(x)} = O_x(\rho)$ with discord $\delta^{(x)}(\mathrm{A}|\mathrm{B})$.

Let us decompose the discord of ρ, $\delta(\mathrm{A}|\mathrm{B})$ into three components:

$$\delta(\mathrm{A}|\mathrm{B}) = \delta_{\mathrm{loss}} + \bar{\delta}(\mathrm{A}|\mathrm{B}) + \delta_{\mathrm{con}}(\mathrm{A}|\mathrm{B}) \tag{D.12}$$

The first component δ_{loss} is the amount of discord lost to the environment during the encoding process. This can be evaluated by first defining

$$\delta_{\mathrm{loss}}^{(x)} = \delta(\mathrm{A}|\mathrm{B}) - \delta^{(x)}(\mathrm{A}|\mathrm{B}) \tag{D.13}$$

as the loss of discord for each possible value of x that Alice can encode, and then taking the weighted average over the probability of encoding that x. This results in

$$\delta_{\mathrm{loss}} = \sum_x p_x \delta_{\mathrm{loss}}^{(x)} \tag{D.14}$$

The second component $\bar{\delta}(\mathrm{A}|\mathrm{B})$ is the discord of $\bar{\rho} = p_0\rho^{(0)} + p_1\rho^{(1)}$, the state after encoding. This is the state seen by Bob who is oblivious to the value of X.

We term the remaining component the *consumed discord* $\delta_{\mathrm{con}}(\mathrm{A}|\mathrm{B})$, and represents the discord in ρ that remain unaccounted for. In prior literature, it was proposed to capture the amount of discord consumed to encode the value of X on the state ρ [272]. For the special case where encodings were unitary, such that $\delta_{\mathrm{loss}}^{(x)} = 0$, $\delta_{\mathrm{con}}(\mathrm{A}|\mathrm{B})$ was related to the advantage of using coherent interactions [251]. It is also interesting to note that $\delta_{\mathrm{con}}(\mathrm{A}|\mathrm{B})$ also coincides with the the extra discord Bob sees between A and B, should he learn the value of X.

In quantum illumination, when $X = 0$, Alice performs an identity operation, thus $\delta^{(0)}(\mathrm{A}|\mathrm{B}) = \delta(\mathrm{A}|\mathrm{B})$ and $\delta_{\mathrm{loss}}^{(0)} = 0$. When $X = 1$, Alice performs a swap operation between mode A of ρ with the environment noise, destroying all correlations between the two modes. All discord is lost and $\delta_{\mathrm{loss}}^{(1)} = \delta(\mathrm{A}|\mathrm{B})$. Putting this together, the average discord loss is thus $\delta_{\mathrm{loss}} = p_1\delta(\mathrm{A}|\mathrm{B})$. Hence the consumed discord for quantum illumination is

$$\delta_{\mathrm{con}}(A|B) = p_0\delta^{(0)}(\mathrm{A}|\mathrm{B}) - \bar{\delta}(\mathrm{A}|\mathrm{B}). \tag{D.15}$$

D.4 Method and results

In section D.4.1 we first derive a general result that if certain conditions are fulfilled, the discord consumed is equal to the Holevo information quantum advantage. In section D.4.2, we numerically calculate the illumination information quantities. In section D.4.3 we numerically evaluate the consumed discord and compare it to the quantum advantages. Our main result is that for continuous variable quantum illumination, the consumed discord is approximately equal to the Holevo information quantum advantage.

D.4.1 Analytic result

We prove the following theorem:

Theorem 1 *Let $\rho_{\mathrm{AB}}^{(0)}$ and $\rho_{\mathrm{AB}}^{(1)}$ be two arbitrary two mode states. If the following conditions are met:*

1. *Mode B is the same for both states: $\rho_{\mathrm{B}}^{(0)} = \rho_{B}^{(1)}$ where $\rho_{\mathrm{B}}^{(x)} = \mathrm{Tr}_A(\rho_{\mathrm{AB}}^{(x)})$ where Tr_{A} denotes the partial trace over subsystem A.*
2. *$\rho_{\mathrm{AB}}^{(1)}$ is a product state: $\rho_{\mathrm{AB}}^{(1)} = \rho_{A}^{(1)} \otimes \rho_{B}^{(1)}$*
3. *The Holevo information of local measurement χ_c, the discord of $\bar{\rho}_{\mathrm{AB}} = p_0\rho_{\mathrm{AB}}^{(0)} + p_1\rho_{\mathrm{AB}}^{(1)}$, and the discord of $\rho_{\mathrm{AB}}^{(0)}$ are achieved by the same measurement,*

then $\delta_{\mathrm{con}}(\mathrm{A}|\mathrm{B}) = \chi_q - \chi_c$, where

$$\chi_q = \chi(\rho_{\mathrm{AB}}^{(0)}, \rho_{\mathrm{AB}}^{(1)})$$
$$\chi_c = \max_{\{\Pi_b\}} \sum_b p_b \chi(\rho_{\mathrm{A}|b}^{(0)}, \rho_{\mathrm{A}|b}^{(1)}),$$

where p_b is the probability of measuring outcome Π_b on subsystem B, and $\rho_{\mathrm{A}|b}^{(x)}$ are the states of subsystem A conditioned on that outcome.

Proof:

Let $\{\Pi_b\}$ be the measurement in condition 3 that simultaneously optimizes χ_c, as well as the discord of states $\bar{\rho}_{\mathrm{AB}}$ and $\rho_{\mathrm{AB}}^{(0)}$. The measurement outcome probability is

$$p_b = \mathrm{Tr}\Big((\Pi_b \otimes I)\rho_{\mathrm{AB}}^{(0)}\Big) = \mathrm{Tr}\Big((\Pi_b \otimes I)\rho_{\mathrm{AB}}^{(1)}\Big),$$

where we have used condition 1. The resulting conditional states are

$$\rho_{\mathrm{A}|b}^{(x)} = \frac{\mathrm{Tr}_{\mathrm{B}}(\Pi_b \rho_{\mathrm{AB}}^{(x)})}{p_b}.$$

Our goal is to prove $\delta_{\text{con}}(\text{A}|\text{B}) = \chi_q - \chi_c$. Because of condition 2, $\delta^{(1)}(\text{A}|\text{B}) = 0$, as so the consumed discord is

$$\begin{aligned}\delta_{\text{con}}(\text{A}|\text{B}) &= p_0\delta^{(0)}(\text{A}|\text{B}) - \bar{\delta}(\text{A}|\text{B}) \\ &= p_0(S(\rho_{\text{B}}^{(0)}) - S(\rho_{\text{AB}}^{(0)}) + \sum_b p_b S(\rho_{\text{A}|b}^{(0)})) \\ &\quad - S(\bar{\rho}_{\text{B}}) + S(\bar{\rho}_{\text{AB}}) - \sum_b p_b S(\bar{\rho}_{\text{A}|b}).\end{aligned}$$

We also have that:

$$\begin{aligned}\chi_q - \chi_c = {}& S(\bar{\rho}_{\text{AB}}) - p_0 S(\rho_{\text{AB}}^{(0)}) - p_1 S(\rho_{\text{AB}}^{(1)}) \\ &+ \sum_b p_b(-S(\bar{\rho}_{\text{A}|b}) + p_0 S(\rho_{\text{A}|b}^{(0)}) + p_1 S(\rho_{\text{A}|b}^{(1)})).\end{aligned}$$

This leads to

$$\delta_{\text{con}}(\text{A}|\text{B}) - (\chi_q - \chi_c) = p_0 S(\rho_{\text{B}}^{(0)}) - S(\bar{\rho}_{\text{B}}) + p_1 S(\rho_{\text{AB}}^{(1)}) - \sum_b p_b p_1 S(\rho_{\text{A}|b}^{(1)}).$$

From condition 1 we have that $\rho_{\text{B}}^{(0)} = \rho_{\text{B}}^{(1)} = \bar{\rho}_{\text{B}}$. From condition 2, $\rho_{\text{AB}}^{(1)}$ is a product state, so $S(\rho_{\text{AB}}^{(1)}) = S(\rho_{\text{A}}^{(1)}) + S(\rho_{\text{B}}^{(1)})$ and $\rho_{\text{A}|b}^{(1)} = \rho_{\text{A}}^{(1)}$. So this becomes

$$\begin{aligned}\delta_{\text{con}}(\text{A}|\text{B}) - (\chi_q - \chi_c) &= S(\rho_{\text{B}}^{(0)})(p_0 - 1 + p_1) + S(\rho_{\text{A}}^{(1)})(p_1 - p_1) \\ &= 0.\end{aligned}$$

In continuous variable quantum illumination, condition 1 is satisfied since the idler is not interacting with the illumination object. Condition 2 is met by the fact that the swap operation decorrelates mode A and mode B. By restricting ourselves to Gaussian quantum discord, together with the assumption that a Gaussian heterodyne measurement is the optimal measurement for the quantities in condition 3, we have $\delta_{\text{con}}^{\text{G}}(\text{A}|\text{B}) = \chi_q - \chi_c$. This assumption is justified by numerical results in the next subsections.

D.4.2 Accessible information and Holevo information calculations

The accessible information and Holevo information quantities A_q, χ_q, A_c, χ_c, A_s and χ_s were calculated numerically for typical settings of quantum illumination. Due to finite computational resources, the states must be approximated to a Hilbert space with finite dimensions. Under this restriction, the highest noise mean photon number that does not result in significant error is $\bar{n}_{\text{env}} = 4$. Plots are shown in Fig. D.2, of the information quantities for noise mean photon number 4, and probe mean photon number $\bar{n} = (0.01, 0.5)$. We will now review the information quantities for each case listed in Sec. D.2.3.

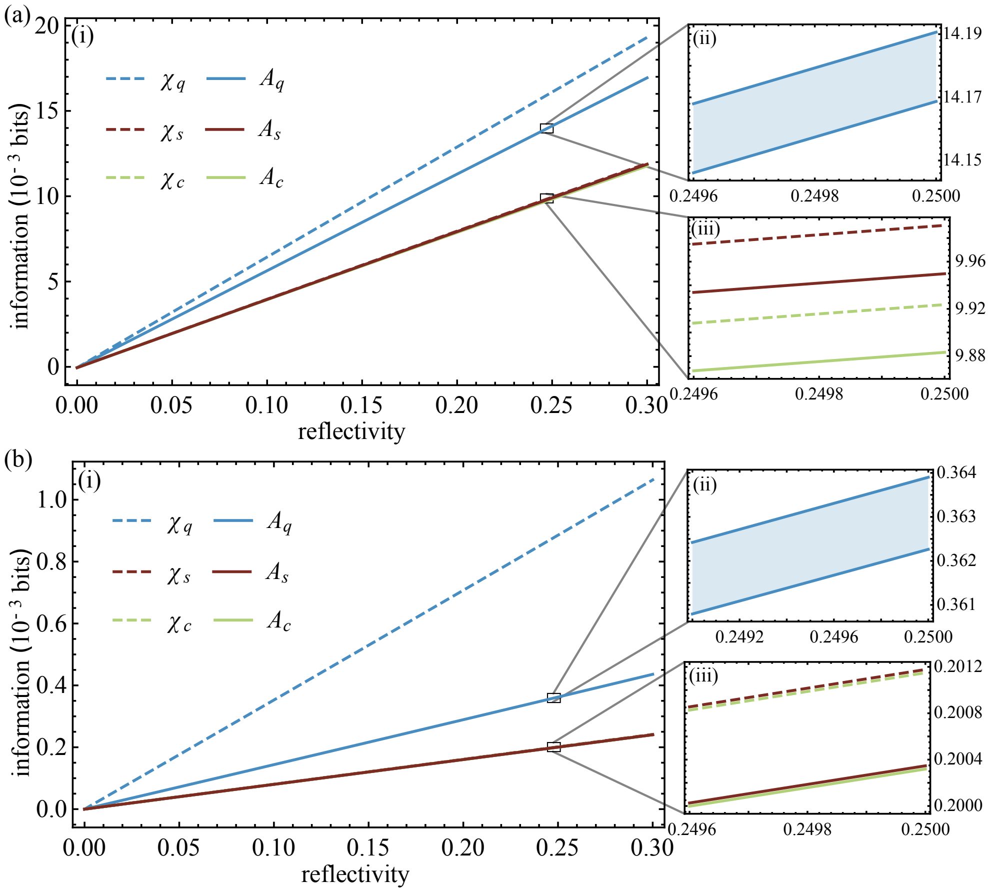


Figure D.2: Information versus object reflectivity ϵ when probe has mean photon number (a) 0.5 and (b) 0.01. The environment noise has mean photon number 4. Each plot has two insets showing zoomed portions. Insets (ii) show the upper and lower bounds for A_q, the true value of lying somewhere in the shaded region. Insets (iii) show that χ_s, χ_c, A_s and A_c differ slightly, despite appearing as a single line in the main plot.

Case 1. The Holevo information χ_q and Fuchs upper and lower bounds for the accessible information A_q for quantum illumination with joint measurement are shown in Fig. D.2. The difference between the upper and lower bounds of A_q are at most 0.7%, implying that the true accessible information is close to the Fuchs bounds. As evident in the plot, there is a substantial difference between the χ_q and A_q.

Case 2. χ_c and A_c: In the previous section, we assume that a heterodyne measurement is the optimal local Gaussian measurement to make on mode B. It can be shown that this is true for a typical choice of parameters [278]. Since a heterodyne measurement on mode B collapses mode A into a distribution of coherent states, χ_c and A_c were calculated by integrating the information quantities of single coherent probe (χ_s, A_s) as as function of energy. The computed upper and lower bounds for A_c are equal to within 6 significant figures.

Case 3. χ_s and A_s: The Holevo information χ_s is plotted in Fig. D.2. Fuchs lower and upper bounds for A_s were calculated and are equal to within 7 significant figures, and are indistinguishable in Fig. D.2. Unlike Case 1, when using a coherent state the Holevo and accessible information differ by a small amount, only 0.4%.

From Fig. D.2(a)(i)(iii) and (b)(i)(iii), we see that χ_q is greater than χ_s, and A_q is greater than A_s, showing that quantum illumination with joint measurement does indeed have an advantage over single-mode illumination. In the communication context, Alice can communicate with Bob with a higher bit-rate if Bob uses a probe entangled with an idler instead of a coherent state probe.

From Fig. D.2, we see that the performance of a coherent state probe is approximately equal to performance of an EPR probe when a local Gaussian measurement is performed on the mode B. However, A_s is slightly higher than A_c (and χ_s slightly higher than χ_c), because A_s is a concave function of energy [278]. By considering the ratio of A_s and A_c, we find that their relative difference approaches zero in both the limits $\epsilon \to 0$ and $\bar{n} \to 0$. This indicates that there is no advantage to using an EPR state for illumination, over a coherent state probe, if a Gaussian measurement is first made on mode B of the EPR state. A local Gaussian measurement on mode B of an EPR state will cause mode A to collapse to a single-mode Gaussian state. Hence, this is equivalent to using a distribution of single-mode Gaussian states for the probe, which, under the masking of strong environmental noise, gives an approximately equal knowledge about a weakly reflecting object as using a single mode coherent state probe.

D.4.3 Relating quantum advantage to discord consumed

To calculate the consumed discord $\delta_{\text{con}}(\text{A}|\text{B})$, we need to compute the discord of states $\rho^{(0)}$ and $\bar{\rho}$ when the entangled state ρ_{EPR} is used as probe and idler. $\rho^{(0)}$, the resulting state when Alice does nothing, is a Gaussian state whose discord is equal to the Gaussian discord, and additionally this discord is obtained when the measurement is a heterodyne measurement [279]. The state after encoding $\bar{\rho}$, however, is not Gaussian, thus the same rule does not apply. Unfortunately, calculating the discord of a general state is an NP-hard problem [280], so there is no method to calculate it efficiently. Here, we simplify the problem by restricting ourselves to Gaussian discord and calculate the consumed Gaussian discord $\delta^{\text{G}}_{\text{con}}(\text{A}|\text{B})$ instead. This is just Eq. (D.15) with the discords replaced with Gaussian discords.

The Gaussian discord of state $\bar{\rho}$ was obtained by numerically optimizing Eq. (D.11) over Gaussian measurements. It was found that the optimal point occurs when the measurement is a heterodyne measurement. The two discord values $\delta^{G(0)}(\text{A}|\text{B})$ and $\bar{\delta}^{\text{G}}(\text{A}|\text{B})$ are then substituted into Eq. (D.15) to obtain the consumed Gaussian discord.

Due to the optimality of the Gaussian discord of state $\rho^{(0)}$, and the fact that Gaussian discord is an upper bound for the discord for state $\bar{\rho}$, the consumed Gaussian discord

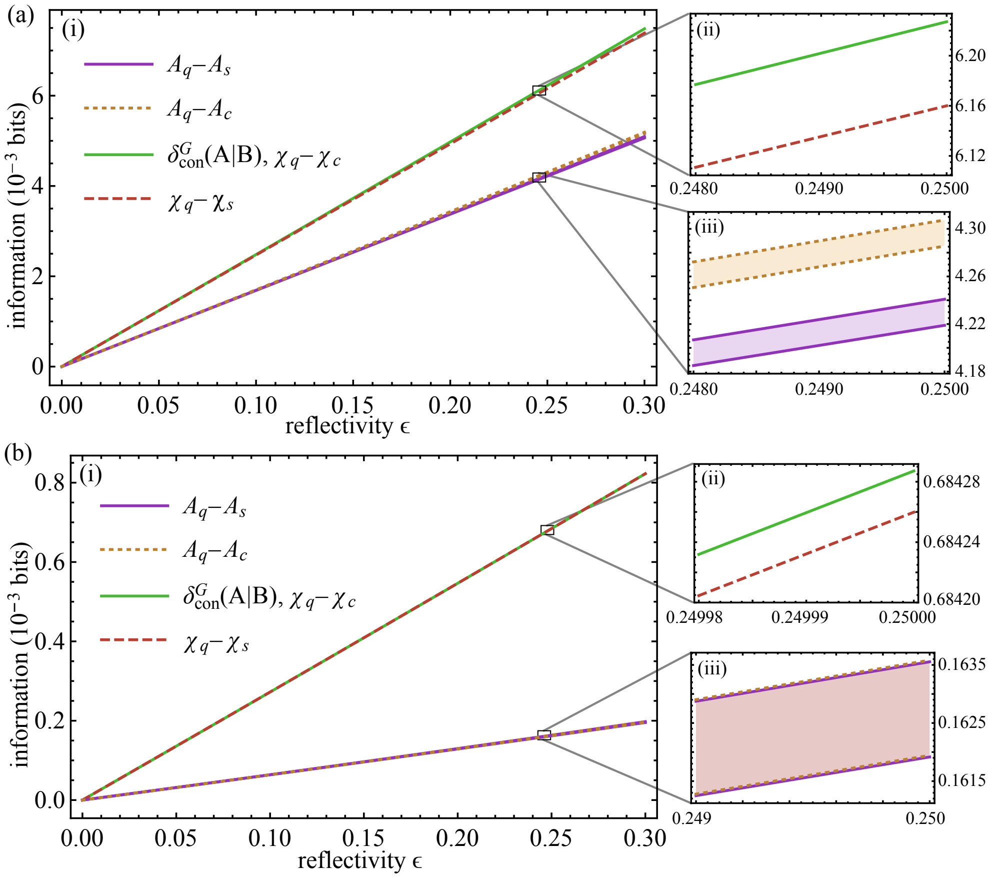


Figure D.3: The quantities $\chi_q - \chi_s$, $\chi_q - \chi_c$, $A_q - A_s$ and $A_q - A_c$, compared to the consumed Gaussian discord $\delta^{\mathrm{G}}_{\mathrm{con}}(\mathrm{A|B})$. The average photon number of the probe is (a) 0.5 and (b) 0.01. The mean photon number of the environment noise is 4. Each plot has two insets showing zoomed portions. The insets (ii) show $\delta^{\mathrm{G}}_{\mathrm{con}}(\mathrm{A|B})$, $\chi_q - \chi_s$ and $\chi_q - \chi_c$. The insets (iii) shows upper and lower bounds of $A_q - A_s$ and $A_q - A_c$.

is a lower bound of the consumed discord, i.e. $\delta^{\mathrm{G}}_{\mathrm{con}}(\mathrm{A|B}) \leq \delta_{\mathrm{con}}(\mathrm{A|B})$. A plot of the $\delta^{\mathrm{G}}_{\mathrm{con}}(\mathrm{A|B})$ compared to the information differences is shown in Fig. D.3.

As discussed in Sec. D.4.1, since a heterodyne measurement on mode B optimizes $\delta^{(0)}(\mathrm{A|B})$, and numerical results show that this is the case for $\bar{\delta}(\mathrm{A|B})$ and χ_c, from theorem 1, $\delta^{(0)}(\mathrm{A|B}) = \chi_q - \chi_c$. Numerical calculation of $\delta^{(0)}(\mathrm{A|B})$ and $\chi_q - \chi_c$ agree within the precision of the calculation, further verifying the theorem.

From Fig. D.3, we see that the difference in Holevo information between quantum illumination ($\chi_q - \chi_c$) and single-mode illumination ($\chi_q - \chi_s$) differ by 1.3% for $\bar{n} = 0.5$ and 0.005% for $\bar{n} = 0.01$ when $\epsilon = 0.3$. The percentage difference approaches zero when $\epsilon \to 0$. Since $\delta^{\mathrm{G}}_{\mathrm{con}}(\mathrm{A|B}) = \chi_q - \chi_c$, this leads us to the conclusion that in limit of low reflectivity and low probe energy, $\chi_q - \chi_s$ converges to the Gaussian discord consumed. Hence, discord encoded can suitably explain the quantum advantage of quantum illumination, if quantum illumination is viewed as a communication problem with access to devices such as quantum memory.

On the other hand, $A_q - A_s$ which quantifies the performance advantage for quantum illumination in the single copy measurement case is more relevant from a practical point of view since this does not require the storage of quantum states [261]. From Fig. D.3 we see that $\delta_{\mathrm{con}}^{\mathrm{G}}(\mathrm{A}|\mathrm{B})$ is greater than $A_q - A_s$ and $A_q - A_c$. This discrepancy is mainly due to the difference between the Holevo information χ_q and the accessible information A_q for the states involved in quantum illumination. Hence, measuring each illumination event separately does not fully harness the benefits offered by the discord. However, it is sufficient to provide some quantum advantage over single-mode illumination.

D.5 Conclusion

In [272], it has been shown that quantum discord coincide exactly with quantum advantage in a DV quantum illumination. Here, we complete the picture by extending the framework to CV quantum illumination [260]. To this end, we numerically calculated the performance enhancement quantum illumination has over single-mode illumination and compared it to the Gaussian discord of the system. We derived an analytic result showing that $\delta_{\mathrm{con}}^{\mathrm{G}}(\mathrm{A}|\mathrm{B}) = \chi_q - \chi_c$ provided condition 3 of theorem 1 is met. Our main result is that the quantum advantage in terms of Holevo information matches the consumed discord in the limit of low probe energy and low object reflectivity ($\bar{n} \to 0$ and $\epsilon \to 0$). This is in agreement with the DV counterpart, which analogously assumes an maximally entropic illumination environment.

Several remarks on relation with other works are in order. In deriving our results, we have demonstrated that a joint measurement over the returning probe and idler is necessary to exploit the surviving quantum correlation to determine the non-unitary encoding. Similar to [251], a coherent interaction is required to unlock the information encoded via unitary discord consumption. The discrepancy between the quantum advantage offered by Holevo information and accessible information is in concordance with recent findings, where the improvement of error probability of quantum illumination over single-mode illumination is limited to 3 dB (out of maximum gain of 6 dB) for single copies separate measurement in the intense white noise limit [262, 261].

We note other efforts in quantifying the source of enhancement in quantum illumination-like protocols. In [281], mutual information is used to quantify the advantage offered by entangled source over correlated thermal source. Gaussian discriminating strength is proposed to distinguish the absence or presence of a set of unitary operation in [282, 283]. The role of correlation in the improvement of channel loss detection is also established by linking discord to the performance numerically [284]. Meanwhile, several other cryptographic and metrological variants of illumination has been proposed and demonstrated recently [267, 264], which we envisage our framework would shed light in understanding the discord's role in the their quantum enhancement.

Bibliography

[1] A. Franzen, "ComponentLibrary: a free vector graphics library for optics," *Licensed under a Creative Commons Attribution-NonCommercial* **3**.

[2] T. Denny, B. Dodson, A. K. Lenstra, and M. S. Manasse, "On the factorization of RSA-120," in *Annual International Cryptology Conference* pp. 166–174 Springer 1993.

[3] T. Kleinjung et al., "Factorization of a 768-bit RSA modulus," in *Annual Cryptology Conference* pp. 333–350 Springer 2010.

[4] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review* **41**, 303 (1999).

[5] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature* **299**, 802 (1982).

[6] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Rev. Mod. Phys.* **89**, 015004 (2017).

[7] IDQuantique, *QUANTIS random number generator*, `http://www.idquantique.com/random-number-generation`.

[8] QuintessenceLabs, *qStream*, `https://www.quintessencelabs.com/products/qstream-quantum-true-random-number-generator`.

[9] M. Peev et al., "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics* **11**, 075001 (2009).

[10] M. Sasaki et al., "Field test of quantum key distribution in the Tokyo QKD Network," *Optics express* **19**, 10387 (2011).

[11] S.-K. Liao et al., "Satellite-to-ground quantum key distribution," *Nature* **549**, 43 (2017).

[12] L. K. Shalm et al., "Strong loophole-free test of local realism," *Phys. Rev. Lett.* **115**, 250402 (2015).

[13] M. Giustina et al., "Significant-loophole-free test of Bell's theorem with entangled photons," *Phys. Rev. Lett.* **115**, 250401 (2015).

[14] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W.

Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres," *Nature* **526**, 682 (2015).

[15] E. Diamanti, H. K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Information* **2** (2016).

[16] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photonics* **9**, 163 (2015).

[17] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," *Scientific Reports* **6** (2016).

[18] P. A. M. Dirac*The principles of quantum mechanics* No. 27 (Oxford university press, 1981).

[19] R. J. Glauber, "The quantum theory of optical coherence," *Physical Review* **130**, 2529 (1963).

[20] C. Cohen-Tannoudji, J. Dupont-Roc, and G. Grynberg, "Photons and atoms: introduction to quantum electrodynamics," (2001).

[21] W. Vogel and D.-G. Welsch, *Quantum optics* (John Wiley & Sons, 2006).

[22] G. Grynberg, A. Aspect, and C. Fabre, *Introduction to quantum optics: from the semi-classical approach to quantized light* (Cambridge university press, 2010).

[23] M. A. Nielsen and I. L. Chuang, "Quantum information and quantum computation," *Cambridge University Press* **2**, 23 (2000).

[24] 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).

[25] U. Leonhardt and H. Paul, "Measuring the quantum state of light," *Progress in Quantum Electronics* **19**, 89 (1995).

[26] R. J. Glauber, "Coherent and Incoherent States of the Radiation Field," *Phys. Rev.* **131**, 2766 (1963).

[27] E. C. G. Sudarshan, "Equivalence of Semiclassical and Quantum Mechanical Descriptions of Statistical Light Beams," *Phys. Rev. Lett.* **10**, 277 (1963).

[28] T. Kiesel and W. Vogel, "Nonclassicality filters and quasiprobabilities," *Phys. Rev. A* **82**, 032107 (2010).

[29] T. Kiesel, W. Vogel, B. Hage, and R. Schnabel, "Direct Sampling of Negative Quasiprobabilities of a Squeezed State," *Phys. Rev. Lett.* **107**, 113604 (2011).

[30] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal* **27**, 379 (1948).

[31] A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," *Problemy Peredachi Informatsii* **9**, 3 (1973).

[32] T. M. Cover and J. A. Thomas, *Elements of information theory* (John Wiley & Sons, 2012).

[33] P. K. Lam, *Applications of Quantum Electro-Optic Control and Squeezed Light*, PhD thesis Australian National University 1998.

[34] W. P. Bowen, *Experiments towards a quantum information network with squeezed light and entanglement*, PhD thesis Australian National University 2003.

[35] K. Blow, R. Loudon, S. J. Phoenix, and T. Shepherd, "Continuum fields in quantum optics," *Phys. Rev. A* **42**, 4102 (1990).

[36] E. D. Black, "An introduction to Pound–Drever–Hall laser frequency stabilization," *American Journal of Physics* **69**, 79 (2001).

[37] B. Sparkes, H. Chrzanowski, D. Parrain, B. Buchler, P. Lam, and T. Symul, "A scalable, self-analyzing digital locking system for use on quantum optics experiments," *Review of Scientific Instruments* **82**, 075113 (2011).

[38] H. P. Yuen and V. W. Chan, "Noise in homodyne and heterodyne detection," *Optics Letters* **8**, 177 (1983).

[39] B. C. Buchler, *Electro-optic Control of Quantum Measurements*, PhD thesis Australian National University 2001.

[40] E. Arthurs and J. Kelly, "BSTJ briefs: On the simultaneous measurement of a pair of conjugate observables," *The Bell System Technical Journal* **44**, 725 (1965).

[41] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *npj Quantum Information* **2**, 16021 (2016).

[42] M. N. Bera, A. Acín, M. Kuś, M. Mitchell, and M. Lewenstein, "Randomness in Quantum Mechanics: Philosophy, Physics and Technology," *arXiv preprint arXiv:1611.02176* (2016).

[43] G. Marsaglia, "Random numbers fall mainly in the planes," *Proceedings of the National Academy of Sciences* **61**, 25 (1968).

[44] M. Stipcevic, "Quantum random number generators and their applications in cryptography," in *SPIE Defense, Security, and Sensing* pp. 837504–837504 International Society for Optics and Photonics 2012.

[45] P. Xu, Y. Wong, T. Horiuchi, and P. Abshire, "Compact floating-gate true random number generator," *Electronics Letters* **42**, 1346 (2006).

[46] B. Sunar, W. J. Martin, and D. R. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," *Computers, IEEE Transactions on* **56**, 109 (2007).

[47] A. Uchida et al., "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photonics* **2**, 728 (2008).

[48] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," *Nature Photonics* **4**, 58 (2010).

[49] D. Marangon, G. Vallone, and P. Villoresi, "Random bits, true and unbiased, from atmospheric turbulence.," *Scientific Reports* **4**, 5490 (2014).

[50] C. S. Calude, M. J. Dinneen, M. Dumitrescu, and K. Svozil, "Experimental evidence of quantum randomness incomputability," *Phys. Rev. A* **82**, 022102 (2010).

[51] K. Svozil, "Three criteria for quantum random-number generators based on beam splitters," *Phys. Rev. A* **79**, 054306 (2009).

[52] M. Born, "Quantenmechanik der stoßvorgänge," *Zeitschrift für Physik* **38**, 803 (1926).

[53] D. Bohm, "A suggested interpretation of the quantum theory in terms of" hidden" variables. I," *Phys. Rev.* **85**, 166 (1952).

[54] W. Kinzel and G. Reents, "Physik per Computer," *Spektrum Akademischer Verlag, Heidelberg* **22**, 33 (1996).

[55] M. Isida and H. Ikeda, "Random number generator," *Annals of the Institute of Statistical Mathematics* **8**, 119 (1956).

[56] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Review of Scientific Instruments* **71**, 1675 (2000).

[57] M. Fiorentino, C. Santori, S. Spillane, R. Beausoleil, and W. Munro, "Secure self-calibrating quantum random-bit generator," *Physical Review A* **75**, 032334 (2007).

[58] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson, "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements," *Applied Physics Letters* **98**, 171105 (2011).

[59] M. A. Wayne and P. G. Kwiat, "Low-bias high-speed quantum random number generator via shaped optical pulses," *Optics Express* **18**, 9351 (2010).

[60] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, post-processing free, quantum random number generator," *Applied Physics Letters* **93**, 031109 (2008).

[61] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, "Quantum Random Number Generation on a Mobile Phone," *Phys. Rev. X* **4**, 031056 (2014).

[62] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," *Optics Letters* **35**, 312 (2010).

[63] H. Guo, W. Tang, Y. Liu, and W. Wei, "Truly random number generation based on measurement of phase noise of a laser," *Phys. Rev. E* **81**, 051137 (2010).

[64] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. Torres, M. Mitchell, and V. Pruneri, "True random numbers from amplified quantum vacuum," *Optics Express* **19**, 20665 (2011).

[65] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H. K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," *Optics Express* **20**, 12366 (2012).

[66] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. Mitchell, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," *Optics Express* **22**, 1645 (2014).

[67] Z. Yuan, M. Lucamarini, J. Dynes, B. Fröhlich, A. Plews, and A. Shields, "Robust random number generation using steady-state emission of gain-switched laser diodes," *Applied Physics Letters* **104**, 261112 (2014).

[68] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations," *Review of Scientific Instruments* **86**, 063105 (2015).

[69] M. Stipčević and B. M. Rogina, "Quantum random number generator based on photonic emission in semiconductors," *Review of Scientific Instruments* **78**, 045104 (2007).

[70] C. R. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission," *Optics Express* **18**, 23584 (2010).

[71] Y. Liu, M. Zhu, B. Luo, J. Zhang, and H. Guo, "Implementation of 1.6 Tb s- 1 truly random number generation based on a super-luminescent emitting diode," *Laser Physics Letters* **10**, 045001 (2013).

[72] P. J. Bustard, D. G. England, J. Nunn, D. Moffatt, M. Spanner, R. Lausten, and B. J. Sussman, "Quantum random bit generation using energy fluctuations in stimulated Raman scattering," *Optics Express* **21**, 29350 (2013).

[73] Y. Shen, L. Tian, and H. Zou, "Practical quantum random number generator based on measuring the shot noise of vacuum states," *Phys. Rev. A* **81**, 063814 (2010).

[74] T. Symul, S. Assad, and P. K. Lam, "Real time demonstration of high bitrate quantum random number generation with coherent laser light," *Applied Physics Letters* **98**, 231103 (2011).

[75] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," *Nature Photonics* **4**, 711 (2010).

[76] S. Pironio et al., "Random numbers certified by Bell's theorem," *Nature* **464**, 1021 (2010).

[77] A. N. Kolmogorov, "On tables of random numbers," *Sankhyā: The Indian Journal of Statistics, Series A* , 369 (1963).

[78] P. Martin-Löf, "The definition of random sequences," *Information and control* **9**, 602 (1966).

[79] D. Frauchiger, R. Renner, and M. Troyer, "True randomness from realistic quantum devices," *arXiv:1311.4547* (2013).

[80] E. Barker and J. Kelsey, "Recommendation for the Entropy Sources Used for Random Bit Generation," *NIST DRAFT Special Publication 800-90B* (2012).

[81] G. Marsaglia, "DIEHARD Test suite," 1998.

[82] R. Konig, R. Renner, and C. Schaffner, "The operational meaning of min-and max-entropy," *Information Theory, IEEE Transactions on* **55**, 4337 (2009).

[83] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM Journal on Computing* **38**, 97 (2008).

[84] C. Abellán, W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell, "Generation of fresh and pure random numbers for loophole-free Bell tests," *Phys. Rev. Lett.* **115**, 250403 (2015).

[85] R. Shaltiel, "Recent developments in explicit constructions of extractors," *Bulletin of the EATCS* **77**, 67 (2002).

[86] A. De, C. Portmann, T. Vidick, and R. Renner, "Trevisan's extractor in the presence of quantum side information," *SIAM Journal on Computing* **41**, 915 (2012).

[87] W. Mauerer, C. Portmann, and V. B. Scholz, "A modular framework for randomness extraction based on Trevisan's construction," *arXiv:1212.0520* (2012).

[88] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," *Phys. Rev. A* **87** (2013).

[89] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, "Quantum randomness certified by the uncertainty principle," *Physical Review A* **90**, 052327 (2014).

[90] Y. Z. Law et al., "Quantum randomness extraction for various levels of characterization of the devices," *Journal of Physics A: Mathematical and Theoretical* **47**, 424028 (2014).

[91] R. Renner, "Security of quantum key distribution," *International Journal of Quantum Information* **6**, 1 (2008).

[92] S. Pironio and S. Massar, "Security of practical private randomness generation," *Phys. Rev. A* **87**, 012336 (2013).

[93] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover hashing against quantum side information," *Information Theory, IEEE Transactions on* **57**, 5524 (2011).

[94] B. Christensen et al., "Detection-loophole-free test of quantum nonlocality, and applications," *Phys. Rev. Lett.* **111**, 130406 (2013).

[95] T. Durt, C. Belmonte, L.-P. Lamoureux, K. Panajotov, F. Van den Berghe, and H. Thienpont, "Fast quantum-optical random-number generators," *Phys. Rev. A* **87**, 022339 (2013).

[96] T. Yamazaki and A. Uchida, "Performance of Random Number Generators Using Noise-Based Superluminescent Diode and Chaos-Based Semiconductor Lasers," *IEEE Journal of Selected Topics in Quantum Electronics* **19**, 0600309 (2013).

[97] N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer, "Fast Random Bit Generation Using a Chaotic Laser: Approaching the Information Theoretic Limit," *IEEE Journal of Quantum Electronics* **49**, 910 (2013).

[98] B. Barak, R. Shaltiel, and E. Tromer, "True random number generators secure in a changing environment," p. 166 (2003).

[99] Y. Dodis, R. Gennaro, J. Håstad, H. Krawczyk, and T. Rabin, "Randomness extraction and key derivation using the CBC, cascade and HMAC modes," in *Advances in Cryptology–CRYPTO 2004* pp. 494–510 Springer 2004.

[100] H. Krawczyk, "Cryptographic extraction and key derivation: The HKDF scheme," in *Advances in Cryptology–CRYPTO 2010* pp. 631–648 Springer 2010.

[101] Y. Cliff, C. Boyd, and J. G. Nieto, "How to Extract and Expand Randomness: A Summary and Explanation of Existing Results," in *Applied Cryptography and Network Security* pp. 53–70 Springer 2009.

[102] O. Chevassut, P.-A. Fouque, P. Gaudry, and D. Pointcheval, "The twist-augmented technique for key exchange,", in *Public Key Cryptography-PKC 2006* pp. 410–426 Springer 2006.

[103] Y.-Q. Nie, H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan, "Practical and fast quantum random number generation based on photon arrival time relative to external reference," *Applied Physics Letters* **104**, 051110 (2014).

[104] B. Barak, Y. Dodis, H. Krawczyk, O. Pereira, K. Pietrzak, F.-X. Standaert, and Y. Yu, "Leftover hash lemma, revisited,", in *Advances in Cryptology–CRYPTO 2011* pp. 1–20 Springer 2011.

[105] P. FIPS, "197: Advanced encryption standard (AES)," *National Institute of Standards and Technology* (2001).

[106] A. Rukhin et al., "Statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST special publication," (2010).

[107] *The Australian National University Quantum Random Number Server*, `https://qrng.anu.edu.au`.

[108] I. Białynicki-Birula and J. Mycielski, "Uncertainty relations for information entropy in wave mechanics," *Commun.Math. Phys.* **44**, 129 (1975).

[109] H. Maassen and J. Uffink, "Generalized entropic uncertainty relations," *Phys. Rev. Lett.* **60**, 1103 (1988).

[110] A. Einstein, B. Podolsky, and N. Rosen, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?," *Phys. Rev.* **47**, 777 (1935).

[111] M. Berta, M. Christandl, R. Colbeck, J. Renes, and R. Renner, "The uncertainty principle in the presence of quantum memory," *Nature Phys.* **6**, 659 (2010).

[112] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.* **81**, 1301 (2009).

[113] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," Proceedings of International Conference on Computers, Systems and Signal Processing, Bangalore, India 1984.

[114] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.* **67**, 661 (1991).

[115] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A* **61**, 010303 (1999).

[116] M. Hillery, "Quantum cryptography with squeezed states," *Phys. Rev. A* **61**, 022309 (2000).

[117] M. Reid, "Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations," *Phys. Rev. A* **62**, 062308 (2000).

[118] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," *Phys. Rev. Lett.* **88**, 057902 (2002).

[119] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," *Nature* **421**, 238 (2003).

[120] V. Scarani and R. Renner, "Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Post-processing," *Phys. Rev. Lett.* **100**, 200501 (2008).

[121] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nature Communications* **3**, 634 (2012).

[122] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. Scholz, M. Tomamichel, and R. Werner, "Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks," *Phys. Rev. Lett.* **109**, 100502 (2012).

[123] F. Furrer, "Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle," *Phys. Rev. A* **90**, 042325 (2014).

[124] M. Berta, F. Furrer, and V. B. Scholz, "The smooth entropy formalism for von Neumann algebras," *Journal of Mathematical Physics* **57**, 015213 (2016).

[125] F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, "Position-momentum uncertainty relations in the presence of quantum memory," *Journal of Mathematical Physics* **55**, 122205 (2014).

[126] R. L. Frank and E. H. Lieb, "Extended Quantum Conditional Entropy and Quantum Uncertainty Inequalities," *Communications In Mathematical Physics* **323**, 487 (2014).

[127] N. Walk, *"Continuous Variable Quantum Communication"*, PhD thesis The University of Queensland 2014.

[128] C. Weedbrook, A. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum Cryptography Without Switching," *Phys. Rev. Lett.* **93**, 170504 (2004).

[129] F. Grosshans, N. J. Cerf, P. Grangier, J. Wenger, and R. Tualle-Brouri, "Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables," *Quantum Inf. Comput.* **3**, 535 (2003).

[130] 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).

[131] R. García-Patrón and N. J. Cerf, "Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution," *Phys. Rev. Lett.* **97**, 190503 (2006).

[132] M. Navascués, F. Grosshans, and A. Acín, "Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography," *Phys. Rev. Lett.* **97**, 190502 (2006).

[133] R. Renner and J. Cirac, "de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography," *Phys. Rev. Lett.* **102**, 110504 (2009).

[134] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proc. R. Soc. A* **461**, 207 (2005).

[135] M. Tomamichel and R. Renner, "Uncertainty Relation for Smooth Entropies," *Phys. Rev. Lett.* **106**, 110506 (2011).

[136] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, "One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering," *Phys. Rev. A* **85**, 010301 (2012).

[137] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-Independent Security of Quantum Cryptography against Collective Attacks," *Phys. Rev. Lett.* **98**, 230501 (2007).

[138] L. Masanes, S. Pironio, and A. Acin, "Secure device-independent quantum key distribution with causally independent measurement devices," *Nature Communications* **2**, 238 (2011).

[139] E. Hänggi and R. Renner, "Device-Independent Quantum Key Distribution with Commuting Measurements," *arXiv:1009.1833* (2010).

[140] J. Barrett, L. Hardy, and A. Kent, "No signaling and quantum key distribution," *Phys. Rev. Lett.* **95**, 10503 (2005).

[141] J. Barrett, R. Colbeck, and A. Kent, "Unconditionally secure device-independent quantum key distribution with only two devices," *Phys. Rev. A* **86**, 062326 (2012).

[142] U. Vazirani and T. Vidick, "Fully Device-Independent Quantum Key Distribution," *Phys. Rev. Lett.* **113**, 140501 (2014).

[143] B. G. Christensen, K. T. Mccusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, "Detection-Loophole-Free Test of Quantum Nonlocality, and Applications," *Phys. Rev. Lett.* **111**, 130406 (2013).

[144] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger, "Bell violation using entangled photons without the fair-sampling assumption," *Nature* **497**, 227 (2013).

[145] J. S. Bell, "EPR Correlations and EPW Distributions," *Annals of the New York Academy of Sciences* **480**, 263 (1986).

[146] H. Wiseman, S. Jones, and A. Doherty, "Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox," *Phys. Rev. Lett.* **98**, 140402 (2007).

[147] H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," *Phys. Rev. Lett.* **108**, 130503 (2012).

[148] S. Braunstein and S. Pirandola, "Side-Channel-Free Quantum Key Distribution," *Phys. Rev. Lett.* **108**, 130502 (2012).

[149] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, "High-rate measurement-device-independent quantum cryptography," *Nature Photonics* **9**, 397 (2015).

[150] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, "Measurement-device-independent quantum key distribution over 200 km," *Phys. Rev. Lett.* **113**, 190501 (2014).

[151] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, "Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks," *Phys. Rev. Lett.* **111**, 130501 (2013).

[152] M. D. Reid, "Demonstration of the Einstein-Podolsky-Rosen paradox using nondegenerate parametric amplification," *Phys. Rev. A* **40**, 913 (1989).

[153] M. Reid, "Signifying quantum benchmarks for qubit teleportation and secure quantum communication using Einstein-Podolsky-Rosen steering inequalities," *Phys. Rev. A* **88**, 062338 (2013).

[154] 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," *Nature Phys.* **11**, 167 (2015).

[155] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a Gaussian modulation," *Phys. Rev. A* **84**, 062317 (2011).

[156] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature Photon* **7**, 378 (2013).

[157] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, "Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks," *Nature Communications* **6**, 8795 (2015).

[158] H. A. Haus and J. A. Mullen, "Quantum Noise in Linear Amplifiers," *Phys. Rev.* **128**, 2407 (1962).

[159] C. M. Caves, "Quantum limits on noise in linear amplifiers," *Phys. Rev. D* **26**, 1817 (1982).

[160] T. C. Ralph and A. P. Lund, "Nondeterministic Noiseless Linear Amplification of Quantum Systems," *AIP Conference Proceedings* **1110**, 155 (2009).

[161] J. Fiurášek, "Optimal probabilistic cloning and purification of quantum states," *Phys. Rev. A* **70**, 032308 (2004).

[162] V. Dunjko and E. Andersson, "Truly noiseless probabilistic amplification," *Phys. Rev. A* **86**, 042322 (2012).

[163] J. Jeffers, "Nondeterministic amplifier for two-photon superpositions," *Phys. Rev. A* **82**, 063828 (2010).

[164] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, "Heralded noiseless linear amplification and distillation of entanglement," *Nature Photonics* **4**, 316 (2010).

[165] F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, and P. Grangier, "Implementation of a nondeterministic optical noiseless amplifier," *Phys. Rev. Lett.* **104**, 123603 (2010).

[166] F. Ferreyrol, R. Blandino, M. Barbieri, R. Tualle-Brouri, and P. Grangier, "Experimental realization of a nondeterministic optical noiseless amplifier," *Phys. Rev. A* **83**, 063801 (2011).

[167] J. Fiurasek, "Engineering quantum operations on traveling light beams by multiple photon addition and subtraction," *Phys. Rev. A* **80**, 053822 (2009).

[168] P. Marek and R. Filip, "Coherent-state phase concentration by quantum probabilistic amplification," *Phys. Rev. A* **81**, 022302 (2010).

[169] A. Zavatta, J. Fiurášek, and M. Bellini, "A high-fidelity noiseless amplifier for quantum light states," *Nature Photonics* **5**, 52 (2010).

[170] M. A. Usuga, C. R. Müller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs, and U. L. Andersen, "Noise-powered probabilistic concentration of phase information," *Nat Phys* **6**, 767 (2010).

[171] S. Pandey, Z. Jiang, J. Combes, and C. M. Caves, "Quantum limits on probabilistic amplifiers," *Phys. Rev. A* **88**, 033852 (2013).

[172] N. A. McMahon, A. P. Lund, and T. C. Ralph, "Optimal architecture for a nondeterministic noiseless linear amplifier," *Phys. Rev. A* **89**, 023846 (2014).

[173] N. Gisin, S. Pironio, and N. Sangouard, "Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier," *Physical review letters* **105**, 070501 (2010).

[174] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, "Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier," *Phys. Rev. A* **86** (2012).

[175] J. Fiurášek and N. J. Cerf, "Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution," *Phys. Rev. A* **86**, 060302 (2012).

[176] N. Walk, T. C. Ralph, T. Symul, and P. K. Lam, "Security of continuous-variable quantum cryptography with Gaussian postselection," *Physical Review A* **87**, 020303 (2013).

[177] T. C. R. S. Kocsis, G. Y. Xiang and G. J. Pryde, "Heralded noiseless amplification of a photon polarization qubit," *Nat Phys* **9**, 23 (2013).

[178] A. E. Ulanov, I. A. Fedorov, A. A. Pushkina, Y. V. Kurochkin, T. C. Ralph, and L. I., "Undoing the effect of loss on quantum entanglement," *Nat Photon* **9**, 764 (2015).

[179] C. R. Müller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs, and U. L. Andersen, "Probabilistic cloning of coherent states without a phase reference," *Phys. Rev. A* **86**, 010305 (2012).

[180] J. Bernu, S. Armstrong, T. Symul, T. C. Ralph, and P. K. Lam, "Theoretical analysis of an ideal noiseless linear amplifier for Einstein-Podolsky-Rosen entanglement distillation," *Journal of Physics B: Atomic, Molecular and Optical Physics* **47**, 215503 (2014).

[181] J. Dias and T. C. Ralph, "Quantum repeaters using continuous-variable teleportation," *Phys. Rev. A* **95**, 022312 (2017).

[182] T. C. Ralph, "Quantum error correction of continuous-variable states against Gaussian noise," *Phys. Rev. A* **84**, 022339 (2011).

[183] J. Fiurášek and N. Cerf, "Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution," *Phys. Rev. A* **86**, 060302 (2012).

[184] N. Walk, T. C. Ralph, T. Symul, and P. K. Lam, "Security of continuous-variable quantum cryptography with Gaussian postselection," *Phys. Rev. A* **87**, 020303 (2013).

[185] H. M. Chrzanowski, N. Walk, S. M. Assad, J. Janousek, S. Hosseini, T. C. Ralph, T. Symul, and P. K. Lam, "Measurement-based noiseless linear amplification for quantum communication," *Nature Photonics* **8**, 333 (2014).

[186] J. Fiurášek, "Optimal probabilistic cloning and purification of quantum states," *Phys. Rev. A* **70**, 032308 (2004).

[187] K. Shimoda, H. Takahasi, and C. H. Townes, "Fluctuations in amplification of quanta with application to maser amplifiers," *Journal of the Physical Society of Japan* **12**, 686 (1957).

[188] H. P. Yuen and J. H. Shapiro, "Generation and detection of two-photon coherent states in degenerate four-wave mixing," *Optics Letters* **4**, 334 (1979).

[189] Z. Ou, S. Pereira, and H. Kimble, "Quantum noise reduction in optical amplification," *Phys. Rev. Lett.* **70**, 3239 (1993).

[190] J. A. Levenson, I. Abram, T. Rivera, and P. Grangier, "Reduction of quantum noise in optical parametric amplification," *JOSA B* **10**, 2233 (1993).

[191] V. Josse, M. Sabuncu, N. J. Cerf, G. Leuchs, and U. L. Andersen, "Universal optical amplification without nonlinearity," *Phys. Rev. Lett.* **96**, 163602 (2006).

[192] U. L. Andersen and R. Filip, "Quantum feed-forward control of light," *Progress in Optics* **53**, 365 (2009).

[193] R. Blandino, N. Walk, A. P. Lund, and T. C. Ralph, "Channel purification via continuous-variable quantum teleportation with Gaussian postselection," *Phys. Rev. A* **93**, 012326 (2016).

[194] T. C. Ralph and A. P. Lund, *Quantum Communication Measurement and Computing Proceedings of 9th International Conference* , 155 (2009).

[195] S. Kocsis, G. Y. Xiang, T. C. Ralph, and G. J. Pryde, "Heralded noiseless amplification of a photon polarization qubit," *Nat Phys* **9**, 23 (2012).

[196] U. L. Andersen, V. Josse, and G. Leuchs, "Unconditional quantum cloning of coherent states with linear optics," *Phys. Rev. Lett.* **94**, 240503 (2005).

[197] V. Scarani, S. Iblisdir, N. Gisin, and A. Acin, "Quantum Cloning," *Rev. Mod. Phys.* **77**, 1225 (2005).

[198] N. J. Cerf and J. Fiurášek, "Optical quantum cloning," *Progress in Optics* **49**, 455 (2006).

[199] V. Bužek and M. Hillery, "Quantum copying: Beyond the no-cloning theorem," *Phys. Rev. A* **54**, 1844 (1996).

[200] N. Gisin and S. Massar, "Optimal Quantum Cloning Machines," *Phys. Rev. Lett.* **79**, 2153 (1997).

[201] D. Bruss, A. Ekert, and C. Macchiavello, "Optimal Universal Quantum Cloning and State Estimation," *Phys. Rev. Lett.* **81**, 2598 (1998).

[202] V. Bužek and M. Hillery, "Universal Optimal Cloning of Arbitrary Quantum States: From Qubits to Quantum Registers," *Phys. Rev. Lett.* **81**, 5003 (1998).

[203] C. Simon, G. Weihs, and A. Zeilinger, "Optimal Quantum Cloning via Stimulated Emission," *Phys. Rev. Lett.* **84**, 2993 (2000).

[204] N. J. Cerf, A. Ipe, and X. Rottenberg, "Cloning of Continuous Quantum Variables," *Phys. Rev. Lett.* **85**, 1754 (2000).

[205] N. J. Cerf and S. Iblisdir, "Optimal **N** -to-M cloning of conjugate quantum variables," *Phys. Rev. A* **62**, 040301 (2000).

[206] G. Lindblad, "Cloning the quantum oscillator," *Journal of Physics A: Mathematical and General* **33**, 5059 (2000).

[207] J. Fiurášek, "Optical implementation of continuous-variable quantum cloning machines," *Phys. Rev. Lett.* **86**, 4942 (2001).

[208] S. L. Braunstein, N. J. Cerf, S. Iblisdir, P. van Loock, and S. Massar, "Optimal Cloning of Coherent States with a Linear Amplifier and Beam Splitters," *Phys. Rev. Lett.* **86**, 4938 (2001).

[209] A. Lamas-Linares, C. Simon, J. C. Howell, and D. Bouwmeester, "Experimental quantum cloning of single photons," *Science* **296**, 712 (2002).

[210] S. Fasel, N. Gisin, G. Ribordy, V. Scarani, and H. Zbinden, "Quantum Cloning with an Optical Fiber Amplifier," *Phys. Rev. Lett.* **89** (2002).

[211] L.-M. Duan and G.-C. Guo, "Probabilistic cloning and identification of linearly independent quantum states," *Phys. Rev. Lett.* **80**, 4999 (1998).

[212] T. C. Ralph, A. Gilchrist, G. J. Milburn, W. J. Munro, and S. Glancy, "Quantum computation with optical coherent states," *Phys. Rev. A* **68**, 042319 (2003).

[213] H. Chen, D. Lu, B. Chong, G. Qin, X. Zhou, X. Peng, and J. Du, "Experimental Demonstration of Probabilistic Quantum Cloning," *Phys. Rev. Lett.* **106**, 180404 (2011).

[214] H.-J. Kim, S.-Y. Lee, S.-W. Ji, and H. Nha, "Quantum linear amplifier enhanced by photon subtraction and addition," *Phys. Rev. A* **85**, 013839 (2012).

[215] E. Eleftheriadou, S. M. Barnett, and J. Jeffers, "Quantum Optical State Comparison Amplifier," *Phys. Rev. Lett.* **111**, 213601 (2013).

[216] M. A. Usuga, C. R. Muller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs, and U. L. Andersen, "Noise-powered probabilistic concentration of phase information," *Nat Phys* **6**, 767 (2010).

[217] R. J. Donaldson, R. J. Collins, E. Eleftheriadou, S. M. Barnett, J. Jeffers, and G. S. Buller, "Experimental Implementation of a Quantum Optical State Comparison Amplifier," *Phys. Rev. Lett.* **114**, 120505 (2015).

[218] A. Chefles and S. M. Barnett, "Strategies and networks for state-dependent quantum cloning," *Phys. Rev. A* **60**, 136 (1999).

[219] J. Combes, N. Walk, A. Lund, T. Ralph, and C. M. Caves, "Models of reduced-noise, probabilistic linear amplifiers," *Phys. Rev. A* **93**, 052310 (2016).

[220] N. Walk, A. P. Lund, and T. C. Ralph, "Nondeterministic noiseless amplification via non-symplectic phase space transformations," *New Journal of Physics* **15**, 073014 (2013).

[221] N. Walk, T. C. Ralph, T. Symul, and P. K. Lam, "Security of continuous-variable quantum cryptography with Gaussian postselection," *Phys. Rev. A* **87** (2013).

[222] M. G. Paris, "Displacement operator by beam splitter," *Physics Letters A* **217**, 78 (1996).

[223] J. Jeffers, "Optical amplifier-powered quantum optical amplification," *Phys. Rev. A* **83**, 053818 (2011).

[224] F. Grosshans and P. Grangier, "Quantum cloning and teleportation criteria for continuous quantum variables," *Phys. Rev. A* **64**, 010301 (2001).

[225] U. L. Andersen and G. Leuchs, "Optical amplification at the quantum limit," *Journal of Modern Optics* **54**, 2351 (2007).

[226] D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent ultrafast quantum random number generation," *Physical review letters* **118**, 060503 (2017).

[227] S. Wehner, C. Schaffner, and B. Terhal, "Cryptography from Noisy Storage," *Phys. Rev. Lett.* **100**, 220502 (2008).

[228] S. Wehner, M. Curty, C. Schaffner, and H.-K. Lo, "Implementation of two-party protocols in the noisy-storage model," *Phys. Rev. A* **81**, 052336 (2010).

[229] C. Schaffner, "Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model," *Phys. Rev. A* **82**, 032308 (2010).

[230] S. Pironio, L. Masanes, A. Leverrier, and A. Acín, "Security of Device-Independent Quantum Key Distribution in the Bounded-Quantum-Storage Model," *Phys. Rev. X* **3**, 031007 (2013).

[231] N. Gisin, S. Pironio, and N. Sangouard, "Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier," *Phys. Rev. Lett.* **105**, 70501 (2010).

[232] R. Blandino, M. Barbieri, P. Grangier, and R. Tualle-Brouri, "Heralded noiseless linear amplification and quantum channels," *Phys. Rev. A* **91**, 062305 (2015).

[233] Y. Zhang, Z. Li, C. Weedbrook, K. Marshall, S. Pirandola, S. Yu, and H. Guo, "Noiseless Linear Amplifiers in Entanglement-Based Continuous-Variable Quantum Key Distribution," *Entropy* **17**, 4547 (2015).

[234] Z. Li, Y. Zhang, X. Wang, B. Xu, X. Peng, and H. Guo, "Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution," *Phys. Rev. A* **93**, 012310 (2016).

[235] D. Abdelkhalek, M. Syllwasschy, N. J. Cerf, J. Fiurášek, and R. Schnabel, "Efficient entanglement distillation without quantum memory," *Nature communications* **7**, 11720 (2016).

[236] M. Sabuncu, U. L. Andersen, and G. Leuchs, "Experimental demonstration of continuous variable cloning with phase-conjugate inputs," *Phys. Rev. Lett.* **98**, 170503 (2007).

[237] S. Olivares, M. G. Paris, and U. L. Andersen, "Cloning of Gaussian states by linear optics," *Phys. Rev. A* **73**, 062330 (2006).

[238] C. Weedbrook, N. B. Grosse, T. Symul, P. K. Lam, and T. C. Ralph, "Quantum cloning of continuous-variable entangled states," *Phys. Rev. A* **77**, 052313 (2008).

[239] S. Koike, H. Takahashi, H. Yonezawa, N. Takei, S. L. Braunstein, T. Aoki, and A. Furusawa, "Demonstration of quantum telecloning of optical coherent states," *Phys. Rev. Lett.* **96**, 060504 (2006).

[240] M. F. Sacchi, "Phase-covariant cloning of coherent states," *Phys. Rev. A* **75**, 042328 (2007).

[241] M. Sabuncu, G. Leuchs, and U. L. Andersen, "Experimental continuous-variable cloning of partial quantum information," *Phys. Rev. A* **78**, 052312 (2008).

[242] D. Qiu, "Combinations of probabilistic and approximate quantum cloning and deleting," *Phys. Rev. A* **65**, 052329 (2002).

[243] A. Shehu, "Quantum State Discrimination and Quantum Cloning: Optimization and Implementation," *CUNY Academic Works* (2015).

[244] F. Grosshans and N. J. Cerf, "Continuous-variable quantum cryptography is secure against non-Gaussian attacks," *Phys. Rev. Lett.* **92**, 047905 (2004).

[245] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Coherent-state quantum key distribution without random basis switching," *Phys. Rev. A* **73**, 022316 (2006).

[246] S. L. Braunstein, V. Bužek, and M. Hillery, "Quantum-information distributors: Quantum network for symmetric and asymmetric cloning in arbitrary dimension and continuous limit," *Phys. Rev. A* **63**, 052313 (2001).

[247] E. F. Galvao and L. Hardy, "Cloning and quantum computation," *Phys. Rev. A* **62**, 022301 (2000).

[248] E. Knill and R. Laflamme, "Power of one bit of quantum information," *Phys. Rev. Lett.* **81**, 5672 (1998).

[249] H. Ollivier and W. H. Zurek, "Quantum Discord: A Measure of the Quantumness of Correlations," *Phys. Rev. Lett.* **88**, 017901 (2001).

[250] A. Datta, A. Shaji, and C. M. Caves, "Quantum Discord and the Power of One Qubit," *Phys. Rev. Lett.* **100**, 050502 (2008).

[251] M. Gu, H. M. Chrzanowski, S. M. Assad, T. Symul, K. Modi, T. C. Ralph, V. Vedral, and P. K. Lam, "Observing the operational significance of discord consumption," *Nature Physics* **8**, 671 (2012).

[252] G. Adesso and A. Datta, "Quantum versus Classical Correlations in Gaussian States," *Phys. Rev. Lett.* **105**, 030501 (2010).

[253] P. Giorda and M. G. A. Paris, "Gaussian Quantum Discord," *Phys. Rev. Lett.* **105**, 020503 (2010).

[254] H. Ollivier and W. H. Zurek, "Quantum Discord: A Measure of the Quantumness of Correlations," *Phys. Rev. Lett.* **88**, 017901 (2001).

[255] U. Vogl, R. T. Glasser, Q. Glorieux, J. B. Clark, N. V. Corzo, and P. D. Lett, "Experimental characterization of Gaussian quantum discord generated by four-wave mixing," *Phys. Rev. A* **87** (2013).

[256] L. S. Madsen, A. Berni, M. Lassen, and U. L. Andersen, "Experimental Investigation of the Evolution of Gaussian Quantum Discord in an Open System," *Phys. Rev. Lett.* **109**, 030402 (2012).

[257] E. Prugovečki, "Information-theoretical aspects of quantum measurement," *International Journal of Theoretical Physics* **16**, 321 (1977).

[258] P. Busch, "Informationally complete sets of physical quantities," *International Journal of Theoretical Physics* **30**, 1217 (1991).

[259] S. Lloyd, "Enhanced Sensitivity of Photodetection via Quantum Illumination," *Science* **321**, 1463 (2008).

[260] S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, "Quantum illumination with Gaussian states," *Phys. Rev. Lett.* **101**, 253601 (2008).

[261] M. Sanz, U. Las Heras, J. García-Ripoll, E. Solano, and R. Di Candia, "Quantum estimation methods for quantum illumination," *Phys. Rev. Lett.* **118**, 070803 (2017).

[262] S. Guha and B. I. Erkmen, "Gaussian-state quantum-illumination receivers for target detection," *Phys. Rev. A* **80**, 052310 (2009).

[263] E. D. Lopaeva, I. Ruo Berchera, I. P. Degiovanni, S. Olivares, G. Brida, and M. Genovese, "Experimental Realization of Quantum Illumination," *Phys. Rev. Lett.* **110**, 153603 (2013).

[264] Z. Zhang, M. Tengner, T. Zhong, F. N. C. Wong, and J. H. Shapiro, "Entanglement's Benefit Survives an Entanglement-Breaking Channel," *Phys. Rev. Lett.* **111**, 010501 (2013).

[265] Z. Zhang, S. Mouradian, F. N. C. Wong, and J. H. Shapiro, "Entanglement-Enhanced Sensing in a Lossy and Noisy Environment," *Phys. Rev. Lett.* **114**, 110506 (2015).

[266] S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J. H. Shapiro, and S. Pirandola, "Microwave Quantum Illumination," *Phys. Rev. Lett.* **114**, 080503 (2015).

[267] J. H. Shapiro, "Defeating passive eavesdropping with quantum illumination," *Phys. Rev. A* **80**, 022320 (2009).

[268] E. Knill and R. Laflamme, "Power of One Bit of Quantum Information," *Phys. Rev. Lett.* **81**, 5672 (1998).

[269] B. P. Lanyon, M. Barbieri, M. P. Almeida, and A. G. White, "Experimental Quantum Computing without Entanglement," *Phys. Rev. Lett.* **101**, 200501 (2008).

[270] L. Henderson and V. Vedral, "Classical, quantum and total correlations," *Journal of Physics A: Mathematical and General* **34**, 6899 (2001).

[271] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, "The classical-quantum boundary for correlations: Discord and related measures," *Rev. Mod. Phys.* **84**, 1655 (2012).

[272] C. Weedbrook, S. Pirandola, J. Thompson, V. Vedral, and M. Gu, "How discord underlies the noise resilience of quantum illumination," *New Journal of Physics* **18**, 043027 (2016).

[273] S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, "Quantum Illumination with Gaussian States," *Phys. Rev. Lett.* **101**, 253601 (2008).

[274] C. A. Fuchs and C. M. Caves, "Ensemble-Dependent Bounds for Accessible Information in Quantum Mechanics," *Phys. Rev. Lett.* **73**, 3047 (1994).

[275] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A* , 10 (1997).

[276] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Transactions on Information Theory* **44**, 269 (1998).

[277] S. Pirandola, G. Spedalieri, S. L. Braunstein, N. J. Cerf, and S. Lloyd, "Optimality of Gaussian discord," *Phys. Rev. Lett.* **113**, 140405 (2014).

[278] M. Bradshaw, S. M. Assad, J. Y. Haw, S.-H. Tan, P. K. Lam, and M. Gu, "The overarching framework between Gaussian quantum discord and Gaussian quantum illumination," *Phys. Rev. A* **95**, 022333 (2017).

[279] S. Pirandola, G. Spedalieri, S. L. Braunstein, N. J. Cerf, and S. Lloyd, "Optimality of Gaussian Discord," *Phys. Rev. Lett.* **113**, 140405 (2014).

[280] Y. Huang, "Computing quantum discord is NP-complete," *New Journal of Physics* **16**, 033027 (2014).

[281] S. Ragy, I. R. Berchera, I. P. Degiovanni, S. Olivares, M. G. Paris, G. Adesso, and M. Genovese, "Quantifying the source of enhancement in experimental continuous variable quantum illumination," *JOSA B* **31**, 2045 (2014).

[282] A. Farace, A. De Pasquale, L. Rigovacca, and V. Giovannetti, "Discriminating strength: a bona fide measure of non-classical correlations," *New Journal of Physics* **16**, 073010 (2014).

[283] L. Rigovacca, A. Farace, A. De Pasquale, and V. Giovannetti, "Gaussian discriminating strength," *Phys. Rev. A* **92**, 042331 (2015).

[284] C. Invernizzi, M. G. Paris, and S. Pirandola, "Optimal detection of losses by thermal probes," *Phys. Rev. A* **84**, 022334 (2011).

[285] A. Datta, S. T. Flammia and C. M. Caves, *Entanglement and the power of one qubit*, Phys. Rev. A **72**, 042316 (2005).

[286] V. Madhok & A. Datta, *Interpreting quantum discord through quantum state merging*, Phys. Rev. A **83**, 032323 (2011).

[287] D. Cavalcanti, L. Aolita, S. Boixo, K. Modi, M. Piani and A. Winter, *Operational interpretations of quantum discord*, Phys. Rev. A **83**, 032324 (2011).

[288] R. Tatham, L. Mista, Jr., G. Adesso and N. Korolkova, *Nonclassical correlations in continuous-variable non-Gaussian Werner states*, Phys. Rev. A **85**, 022326 (2012).

[289] R. Rahimi & A. SaiToh, *Single-experiment-detectable nonclassical correlation witness*, Phys. Rev. A **82**, 022314 (2010).

[290] B. Bylicka & D. Chruściński, *Witnessing quantum discord in* $2 \times N$ *systems*, Phys. Rev. A **81**, 062102 (2010).

[291] B. Dakić, V. Vedral and C. Brukner, *Necessary and Sufficient Condition for Nonzero Quantum Discord*, Phys. Rev. Lett. **105**, 190502 (2010).

[292] L. Chen, E. Chitambar, K. Modi and G. Vacanti, *Detecting multipartite classical states and their resemblances*, Phys. Rev. A **83**, 020101(R) (2011).

[293] C. Zhang, S. Yu, Q. Chen, and C. H. Oh, *Detecting the quantum discord of an unknown state by a single observable*, Phys. Rev. A **84**, 032122 (2011).

[294] D. Girolami & G. Adesso, *Observable Measure of Bipartite Quantum Correlations*, Phys. Rev. Lett. **108**, 150403 (2012).

[295] J. Maziero & R. M. Serra, *Classicality Witness for two-qubit states*, Int. J. Quant. Inf. **10**, 1250028 (2012).

[296] R. Auccaise, J. Maziero, L. C. Céleri, D. O. Soares-Pinto, E. R. deAzevedo, T. J. Bonagamba, R. S. Sarthour, I. S. Oliveira, and R. M. Serra, *Experimentally Witnessing the Quantumness of Correlations*, Phys. Rev. Lett. **107**, 070501 (2011).

[297] G. Passante, O. Moussa, D. A. Trottier, and R. Laflamme, *Experimental detection of nonclassical correlations in mixed-state quantum computation*, Phys. Rev. A **84**, 044302 (2011).

[298] G. H. Aguilar, O. Jiménez Farías, J. Maziero, R. M. Serra, P. H. Souto Ribeiro, and S. P. Walborn, *Experimental Estimate of a Classicality Witness via a Single Measurement*, Phys. Rev. Lett. **108**, 063601 (2012).

[299] S. Rahimi-Keshari, C. M. Caves and T. C. Ralph, *Measurement-based method for verifying quantum discord*, Phys. Rev. A **87**, 012119 (2013).

[300] R. Blandino, M. G. Genoni, J. Etesse, M. Barbieri, M. G. A. Paris, P. Grangier and R. Tualle-Brouri, *Homodyne Estimation of Gaussian Quantum Discord*, Phys. Rev. Lett. **109**, 180402 (2012).

[301] A. Meda, S. Olivares, I. P. Degiovanni, G. Brida, M. Genovese and M. G. A. Paris, *Revealing interference by continuous variable discordant states*, Optics Letters **38**, 3099-3102 (2013).

[302] M. S. Kim, W. Son, V. Buzek, and P. L. Knight, *Entanglement by a beam splitter: Nonclassicality as a prerequisite for entanglement*, Phys. Rev. A **65**, 032323 (2002).

[303] W. Xiang-bin, *Theorem for the beam-splitter entangler*, Phys. Rev. A **66**, 024303 (2002).

[304] J. W. Wu, P. K. Lam, M. B. Gray, and H.-A. Bachor, *Optical homodyne tomography of information carrying laser beams*, Optics Express **3**, 154 (1998).