QUANTUM SOURCES AND DETECTORS FOR QUANTUM INFORMATION

Amr Reda Ali Kotb Hossameldin

Mansoura, Egypt

Bachelor of Science, University of Science and Technology - Zewail City, 2019

Master of Arts, University of Virginia, 2021

A Dissertation submitted to the Graduate Faculty

of the University of Virginia in Candidacy for the Degree of

Doctor of Philosophy

Department of Physics

University of Virginia

May 2025

Abstract

Quantum computing offers the potential to solve complex problems beyond the reach of classical systems, with applications in cryptography, optimization, and scientific simulation. Photonic continuous-variable (CV) quantum computing harnesses light's properties to enable scalable, fault-tolerant quantum computation. This dissertation contributes to this field through developing high performing optical parametric oscillators (OPOs) and photon-number-resolving detectors (PNRDs). These efforts improve the generation and detection of quantum states, providing practical tools for quantum information processing.

I built two triply resonant optical parametric oscillators—a nondegenerate design which demonstrated 6 dB gain and a degenerate one achieving 24 dB gain—demonstrating strong potential for record quantum squeezing as the squeezing record is 15dB. These OPOs are sources of two-mode squeezed states, entangled photon pairs, and CV cluster states, supporting measurement-based quantum computing (MBQC) and related applications. As for PNRDs, I significantly enhanced the photon number resolution of the superconducting transition edge sensor (TES) system in our lab, increasing it from 8 to 37 photons per channel, enabling the resolution of up to 100 photons setting a new record up from the previous record of 16. I also modeled segmented detectors using single avalanche photodiodes, offering additional design insights.

PNR detectors enable numerous applications, two of which I explore in this dissertation: a quantum random number generator which I experimentally demonstrated and Fock state interferometry, which I theoretically modeled including losses, validating its use for phase discrimination.

Together, the high-gain OPOs and refined TES bolster photonic CV quantum computing, by paving the way for cubic phase gate realization and by extension universal CV quantum computing.

Acknowledgments

Reaching this point where I am finally defending my PhD almost feels like a dream after all this time and effort. I am feelings many things, chief among which is grateful. I know I could not have done it alone.

First and foremost, I thank God for giving me the strength and patience to complete this degree, and for blessing me with such great people in my life.

I thank my mother and late father for their continuous support and sacrifice throughout their lives, I am forever grateful and can never pay you back.

I thank my advisor, Olivier Pfister, for teaching, supporting, and guiding me throughout the past six years. I have always found his ambition and optimism inspiring, which gave me hope when circumstances where not helping. I could not have asked for a better advisor.

I thank my colleagues in the research group, of which I must start by Miller Eaton. He taught me experimental fundamentals when I was first starting with no background and when he did not have to and was busy. He never got tired of answering my repeated questions and he included me in projects even though he could have done them without me. I learned a lot from him not just in science, but as a one of a kind human being. I'd like to thank Carlos Gonzalez for all the warm and fun conversations we had. I'd also like to thank Paul Renault and Leandre Brunel for all the Physics discussions we had. I'd like to thank Santiago Pinto and Andrew AbdelMalak for helping me move the lab. I'd also like to thank Alison Haskin, Xuan Zhu, Chun-Hung Chang, Rajveer Nehra and our latest group member Debaleena Majumder.

I'd like to thank my friends, they were a constant and reliable support during these years. I'd like to thank Mostafa Alkady, Hossam Almamdouh, Adrian Gutierrez,

Matthew Walker, Jawad Alalami, Mohammed Iskandarani, Abdullah Aljarba, Amgad Ashraf and Ahmed Azzam.

I would also like to thank Reem, my fiance, for supporting me through this past year. Finally, I'd like to thank Ahmed Asakra, my seventh grade Physics teacher, who inspired me with his passion to do the same and peruse a career in Physics.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Quantum computing, first proposed in 1982 by Richard Feynman [1], has undergone rapid development, with major technology companies and startups racing to construct practical quantum computers for real-world applications. The appeal of this technology lies in its potential to address previously intractable problems through what is termed the quantum advantage. This advantage arises from the unique quantum properties of the qubit, in contrast to the classical bit. A classical bit is restricted to a state of either 0 or 1, whereas a qubit can exist in a superposition of 0 and 1 states. This superposition enables a quantum computer to access a vast number of possibilities simultaneously, offering exponential computational power for specific problems [2]. Furthermore, qubits can be entangled, producing correlations that exceed classical bounds [3] and enable enhanced information processing across multiple qubits [2]. It is worth noting that having superposition and entanglement alone does not guarantee exponential speed up over classical computers. One needs to find the right quantum algorithm, which is in general not an easy task[4].

Several quantum algorithms have been developed that demonstrate exponential speedup over their classical counterparts. Notably, Shor's algorithm factors large integers exponentially faster than any known classical method, posing a threat to RSA encryption [5]. Additionally, quantum simulation algorithms, as envisioned by Feynman, provide exponential efficiency in modeling quantum systems [6]. These advancements underscore the transformative potential of quantum computing in fields such as cryp-

tography, optimization, and scientific simulation.

The early development of classical computers saw companies competing to perfect the physical realization of the bit—the transistor—through various technologies, until the metal-oxide-semiconductor field-effect transistor (MOSFET) emerged as the dominant standard due to its scalability and efficiency [7]. A similar competition exists today in quantum computing, with diverse physical implementations of the logical qubit, including superconducting qubits [8], trapped ions[9], neutral atoms[10], and photonics (light-based systems)[11]. The continuous-variable photonic approach stands out because, unlike discrete-variable qubits limited to 0, 1, or their superposition, it leverages the continuous quadratures of quantized electromagnetic fields—analogous to position and momentum—providing access to a continuous state space [12]. Here, the fundamental unit is the qumode, distinguishing continuous-variable (CV) quantum computing from its discrete-variable (DV) counterpart.

Quantum computing also varies by approach, with two primary paradigms: circuit-based and measurement-based quantum computing (MBQC). Circuit-based quantum computing applies quantum gates to a set of qubits, evolving their states through unitary operations until a final measurement yields the computational result [2]. In contrast, MBQC begins by preparing a highly entangled resource state, such as a cluster state, and performs adaptive single-qubit(or qumode) measurements to implement gate operations indirectly, a method well-suited to photonic systems due to their natural entanglement capabilities [13].

Universal computation, whether classical or quantum, requires a complete set of logical gates. In quantum computing, the Clifford gates (gates which transform Pauli operators to other Pauli operators, e.g., Hadamard, CNOT, phase gates) can perform all classical computations but offer no quantum speedup, as they are efficiently simulable classically per the Gottesman-Knill theorem [14]. Achieving a quantum advan-

tage necessitates non-Clifford gates, such as the T-gate [2]. In photonic CV quantum computing, this translates to requiring both Gaussian gates (gates that transform Gaussian wavefunctions to other Gaussian wavefunctions, e.g., squeezing, displacement, beamsplitters) and non-Gaussian gates (e.g., cubic phase gate), as Gaussian operations alone are classically simulable [15].

This dissertation focuses on the photonic, continuous-variable, measurement-based approach to quantum computing. Gaussian gates have been successfully realized with high fidelity using optical techniques [16, 17, 18]. However, the realization of non-Gaussian gates, particularly the cubic phase gate essential for universal CV quantum computing, remains a significant challenge. Proposals to implement the cubic phase gate include adaptive non-Gaussian measurements [19], photon subtraction techniques with sequential subtractions [20], and ancilla-assisted methods [21, 22], all of which benefit from high squeezing levels (e.g., 10 dB as demonstrated or proposed in some schemes) and/or require precise photon number resolution.

This work addresses these challenges through three main chapters:

In Chapter 2, I detail the design and construction of doubly and triply resonant optical parametric oscillators (OPOs), achieving measured gains of 24 dB and 6 dB, respectively — a necessary requirement for observing squeezing, with the current record being 15 dB of squeezing[23]. OPOs serve as critical sources of squeezed states [24], entangled photon pairs [25], and cluster states [26], underpinning numerous quantum optics experiments.

In Chapter 3, I explore photon-number-resolving detectors (PNRDs). I discuss my simulations of single avalanche photodiodes for PNR applications [27] and my group's work with transition-edge sensors (TES), where we resolved up to 100 photons[28], surpassing the previous world record of 16 [29]. This advancement enhances the precision of quantum measurements.

In Chapter 4, I present applications of PNRDs. Leveraging the TES's capabilities, we implemented a quantum random number generator[28]. Additionally, I demonstrate how PNRDs enable Fock state interferometry for phase discrimination with low error rates, even under realistic lossy conditions, advancing quantum metrology[30].

Chapter 2

Optical Parametric Oscillator (OPO)

An optical parametric oscillator (OPO) consists of an optical cavity with a non-linear medium inside. It has many use cases such as in spectroscopy [31], microscopy [32], and in quantum optics where it is used as a source of entangled photon pairs, squeezed states and cluster states. My goal here is to break the record of squeezing and my work has been a series of successful steps towards that. The current record in squeezing is 15 dB[23]. In this chapter I will discuss optical cavities, non-linear media, and the doubly and triply resonant OPOs I built achieving 24 dB and 6 dB of gain respectively, a necessary requirement for observing squeezing. The doubly resonant OPO is a type-0 OPO, which means the pump, signal and idler fields are all in the same polarization. This OPO can be used to generate single-mode squeezed states, which are a necessary ingredient for cat state generation, which in turn can be used to make GKP states (useful for error correction)[33]. The triply resonant OPO is a type-II OPO, which means the signal and idler fields are cross polarized. This can be used to generate two-mode squeezed states and separable (by polarization), entangled photon pairs. Two-mode squeezed states can be used to generate cubic phase states[22].

2.1 Optical cavity

An optical cavity, or optical resonator, consists of two (or more) mirrors with the purpose of trapping light between them allowing for the build up and constructive interference of light waves over multiple round trips producing resonant modes. There are multiple ways to go about building an optical cavity involving not just the number of mirrors used but also their radius of curvature and their separation distance. We are now going to discuss some essential cavity properties.

2.1.1 Stability

In this chapter, we are going to consider what is known as the hemispherical, near-hemispherical or half-concentric stable resonator, compromised of one concave mirror of radius of curvature $\mathcal{R}_1$ and one flat mirror of radius of curvature $\mathcal{R}_2 = \infty$ separated by a distance $L \approx \mathcal{R}_1$, also known as the cavity length. A schematic is shown in Fig. 2.1.

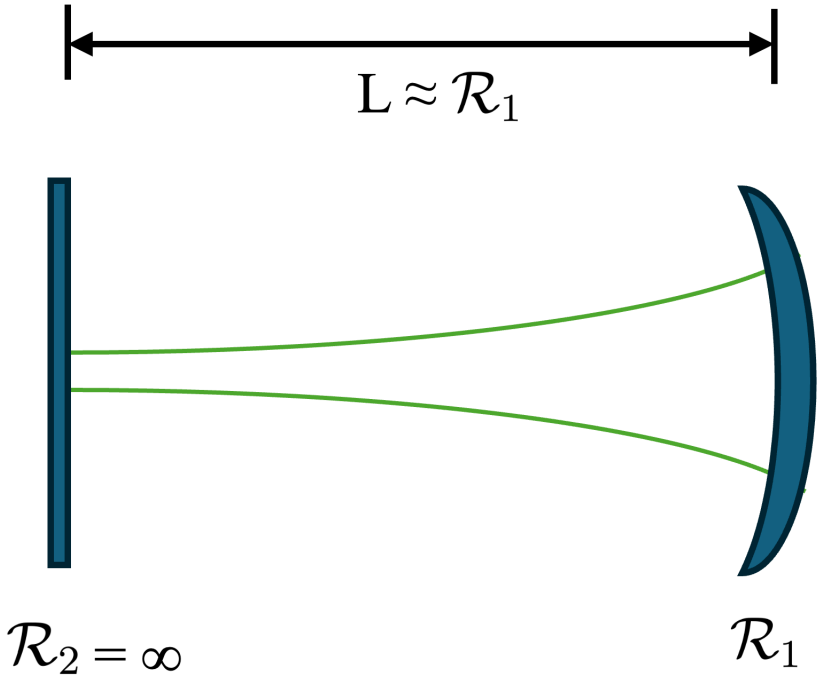


Figure 2.1: Hemispherical resonator schematic with $\mathcal{R}_1$ and $\mathcal{R}_2$ being the radius of curvature of mirror 1 and 2 respectively.

For this cavity to form a stable periodic focusing system, it must satisfy the following stability condition [34]:

$$0 \leq g_1 g_2 \leq 1 \tag{2.1}$$

where $g_1 = 1 + \frac{L}{\mathcal{R}_1}$, $g_2 = 1 + \frac{L}{\mathcal{R}_2}$ and the sign convention is that for a concave mirror R is negative. In our case, $\mathcal{R}_2 = \infty$, so this condition simplifies to:

$$0 \leq L \leq |\mathcal{R}_1| \tag{2.2}$$

The cavity we are using has $\mathcal{R}_1 = 0.1$ m.

The beam widths are approximated, with $\Delta L \ll L$ and $\mathcal{R}_1 = L + \Delta L$, as follows:

For the small spot at the plane mirror:

$$w_0^2 = w_2^2 \approx \frac{L\lambda}{\pi} \times \sqrt{\frac{\Delta L}{L}} \tag{2.3}$$

and for the large spot at the curved mirror:

$$w_1^2 \approx \frac{L\lambda}{\pi} \times \sqrt{\frac{L}{\Delta L}} \tag{2.4}$$

2.1.2 Fields

Let us now consider the reflected, circulating and transmitted electric fields for such a cavity as shown in Fig. 2.2 with electric field reflection and transmission coefficients r_1 and t_1 for mirror 1 and r_2 and t_2 for mirror 2.

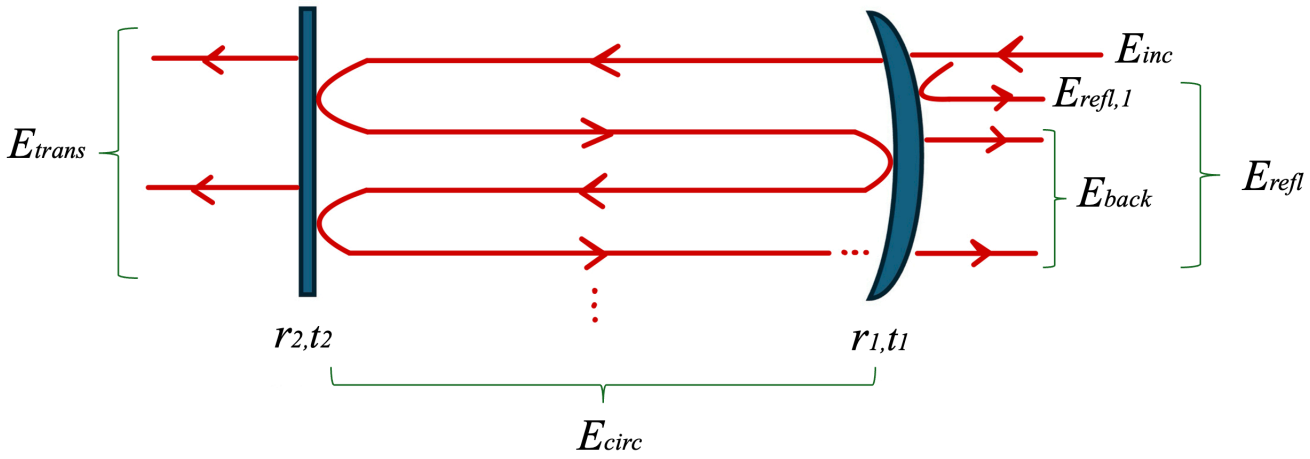


Figure 2.2: The electric fields associated with a two mirror cavity with electric field reflection and transmission coefficients r_1 and t_1 for mirror 1 and r_2 and t_2 for mirror 2.

For a lossless cavity, the the expression for the total circulating field is:

$$E_{circ} = \frac{it_1}{1 - r_1 r_2 e^{\frac{-i\omega 2L}{c}}} E_{inc} \tag{2.5}$$

for the reflected field:

$$E_{refl} = \frac{r_1 - r_2 e^{\frac{-i\omega 2L}{c}}}{1 - r_1 r_2 e^{\frac{-i\omega 2L}{c}}} E_{inc} \tag{2.6}$$

and for the transmitted field:

$$E_{trans} = \frac{-t_1 t_2 e^{\frac{-i\omega 2L}{c}}}{1 - r_1 r_2 e^{\frac{-i\omega 2L}{c}}} E_{inc} \tag{2.7}$$

The electric field reflection and transmission coefficients are related to the intensity reflectivities and transmissivities by:

$$|r_i|^2 = R_i, |t_i|^2 = T_i \tag{2.8}$$

where R_i+T_1=1 as we assume loss and scattering are negligible, as measured in previous experiments.

It is often more useful to have expressions relating the relative intensities of the circulating, reflected and transmitted fields to the incident field. Starting from $I \propto |E|^2$, we begin by the circulating field intensity relative to the incident field, this is given by:

$$A_{circ} = \frac{|E_{circ}|^2}{|E_{inc}|^2} = \frac{T_1}{(1 - \sqrt{R_1 R_2})^2 + 4\sqrt{R_1 R_2}\sin^2(\frac{\omega L}{c})} \tag{2.9}$$

for the reflected field intensity:

$$A_{refl} = \frac{|E_{refl}|^2}{|E_{inc}|^2} = \frac{(\sqrt{R_1} - \sqrt{R_2})^2 + 4\sqrt{R_1 R_2}\sin^2(\frac{\omega L}{c})}{(1 - \sqrt{R_1 R_2})^2 + 4\sqrt{R_1 R_2}\sin^2(\frac{\omega L}{c})} \tag{2.10}$$

and the transmitted field intensity:

$$A_{trans} = \frac{|E_{trans}|^2}{|E_{inc}|^2} = \frac{T_1 T_2}{(1 - \sqrt{R_1 R_2})^2 + 4\sqrt{R_1 R_2}\sin^2(\frac{\omega L}{c})} \tag{2.11}$$

The cavity we are using has mirrors with $R_1 = 0.9$ and $R_2 = 0.99998$ at 532 nm and $R_1 = 0.9999$ and $R_2 = 0.83$ at 1064 nm.

At resonance, the round-trip phase $\frac{\omega \times 2L}{c} = 2\pi$, which means $\frac{\omega L}{c} = \pi$ and the sin

term in the denominator vanishes. Using our mirror intensity reflectivities, we can calculate from Eq. 2.9 that $I_{circ} \approx 38 I_{inc}$ at 532 nm and $I_{circ} \approx 0.0126 I_{inc}$ at 1064 nm.

We are using an Nd:YAG laser, widely used in optical systems for its high power and stability, with a fundamental wavelength of 1064 nm. This is later doubled in frequency in a doubling cavity to output our 532 nm pump laser. Using 1064 nm light is also particularly useful since InGaAs photodiodes (used in balanced homodyne detectors to example to measure squeezing) have the highest quantum efficiency at 1064 nm.

2.1.3 Resonant cavity properties

Let us now define some useful parameters used to describe optical cavities. We begin by plotting Eq. 2.11 substituting ω with $2\pi\nu$. This generates Fig. 2.3 given below.

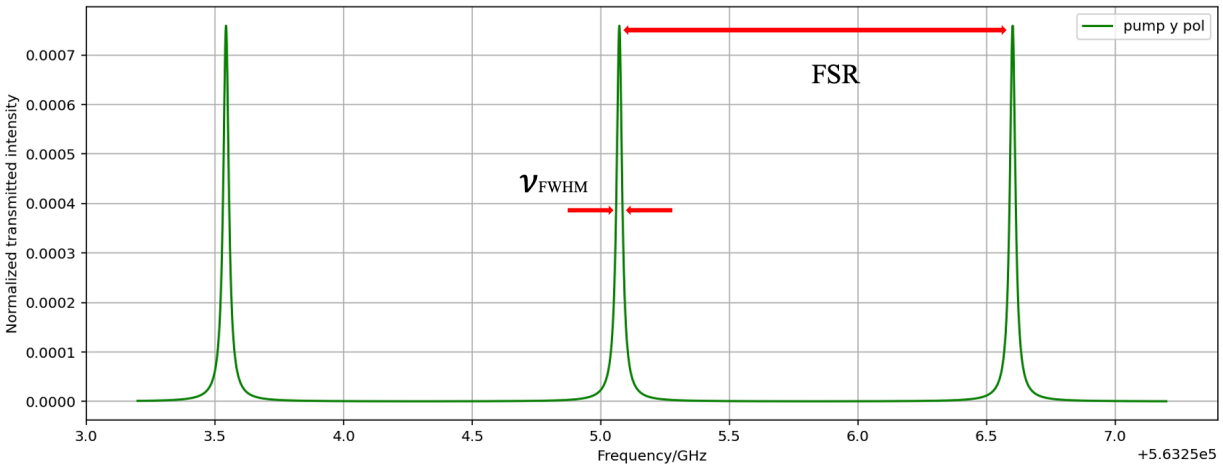


Figure 2.3: Transmitted resonant cavity modes for an optical cavity with $R_1 = 0.9$ and $R_2 = 0.99998$ at 532 nm.

Suppose our incident beam had a continuous frequency distribution, the transmitted output would still have the comb like structure of Fig. 2.3. The cavity acts as filter and only allows light with certain frequencies through, those satisfying the resonance

condition. The resonance condition is that the acquired phase after one round trip is exactly 2πq, where q in an integer. In terms of frequency, this is:

$$\nu_q = q\frac{c}{2L}, \quad q \text{ integer} \tag{2.12}$$

Eq. 2.12 gives the allowed frequencies through the optical cavity. We will use q to label these modes, also called longitudinal or axial modes. We can directly see that the mode spacing, also known as the cavity's free spectral range, is given by:

$$FSR = \frac{c}{2L} \tag{2.13}$$

Each of the comb lines in Fig. 2.3 has a distribution in frequency, also known as the linewidth or full width half maximum, labeled as ν_{FWHM}. To calculate that linewidth, we set A_{trans} given by Eq. 2.11 equal to $\frac{1}{2}A_{trans}^{max}$ which occurs at resonance, and solve for the argument of the sine, which is the phase after traversing one length L, so half a round trip. This gives us $\frac{\delta}{2}$ where δ is the phase after one round trip. Recall $\delta = \frac{\omega \times 2L}{c} = 2\pi$. Solving for δ we now have an expression for the phase at which the power is half the maximum. To get the linewidth we multiply that by 2. This is the linewidth expression in phase space:

$$\delta_{FWHM} = 4\sin^{-1}\left(\frac{1-\sqrt{R_1R_2}}{2(R_1R_2)^{\frac{1}{4}}}\right) \tag{2.14}$$

To get the ν_{FWHM} expression in frequency, we use $\delta = \frac{\omega 2L}{c}$ and substitute $2\pi\nu$ for ω then solve for ν. This gives us:

$$\nu_{FWHM} = \frac{c}{\pi L}\sin^{-1}\left(\frac{1-\sqrt{R_1R_2}}{2(R_1R_2)^{\frac{1}{4}}}\right) \tag{2.15}$$

Next, the finesse is defined as the ratio of FSR over ν_{FWHM}. This is given by:

$$Finesse = \frac{\pi}{2\sin^{-1}\left(\frac{1-\sqrt{R_1R_2}}{2(R_1R_2)^{\frac{1}{4}}}\right)} \tag{2.16}$$

which can be approximated using $\sin\delta \simeq \delta \simeq \sin^{-1}\delta$ to:

$$Finesse \approx \frac{\pi(R_1R_2)^{\frac{1}{4}}}{1-\sqrt{R_1R_2}} \tag{2.17}$$

For our cavity we have FSR ≈1.5 GHz, $\nu_{FWHM} \approx 25$ MHz at 532 nm and $\nu_{FWHM} \approx$ 45 MHz at 1064 nm. With finesse ≈ 60 at 532 nm and finesse ≈ 33 at 1064 nm.

A point of confusion that might arise is when scanning the length of an optical cavity and viewing the output on an oscilloscope when inputting 532 nm and 1064 nm lasers. What you will see is that the spacing between the IR (1064 nm) peaks is double that of the green (532 nm) peaks and one might ask how is their spacing different when the peak spacing we defined in Eq. 2.13 is independent of wavelength and should be the same for both. The answer is yes the spacing of resonant frequencies is the same whether you are in the IR or green regime. What we are viewing now on the oscilloscope is not in the frequency domain but in time as we're varying the cavity length. In that case we can rearrange Eq. 2.12 and use $\nu = c/\lambda$ to write:

$$L_q = q\frac{\lambda}{2}, \quad q \text{ integer} \tag{2.18}$$

where L_q are the cavity lengths that allow resonance. This means the spacing between possible cavity lengths is $\Delta L = \frac{\lambda}{2}$. If the cavity is scanned at a constant rate v_{scan}, the time between peaks (which is what you directly see on the oscilloscope) is given by:

$$\Delta t = \frac{\Delta L}{v_{scan}} = \frac{\lambda}{2v_{scan}} \tag{2.19}$$

For a constant v_{scan} we can see that $\Delta t_{IR} = \frac{1064\times10^{-9}}{2v_{scan}} = 2\times\frac{532\times10^{-9}}{2v_{scan}} = 2\Delta t_{green}$ which is what we observe.

Finally, we recall that the Gaussian beam is not the only solution to the paraxial Helmholtz equation defining a traveling wave with a slowly complex amplitude, but is the lowest order member of a family of solutions called the Hermite-Gaussian beams. These modes are characterized by two parameters, l and m, and are known as the transverse modes. The Gaussian beam is thus the TEM_{q00} mode. The optical cavity can also support these higher order modes. Odd modes (l+m odd) appear in the optical cavity when it is not well aligned, and even modes (l+m even) appear when the cavity is not well mode matched. The formula defining resonance frequencies of the Hermite-Gaussian modes is:

$$\nu_{l,m,q} = \left[q + (l+m+1)\frac{\Delta\zeta}{\pi}\right]\frac{c}{2L} \tag{2.20}$$

where $\Delta\zeta$ is known as the Gouy phase shift defined as:

$$\begin{aligned}\Delta\zeta &= \zeta(z_2) - \zeta(z_1) \\ &= \tan^{-1}(\frac{z_2}{z_0}) - \tan^{-1}(\frac{z_1}{z_0})\end{aligned} \tag{2.21}$$

For the purposes of making the calculation easier, let us set the origin of the z axis on the flat mirror in Fig. 2.1 and call it mirror 1 instead. In that case, $z_1 = 0$, $\mathcal{R}_1 = \infty$, $z_2 = \mathcal{R}_2 - \Delta d$ (with $\Delta d \ll \mathcal{R}_2$) and $\mathcal{R}_2 = -|\mathcal{R}_2|$ substituting all that back in Eq. 2.21 and using the definition $\mathcal{R} = z + \frac{z0^2}{z}$ we get $\Delta\zeta = \frac{\pi}{2}$ and Eq. 2.20 for the hemispherical cavity simplifies to:

$$\nu_{l,m,q} = \left[q + \frac{l+m+1}{2}\right]\frac{c}{2L} \tag{2.22}$$

Fig. 2.4 shows how the resonant modes are ordered for different types of cavities.

Our semi-concentric case is identical to the concentric case in terms of the shape of the Gaussian modes, and identical to the confocal case in terms of Gouy phase and the resultant stability condition, where the $g_1 g_2$ term in Eq. 2.1 is zero in both the hemispherical and confocal cases. We can see how the odd and even modes get separated at half the FSR. This is indeed what we observe with our cavity in the lab. When we align the input beam well, we can make the odd modes disappear.

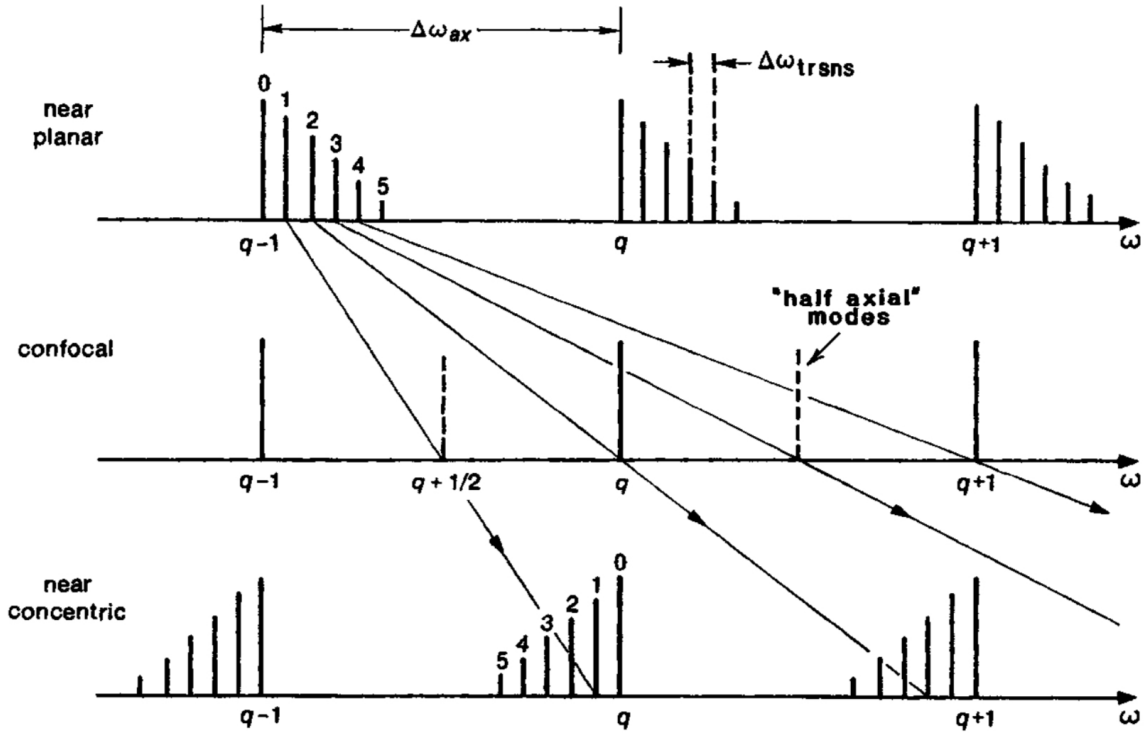


Figure 2.4: Figure from [35]. Transverse mode resonant frequencies in various stable cavities

2.2 Nonlinear media

Nonlinear media are media whose response to an applied optical field depends in a nonlinear way on the field. This allows different optical fields to interact with one another opening the door for numerous new phenomena that constitute the field of nonlinear optics. Among these phenomena, we will primarily be concerned here with parametric amplification and spontaneous parametric down conversion. There are many different materials that exhibit nonlinear behavior that can be leveraged for optical experiments, the material we chose for the two OPOs we built is a periodically poled Potassium Titanyl Phosphate ($KTiOPO_4$) crystal, also known as a PPKTP crystal. An excellent resource on nonlinear optics can be found in Ref. [36].

We begin by recalling that in a linear dielectric medium, the dipole moment per unit volume, or polarization, is given by:

$$\tilde{P}(t) = \epsilon_0 \chi^{(1)} \tilde{E}(t) \tag{2.23}$$

where ϵ_0 is the permittivity of free space, $\chi^{(1)}$ is the linear susceptibility of the medium and E(t) is the input electric field. In a nonlinear dielectric medium, Eq. 2.23 can be generalized to:

$$\begin{aligned} \tilde{P}(t) &= \epsilon_0[\chi^{(1)}\tilde{E}(t) + \chi^{(2)}\tilde{E}^2(t) + \chi^{(3)}\tilde{E}^3(t) + ...] \\ &= \tilde{P}^{(1)}(t) + \tilde{P}^{(2)}(t) + \tilde{P}^{(3)}(t) + ... \end{aligned} \tag{2.24}$$

where $\chi^{(2)}$ and $\chi^{(3)}$ are the second and third order nonlinear susceptibilities. In general $|\chi^{(1)}| \gg |\chi^{(2)}| \gg |\chi^{(3)}|$, so when considering second-order nonlinear effects, we can ignore third-order ones if the fields are not too intense.

Let us now look closer at second order interactions. Consider the case in which two

electric fields with angular frequencies ω_1 and ω_2 are input into a nonlinear material. The total electric field will be given by:

$$\tilde{E}(t) = E_1 e^{-i\omega_1 t} + E_2 e^{-i\omega_2 t} + c.c. \tag{2.25}$$

The second order polarization is then:

$$\begin{aligned} \tilde{P}^{(2)}(t) &= \epsilon_0 \chi^{(2)} E^2(t) \\ &= \epsilon_0 \chi^{(2)} \big[E_1^2 e^{-2i\omega_1 t} + E_2^2 e^{-2i\omega_2 t} + 2E_1 E_2 e^{-i(\omega_1+\omega_2)t} \\ &\quad + 2E_1 E_2^* e^{-i(\omega_1-\omega_2)t} + c.c. \big] + 2\epsilon_0 \chi^{(2)} [E_1 E_1^* + E_2 E_2^*] \end{aligned} \tag{2.26}$$

This can be expressed as:

$$\tilde{P}^{(2)}(t) = \sum_n P(\omega_n) e^{-i\omega_n t}, \tag{2.27}$$

where the summation covers positive and negative ω_n values. We can recognize the complex amplitudes $\mathrm{P}(\omega_n)$ corresponding to different frequency components (and processes) as:

$$\begin{aligned} P(2\omega_1) &= \epsilon_0 \chi^{(2)} E_1^2 \text{ (SHG)}, \\ P(2\omega_2) &= \epsilon_0 \chi^{(2)} E_2^2 \text{ (SHG)}, \\ P(\omega_1 + \omega_2) &= 2\epsilon_0 \chi^{(2)} E_1 E_2 \text{ (SFG)}, \\ P(\omega_1 - \omega_2) &= 2\epsilon_0 \chi^{(2)} E_1 E_2^* \text{ (DFG)}, \\ P(0) &= 2\epsilon_0 \chi^{(2)} (E_1 E_1^* + E_2 E_2^*) \text{ (OR)} \end{aligned} \tag{2.28}$$

where the underlying physical processes are: second harmonic generation (SHG), sum frequency generation (SFG), difference frequency generation (DFG) and optical rectification (OR).

2.2.1 Phase matching

Typically, the four frequency dependent components in Eq. 2.28 are not all simultaneously present with meaningful intensity because they require different phase matching conditions. One is thus able to select which process to favor by satisfying the corresponding phase matching conditions. To see what these are, let's consider the DFG term in Eq. 2.28, that is a function of the difference of the two input frequencies ω_1 and ω_2. Let us call the new output field ω_3. For energy to be conserved, the frequencies must satisfy the condition:

$$\omega_3 = \omega_1 - \omega_2 \tag{2.29}$$

and for momentum to be conserved, the wave vectors must satisfy:

$$\Delta k = k_3 + k_2 - k_1 = 0 \tag{2.30}$$

where $k_i = \frac{n_i \omega_i}{c}$. These are called the phase matching conditions and can be satisfied by tuning the crystal temperature and crystal orientation. That might still not be enough and you end up with $\Delta k \neq 0$, which we would like to avoid since the intensity of the produced field is proportional to $\text{sinc}^2(\frac{\Delta k l}{2})$ where l is the crystal length, as shown in Fig. 2.5 . In this case, we can resort to quasi phase matching. Quasi phase matching is achieved by designing the crystal in such a way to introduce a new term in the wave vector equation compensating for the mismatch. That is done by periodically poling a ferroelectric crystal because, when the polarization of a ferroelectric domain flips, the sign of $\chi^{(2)}$ flips as well, as shown in Fig. 2.6. This results in:

$$\Delta k_Q = k_3 + k_2 - k_1 - \frac{2\pi}{\Lambda} \tag{2.31}$$

where Λ is the poling period, which can be controlled to get $\Delta k_Q = 0$. The periodic polling introduces a square spatial wave, not just a sinusoidal one. The Fourier

series of the square wave has the fundamental component Λ, used here, and odd subharmonics of the wavelength which are normally weaker [37, 38, 39].

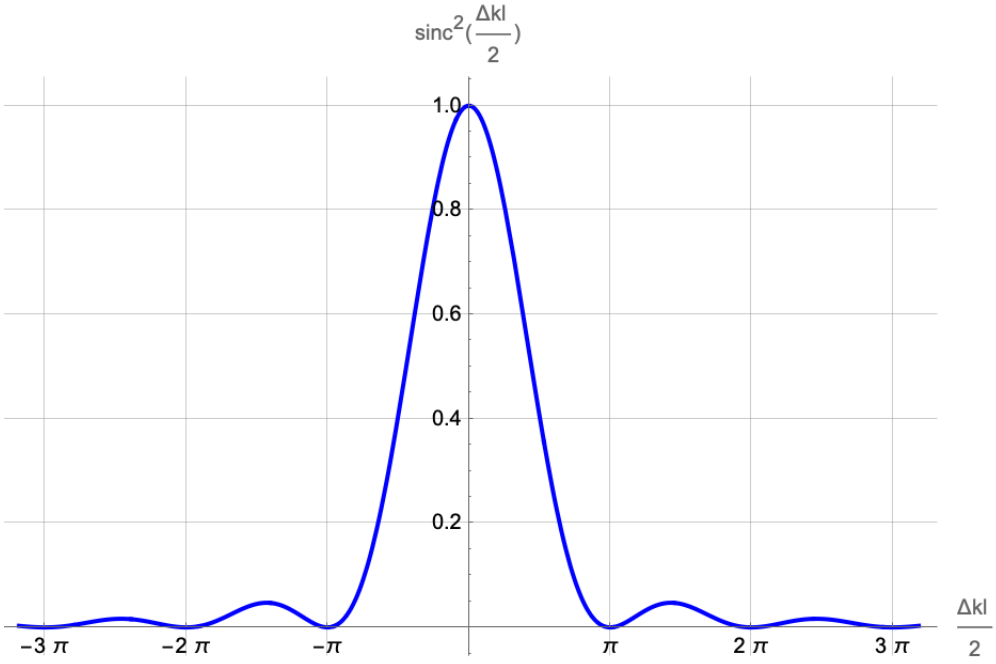


Figure 2.5: Effect of phase mismatch on efficiency

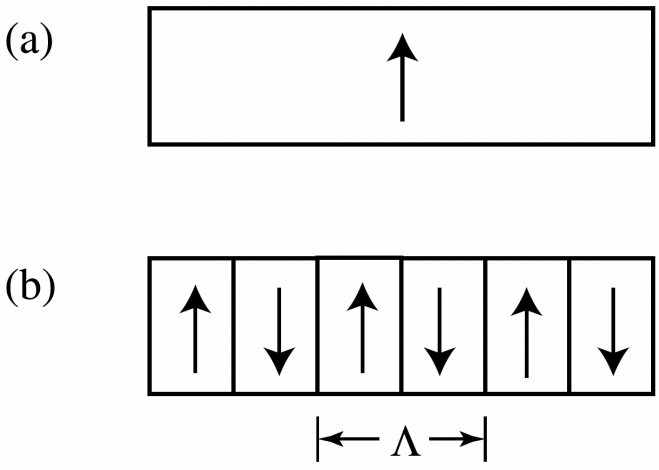


Figure 2.6: Figure from [36]. Schematic representations of a second-order nonlinear optical material in the form of (a) a homogeneous, monodomain single crystal and (b) a periodically poled material in which the positive c axis alternates in orientation with period Λ, flipping the sign of $\chi^{(2)}$.

As mentioned earlier, changing the crystal temperature can be used to achieve phase

matching. This is because each k_i in Eq. 2.30 and Eq. 2.31 depends on the refractive index n_i that the corresponding field experiences in the crystal. The index n, in turn, depends on the wavelength λ and the crystal temperature T. For KTP, the dependence is given by the Sellmeier equations for KTP[40, 41]:

$$\begin{aligned} n_y(\lambda, T) = & \sqrt{2.19229 + \frac{0.83547}{1 - \frac{0.04970}{(\lambda \times 10^6)^2}} - 0.01621(\lambda \times 10^6)^2} \\ & + \left(6.2897 + \frac{6.3061}{\lambda \times 10^6} - \frac{6.0629}{(\lambda \times 10^6)^2} + \frac{2.6486}{(\lambda \times 10^6)^3}\right) \times 10^{-6} \times (T - 25) \\ & + \left(-0.14445 + \frac{2.2244}{\lambda \times 10^6} - \frac{3.5770}{(\lambda \times 10^6)^2} + \frac{1.3470}{(\lambda \times 10^6)^3}\right) \times 10^{-8} \times (T - 25)^2 \end{aligned} \tag{2.32}$$

$$\begin{aligned} n_z(\lambda, T) = & \left[\left(2.12725 + \frac{1.18431(\lambda \times 10^6)^2}{(\lambda \times 10^6)^2 - 0.0514852}\right) + \right. \\ & \left. \left(\frac{0.6603(\lambda \times 10^6)^2}{(\lambda \times 10^6)^2 - 100.00507} - 0.00968956(\lambda \times 10^6)^2\right)\right]^{\frac{1}{2}} \\ & + \left(9.9587 + \frac{9.9228}{\lambda \times 10^6} - \frac{8.9603}{(\lambda \times 10^6)^2} + \frac{4.1010}{(\lambda \times 10^6)^3}\right) \times 10^{-6} \times (T - 25) \\ & + \left(-1.1882 + \frac{10.459}{\lambda \times 10^6} - \frac{9.8136}{(\lambda \times 10^6)^2} + \frac{3.1481}{(\lambda \times 10^6)^3}\right) \times 10^{-8} \times (T - 25)^2 \end{aligned} \tag{2.33}$$

where n_y and n_z represent polarizations along crystal axes, λ is the wavelength in meters and T is the temperature in degrees Celsius. These equations are useful to model how the crystal temperature affects resonant modes, as we will see in the following sections.

2.2.2 Parametric amplification

Let us now assume phase matching conditions are satisfied and let's take a closer look at the DFG process, outlined in Fig. 2.7. We notice that the higher frequency pump photon ω_1 down converts to both ω_2 (which we will call the signal) and ω_3 (which we will call the idler). From this we can expect that that the ω_2 field experiences amplification, which it does. This is called parametric amplification.

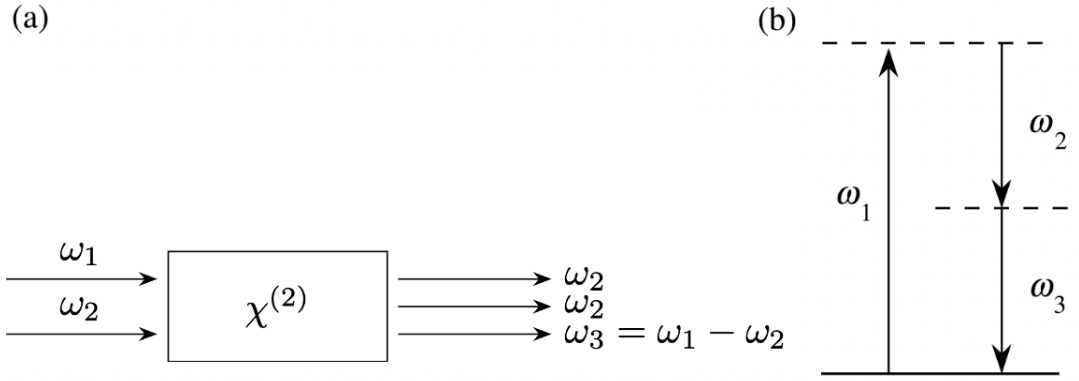


Figure 2.7: Difference-frequency generation. (a) Geometry of the interaction. (b) Energy-level description.

Solving the coupled wave equations derived from Maxwell equations using the DFG polarization term we get, for the degenerate $\omega_2 = \omega_3 = \omega$ case, a solution of the form:

$$E(z) = E_2(0)\cosh(\kappa z) + e^{i\phi}E_2^*(0)\sinh(\kappa z) \tag{2.34}$$

where $E_2(0)$ is the amplitude of the seed beam at z=0 of the crystal, ϕ is the pump phase relative to the seed, and $\kappa^2 = \frac{4d_{\text{eff}}^2\omega^4|E_1|^2}{k^2c^4}$ with $d_{\text{eff}} = \frac{1}{2}\chi^{(2)}$. To get the power of this output beam we calculate:

$$P = |E(z)|^2 = |E_2(0)|^2[\cosh(2\kappa z) + \sinh(2\kappa z)\cos\phi] \tag{2.35}$$

which for ϕ=0, set for maximum amplification, reduces to:

$$P = |E_2(0)|^2 e^{2\kappa z} \tag{2.36}$$

We define the gain as:

$$G = \frac{P_{\text{amplified}}}{P_{\text{input}}} = \frac{|E_2(l_{\text{eff}})|^2}{|E_2(0)|^2} = e^{2\kappa l_{\text{eff}}} \tag{2.37}$$

where l_{eff} is the effective length of the crystal the light sees. In case of single pass that is simply the length of the crystal l, in case of an optical cavity that would be $2n_{\text{rt}}l$ where n_{rt} is the effective number of round trips a light wave successfully makes in the cavity before exiting. It is common to make the substitution $r = \kappa z$ such that the gain is expressed as G=e^{2r} where r is called the squeezing parameter. It is also common to express the gain G in dB, which can be calculated as:

$$G_{dB} = 10\log_{10}(G) = 10\log_{10}(e^{2\kappa l_{\text{eff}}}) = \frac{40 l_{\text{eff}} d_{\text{eff}} \omega^2}{\ln(10) k c^2} |E_1| \tag{2.38}$$

where we can see that the gain in dB, G_{dB}, is proportional to the square root of the pump beam power since $|E_1| \propto \sqrt{P_1}$.

2.2.3 Spontaneous parametric down conversion

Spontaneous parametric down conversion (SPDC) is what happens when only the pump field ω_1 is sent into the the nonlinear medium, which then down converts outputting ω_2 and ω_3. This process cannot be described classically as the generated fields are the result of amplifying vacuum fluctuations in the ω_2 and ω_3 quantized fields[42]. Instead, this process can be described by the following Hamiltonian in the interaction picture:

$$H_I = i\hbar\chi^{(2)}(a_1 a_2^\dagger a_3^\dagger - a_1^\dagger a_2 a_3) \tag{2.39}$$

where a_1 is the pump field and $a_{2,3}$ are the signal and idler fields. In the undepleted pump approximation, which is valid when operating below the OPO threshold, we can treat the pump field as a classical field (coherent state) constant in time and rewrite the Hamiltonian as:

$$H_I = i\hbar\chi^{(2)}\beta(a_2^\dagger a_3^\dagger - a_2 a_3) \tag{2.40}$$

The evolution equations in the interaction picture for the creation and annihilation operators are:

$$\begin{aligned} \frac{da_2}{dt} &= \kappa a_3^\dagger \\ \frac{da_3}{dt} &= \kappa a_2^\dagger \end{aligned} \tag{2.41}$$

where κ here is defined as: $\kappa = \chi^{(2)}\beta$. Solving these equations we the get the Bogoliubov transformation:

$$\begin{aligned} a_2(t) &= a_2(0)\cosh r + a_3^\dagger(0)\sinh r \\ a_3(t) &= a_3(0)\cosh r + a_2^\dagger(0)\sinh r \end{aligned} \tag{2.42}$$

which defines the two mode squeezed state. Here $r = |\kappa|t$ is the squeezing parameter and t is the nonlinear interaction time.

For the degenerate $\omega_2 = \omega_3$ case the Hamiltonian becomes:

$$H_I = i\hbar\frac{\chi^{(2)}}{2}\beta[(a^\dagger)^2 - a^2] \tag{2.43}$$

where the factor $1/2$ comes to account for over-counting. The corresponding evolution

of the operator becomes:

$$a(t) = a(0)\cosh r + a^{\dagger}(0)\sinh r \tag{2.44}$$

which is the single mode squeezed state.

2.2.4 Squeezing

In this subsection I briefly explain what is meant by squeezing. I will use definitions from quantum optics that I will not fully flush out here can be easily found in any quantum optics book [43, 44].

To see what is meant by squeezing, let us first recall that the quadrature operators for a quantized field are defined as:

$$\hat{Q} = \frac{\hat{a}^{\dagger} + \hat{a}}{\sqrt{2}} \tag{2.45}$$

$$\hat{P} = \frac{\hat{a} - \hat{a}^{\dagger}}{i\sqrt{2}} \tag{2.46}$$

And let us replace the creation and annihilation operators in the quadratures by those defined in Eq. 2.44. We get:

$$\hat{Q}_s = e^{r}\hat{Q} \tag{2.47}$$

$$\hat{P}_s = e^{-r}\hat{P} \tag{2.48}$$

where r is the squeezing parameter defined in the previous section. We can see that for a positive r, $\hat{Q}$ gets 'stretched', or anti-squeezed and $\hat{P}$ gets squeezed.

Consider the simplest state, a vacuum state $|0\rangle$ in the Fock basis. The uncertainty is calculated using the quadratures in Eq. 2.45 to be $\Delta\hat{Q} = \sqrt{\langle 0|\,\hat{Q}^2\,|0\rangle - \langle 0|\,\hat{Q}\,|0\rangle^2} = \frac{1}{\sqrt{2}}$. Similarly, $\Delta\hat{P} = \frac{1}{\sqrt{2}}$ and the vacuum state saturates the Heisenberg uncertainty

relation: $\Delta\hat{Q}\Delta\hat{P} = \frac{1}{2}$.

If instead we use the squeezed and anti-squeezed quadratures defined in Eq. 2.47, we get $\Delta\hat{Q}_s = \frac{e^r}{\sqrt{2}}$ and $\Delta\hat{P}_s = \frac{e^{-r}}{\sqrt{2}}$. We see that we still saturate the Heisenberg uncertainty relation: $\Delta\hat{Q}_s\Delta\hat{P}_s = \frac{1}{2}$ but the uncertainties are no longer equal and the state is no longer symmetric.

This squeezing effect can be seen visually if we look at the Wigner function of the squeezed state in question. The Wigner function is a quasi-probability distribution that is in general defined by:

$$W(q,p) = \int_{-\infty}^{\infty} e^{2ipy} \langle q-y| \rho |q+y\rangle_q \, dy \tag{2.49}$$

for a density matrix ρ representing a quantum state. Here, $|s\rangle_q$ and $|t\rangle_p$ are eigenstates of the quadrature operators $\hat{Q}$ and $\hat{P}$ with eigenvalues s and t respectively. For the vacuum state $\rho = |0\rangle\langle 0|$, but this is in the Fock basis. We need to rewrite it in the quadrature basis to use in the Wigner function. In general, the Fock states written in the quadrature basis are given by:

$$|n\rangle = \int dx \frac{\pi^{-1/4}}{\sqrt{n!2^n}} e^{-x^2/2} H_n(x) |x\rangle_q \tag{2.50}$$

where $H_n(x)$ are the physicist's Hermite polynomials. With this we can find and plot the Wigner function for the vacuum state. But what about the squeezed vacuum?

For that we start by defining the squeezing operator and acting with it on the vacuum state. The squeezing operator is a unitary operator and thus takes the form $\hat{U} = e^{-\frac{it}{\hbar}\hat{H}}$. The Hamiltonians we'll use here are none other than those responsible for SPDC that we saw in the previous subsection defined by Eq. 2.40 for the two-mode case and Eq. 2.43 for the single-mode case. We evaluate the squeezing operators are

follows:

$$\hat{S}(r) = e^{\frac{r}{2}[(\hat{a}^\dagger)^2 - \hat{a}^2]} = e^{\frac{-ir}{2}(\hat{Q}\hat{P} + \hat{P}\hat{Q})} \tag{2.51}$$

$$\hat{S}_{ab}(r) = e^{r(\hat{a}^\dagger \hat{b}^\dagger - \hat{a}\hat{b})} = e^{-ir(\hat{Q}_a \hat{P}_b + \hat{P}_a \hat{Q}_b)} \tag{2.52}$$

where $r = \kappa\chi^{(2)}\beta$ is the squeezing parameter as defined in the previous subsection.

Acting by the single-mode squeezing operator on the vacuum state $|0\rangle$ we get:

$$\hat{S}(r)\,|0\rangle = e^{-\frac{r}{2}}\pi^{-1/4}\int ds\; e^{-\frac{e^{-2r}s^2}{2}}\,|s\rangle_q \tag{2.53}$$

which we can use in the Wigner function formula. We now have everything we need to plot the Wigner functions of vacuum and squeezed vacuum. The plots are shown in Fig. 2.8.

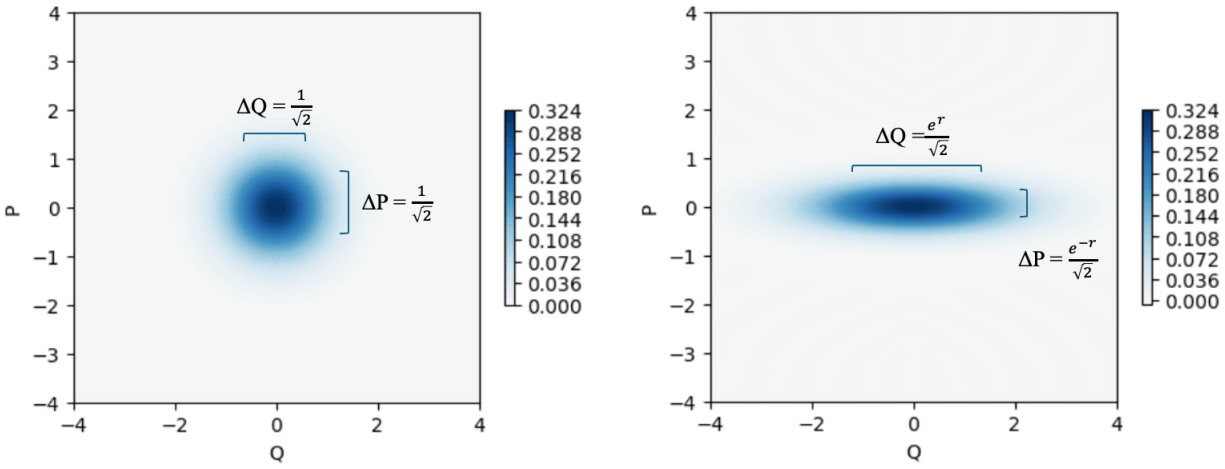
Written in Fock basis, the single-mode squeezed vacuum state is given by:

$$\hat{S}(r)\,|0\rangle = \frac{1}{\sqrt{\cosh(r)}}\sum_{n=0}^{\infty}\tanh^n r\,\frac{\sqrt{(2n)!}}{2^n n!}\,|2n\rangle \tag{2.54}$$

which shows how we will only have even numbered photons coming out of this process. This makes sense as the SPDC process explained earlier emits in photon pairs. The two-mode squeezed vacuum is given by:

$$\hat{S}_{ab}(r)\,|0\rangle_a\,|0\rangle_b = \frac{1}{\cosh(r)}\sum_{n=0}^{\infty}\tanh^n r\,|n\rangle_a\,|n\rangle_b \tag{2.55}$$

where the photons are still emitted in pairs, only in two separate modes this time.



(a) Vacuum state (b) 6 dB squeezed vacuum

Figure 2.8: Wigner functions of vacuum and 6 dB squeezed vacuum.

2.3 Optical parametric oscillator

2.3.1 Properties

Stability

With the components now covered, we are now ready to build our optical parametric oscillator by inserting our PPKTP crystal into the optical cavity as shown in Fig. 2.9.

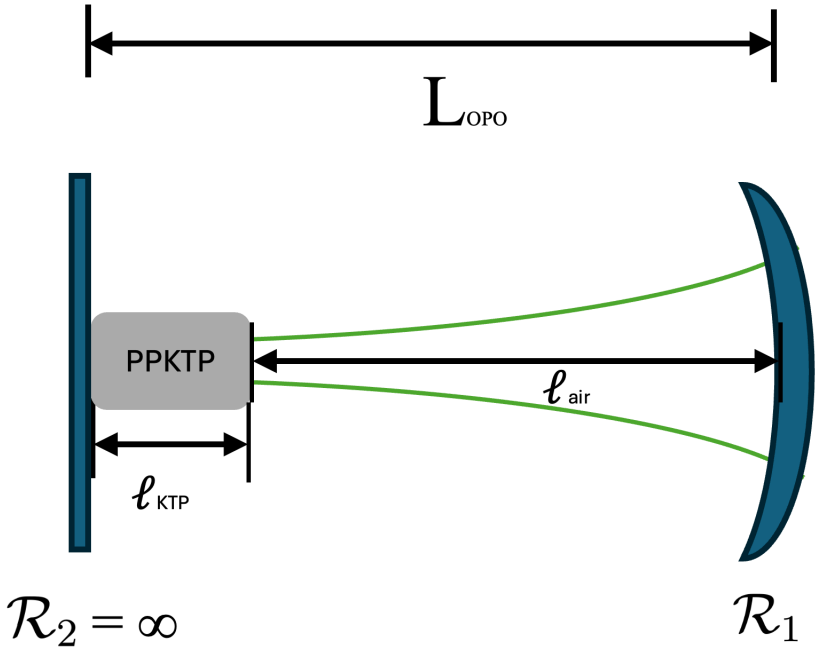


Figure 2.9: Optical parametric oscillator schematic

First, we want to get a sense of L_{OPO}, will it remain $\approx \mathcal{R}_1$ as in the case of the empty cavity? To calculate that, we resort to ray transfer matrices. Recall that the ray transfer matrix for reflecting off a mirror with radius of curvature $\mathcal{R}$ is

$$M_{refl} = \begin{pmatrix} 1 & 0 \\ \frac{2}{\mathcal{R}} & 1 \end{pmatrix}, \tag{2.56}$$

for propagating a distance ℓ through a medium with refractive index n is

$$M_{prop} = \begin{pmatrix} 1 & \frac{\ell}{n} \\ 0 & 1 \end{pmatrix}, \tag{2.57}$$

and for refracting from a medium with refractive index n_1 into a medium with index n_2 is:

$$M_{refr} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{n_1}{n_2} \end{pmatrix}. \tag{2.58}$$

The total matrix for one round trip, starting from the flat mirror, can be written as:

$$\begin{aligned} M_{rt} =& M_{relf}(\infty).M_{refr}(n_{KTP}, n_{air}).M_{prop}(\ell_{KTP}).M_{refr}(n_{air}, n_{KTP}).M_{prop}(\ell_{air}) \\ & .M_{relf}(\mathcal{R}_1).M_{prop}(\ell_{air}).M_{refr}(n_{KTP}, n_{air}).M_{prop}(\ell_{KTP}).M_{refr}(n_{air}, n_{KTP}) \end{aligned} \tag{2.59}$$

which is to be read from right to left. The crystal length $\ell_{KTP} = 0.01$ m, $\mathcal{R}_1 = -0.1$ m, $n_{air} = 1$ and n_{KTP} is given by Eqs. 2.32 and 2.33 depending on the crystal principal axis in question. For λ= 1064 nm we have $n_y \approx 1.74$ and $n_z \approx 1.83$. Evaluating the matrix elements of the 2×2 matrix M_{rt}, we have the following stability condition on its elements [34]: $\frac{1}{2}|A + D| \leq 1$. Where A is the element in the first row and first column and D is the element in the second row and second column. Solving for ℓ_{air} in the equality case in the stability condition to get the smallest possible waist, we

find $\ell_{air} \approx 0.0970$ m. This gives $L_{OPO} \leq 0.107$ m which is larger than that of the empty cavity case.

Resonance properties

We are now ready to recalculate the FSR, ν_{FWHM} and finesse of our OPO taking into account the PPKTP crystal inside. For the Z polarization we have:

$$FSR = \frac{c}{2(\ell_{air} + n_z \ell_{KTP})} \tag{2.60}$$

where we substituted L in Eq. 2.13 with $\ell_{air} + n_z \ell_{KTP}$ to account for the change in the optical path length. We do the same for Eq. 2.15 to get the ν_{FWHM}. We note that the finesse stays the same as it's defined as their ratio of FSR to ν_{FWHM} and thus the updated length term cancels out. We now have, for Z polarized 1064 nm, FSR$\approx$ 1.33 GHz and $\nu_{FWHM} \approx 39$ MHz. And for Z polarized 532 nm, FSR $\approx$ 1.32 GHz and $\nu_{FWHM} \approx 22$ MHz. Both the FSR and ν_{FWHM} are smaller than that of an empty cavity.

Threshold

Next, we want to get an idea of the OPO pump threshold power, which is how much pump power is needed such that round-trip gain of the fields equals round trip loss. The loss here is primarily caused by light escaping from the mirrors since they have non-zero transmissivity. As we saw earlier, the gain (in dB) is proportional to $\sqrt{P_{pump}}$, so to get the most gain, we would want as much pump power as we can get. On the other hand, if we operate above the OPO threshold it starts to lase and that might hurt the crystal, and it would also not give more gain than what is achieved at threshold. This is why we operate the OPO right below threshold. To

calculate this threshold for a triply resonant (pump, signal and idler) OPO, we follow the calculation in [45], in particular their Eq.(33) in chapter 24. I have to note that they have an error in defining their ξ and that instead it should be:

$$\xi_{corrected} = \chi^{(2)} \sqrt{\frac{2\hbar\omega_0\omega_1\omega_2}{\epsilon_0 c^3 n_0 n_1 n_2}} \tag{2.61}$$

where they label the pump field by 0.

We then get the following formula for the input threshold intensity of the pump beam:

$$I_{threshold} = \frac{n_1 n_2 n_3 \epsilon_0 c \lambda_2 \lambda_3}{128(2\pi)^2 |d|^2 l_{KTP}^2} T_1 T_2 T_3 \tag{2.62}$$

where T_1, T_2 and T_3 are the transmissivities of the mirrors for the pump, signal and idler respectively. Here we set T_1=0.1 which is the transmissivity of mirror 1 at 532 nm and $T_2 = T_3 = 0.17$ which is the transmissivity of mirror 2 at 1064 nm. We pick the bigger transmissivity of both mirrors for each field since that is used to account for losses. For reference, if both mirrors for each field had the same transmissivity the threshold intensity would roughly double as the losses are now doubled. Here d accounts for the second order nonlinear susceptibility since $d = \frac{\chi^{(2)}}{2}$. In Eq. 2.62 we will use a d_{eff} in place of d since we're working with a periodically polled non-linear crystal given by $d_{eff} = \frac{2}{\pi} d$. For a KTP crystal, d_{ZZZ}=15.4 pm/V and d_{YZY}=3.75 pm/V where the labels indicate the polarization of the pump, signal and idler fields respectively in the second order nonlinear process under investigation [46, 47].

To calculate the pump threshold power, recall that the total power in a Gaussian beam is $P = \frac{1}{2}\pi w_0^2 I_0$ where w_0 is the beam radius. The threshold power is thus:

$$P_{threshold} = \frac{1}{2}\pi w_1^2 I_{threshold} \tag{2.63}$$

where w_1 is the pump beam radius incident on the OPO at mirror 1. We calculate that

radius (width) assuming it perfectly mode-matches our OPO. We start by imposing the condition that the q(z) parameter, defined from $\frac{1}{q(z)} = \frac{1}{\mathcal{R}(z)} - \frac{i\lambda}{\pi W^2(z)}$ of the pump beam equals itself after one roundtrip in the OPO, where the roundtrip is defined by Eq. 2.59. Solving for the width w_1 at mirror 1 we get $w_1 \approx 330$ μm in the ZZZ case and $w_1 \approx 350$ μm in the YZY case. We give specific threshold calculation results in the next section for the different OPO configurations that we present there.

Expected gain at threshold

At threshold pump power, round trip gain = round trip loss. This can be expressed, following [48] Ch 9 Eq. (52), as:

$$\left(\frac{\kappa}{2}\right)^2 (2l)^2 \approx T^2 \tag{2.64}$$

where we replaced Γ in [48] by $\frac{\kappa}{2}$, l by $2l$ since the pump is also resonant in our case and we get gain by going through the crystal twice in each round trip, and a by T since light leaking from the mirror is the only source of losses in our case. Here T is for the idler and pump fields and has a value of 0.17. From Eq. 2.64 we get $\kappa l \approx T$. Substituting that in Eq. 2.38, with $n_{rt} \sim \frac{1}{T} \sim 6$, we get $G_{dB} \sim 17.7$ dB as the maximum gain, at threshold, for OPO's with our particular value of T.

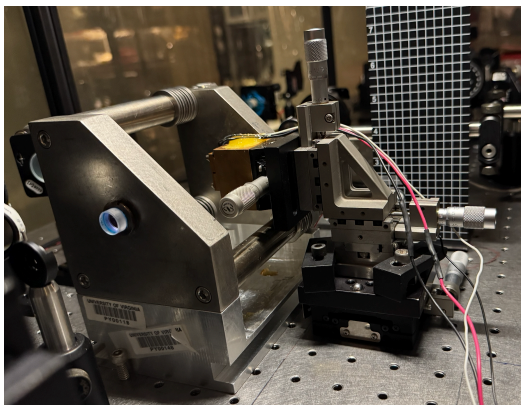
Hardware

The OPO hardware, shown in Fig. 2.10, is made from super invar to bring thermal expansion to a minimum. The knobs on the back plate are threaded such that 40 turns move the whole plate an inch, and 1 turn moves the plate 0.0635 cm. The back plate houses mirror 2, which is mounted on a piezo to enable us to scan the cavity length. The PPKTP crystal in housed in an oven that is used to control the crystal tempera-

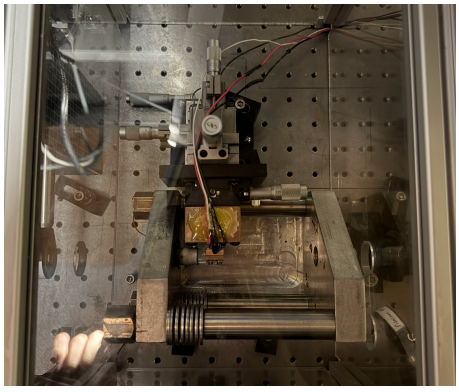
ture via an in-house made temperature controller. Inside the oven is a YSI Precision thermistor of model number 44032 with the following specs: $R_0 = 30\times10^3\Omega, \beta = 3810$ K and $T_0 = 298.15$. The resistance of the thermistor at a temperature T is given by: $R_T = R_0 e^{\beta(\frac{1}{T}-\frac{1}{T_0})}$. The thermistor is connected to temperature controller that outputs a monitor signal in Volts that tells the temperature up to 4 decimal places. To convert the output voltage V to temperature in degrees Celsius we use Eq. 2.65 which we get by using $V = IR_T$ with I=100 μA and solving for T, then subtracting 273.15 to convert from Kelvin to Celsius.

$$T(V) = \frac{1}{\frac{1}{3810}\ln(\frac{V}{3}) + \frac{1}{298.15}} - 273.15 \tag{2.65}$$

The oven with the crystal inside is mounted onto a configuration with a 3D stand and two goniometers to control translations in x, y and z as well as tilts about the y and z axes. For reference, the crystal axes are defined such that the crystal length is along the x-axis, the horizontal direction (width) is the y-axis and the vertical direction (height) is the z-axis as viewed from the entrance of the OPO. The whole OPO is covered by a Plexiglas box to reduce phase fluctuations due to air currents and temperature fluctuations, thus enhancing stability.



(a) OPO side view



(b) OPO top view

Figure 2.10: Optical parametric oscillator hardware

2.3.2 Triply resonant, type-II OPO

A type-II OPO is an OPO where the signal and idler are orthogonal to each other in polarization. A triply resonant OPO is an OPO where all three distinct pump, signal and idler fields are resonant simultaneously in the cavity. We can use such an OPO as a source of two-mode squeezed states and to create a single photon source in heralding experiments. This leverages the fact that the signal and idler are cross polarized and can be easily separated on a polarizing beam splitter. For this OPO we use a 10 mm long X-cut, Z-poled periodically poled $KTiPO_4$ (PPKTP) crystal, poled with a period of 465 μm to phasematch the YZY interaction. The threshold pump power of this setup calculated from Eq. 2.63 is $P_{\text{threshold}} = 3.3$ W.

Finding triple resonance was tricky and is in general not easy. To verify that it is possible to find in our cavity, we employ a Python code to simulate the fields' behavior. The results are shown in Fig. 2.11 and they show that it is indeed possible to find a crystal temperature and laser frequency combination that supports triple resonance in the cavity.

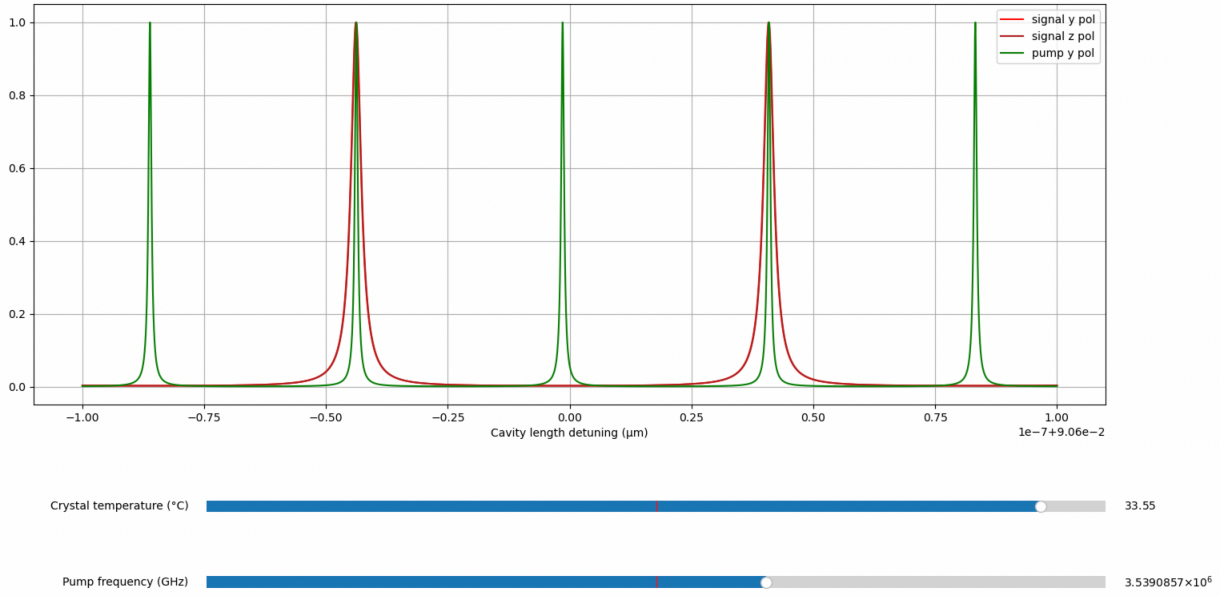


Figure 2.11: Triple resonance simulation

The cavity length L_{OPO}, crystal temperature and laser frequency were all scanned to find the parameter combination producing the largest gain. L_{OPO} was slightly less than the stability limit of the OPO, to get smallest waist in the crystal and thus the highest pump intensity. The crystal temperature and laser frequency were varied to get the best overlap between the pump and seed beams while still within the crystal's phasematching bandwidth, which means getting all three fields resonant simultaneously at the same cavity length to amplify and build up, achieving the best possible gain.

Parametric gain was measured by a setup such as that outlined in Fig. 2.12. The half wave plates (HWP) on each beam are used to control input beam's polarization, the dichroic mirror used transmit 99% at 532 nm while being highly reflective at 1064 nm and is used to combine the IR and green beams going into the OPO. The prism is used to separate the green and IR beams while the polarizing beamsplitter (PBS) is used to separate the two IR polarizations. Recall from Eq. 2.37 that gain is defined as the ratio of amplified power over non-amplified power. To measure gain, we thus measure the ratio of the IR transmission peak height in the amplification case with the pump on, to the IR peak height with the pump blocked. This is done while scanning the cavity length and pump phase. The cavity length is scanned by the back OPO mirror which is mounted on a piezo-as mentioned earlier. The pump phase is also scanned by a mirror mounted on a piezo which directs the input pump into the OPO.

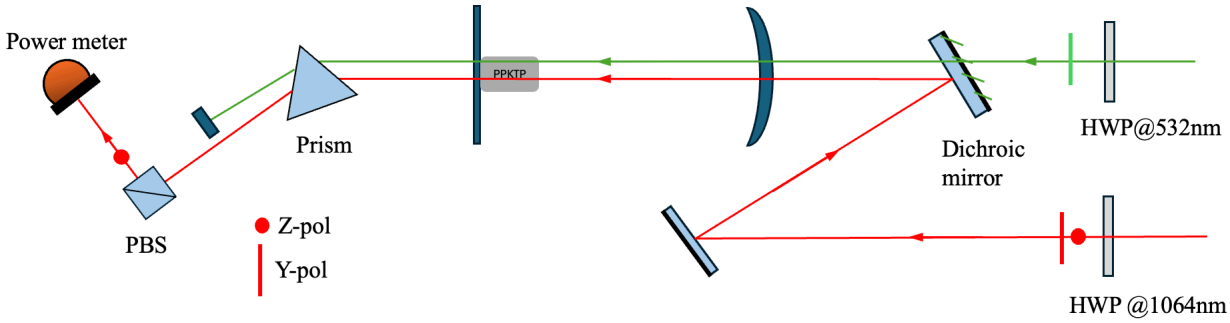


Figure 2.12: Parametric gain experimental setup for YZY interaction.

At pump power = 231 mW and crystal temperature = 33.2932°C, we were able to measure ≈ 6 dB of gain. This was calculated using the amplified IR peak value: 1.6875 V and no pump peak value: 420 mV as measured by the power meter and viewed on the oscilloscope.

2.3.3 Doubly resonant, type-0 OPO

A type-0 OPO is an OPO where the polarization of the pump, signal and idler are all the same. A doubly resonant OPO can be understood to be when the pump and signal are resonant at the same time or when the signal and idler are resonant at the same time. In this case, however, the signal and idler are the same field, Z-polarized IR, and they are resonant at the same time as the pump. We can also call this a triply resonant, degenerate OPO. For this OPO, we use a 10 mm long X-cut, Z-poled periodically poled $KTiPO_4$ (PPKTP) crystal, poled with a period of 9μm to phasematch the ZZZ interaction. The ZZZ interaction typically has a larger d_{eff} than the YZY and can therefore generate higher gain and squeezing. This might be useful in generating highly squeezed states for uses in cluster states. The threshold pump power of this setup calculated from Eq. 2.63 is $P_{\text{threshold}} = 194$ mW. We were able to experimentally observe OPO lasing at a threshold power of ~ 150 mW.

Parametric gain was measured by a setup such as that outlined in Fig. 2.13. The last

two dichroic mirrors are used to filter out the green (pump) beam, so that only the IR is measured on the power meter. Again, this is done while scanning the cavity length and pump phase as explained in the previous subsection. Results are shown in Fig 2.14. We can see that we measured $\approx$ 24 dB of gain while we expected $\sim$ 18 dB as explained in subsection 2.3.1. It is possible that some other phenomena is occurring as well as parametric amplification to cause the observed gain. We would need to do a squeezing measurement to confirm.

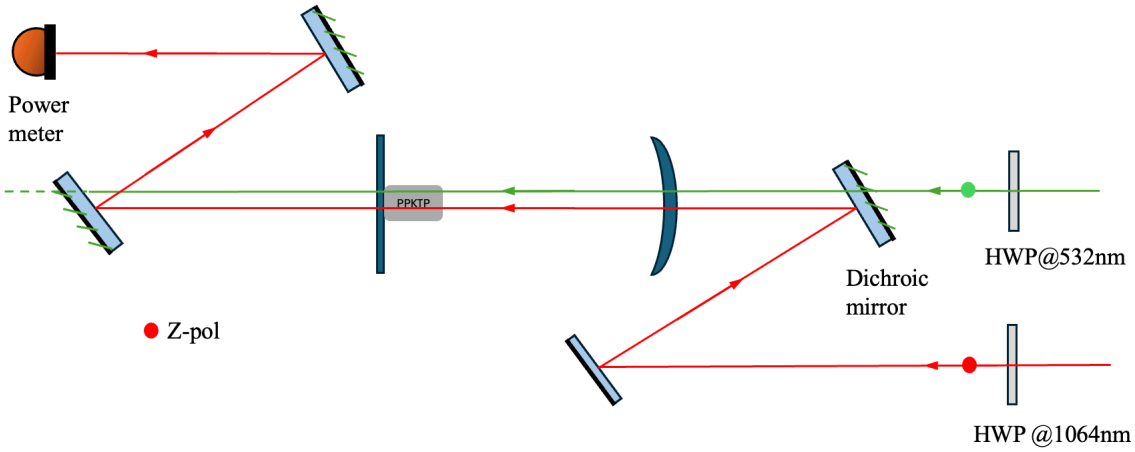


Figure 2.13: Parametric gain experimental setup for ZZZ interaction.

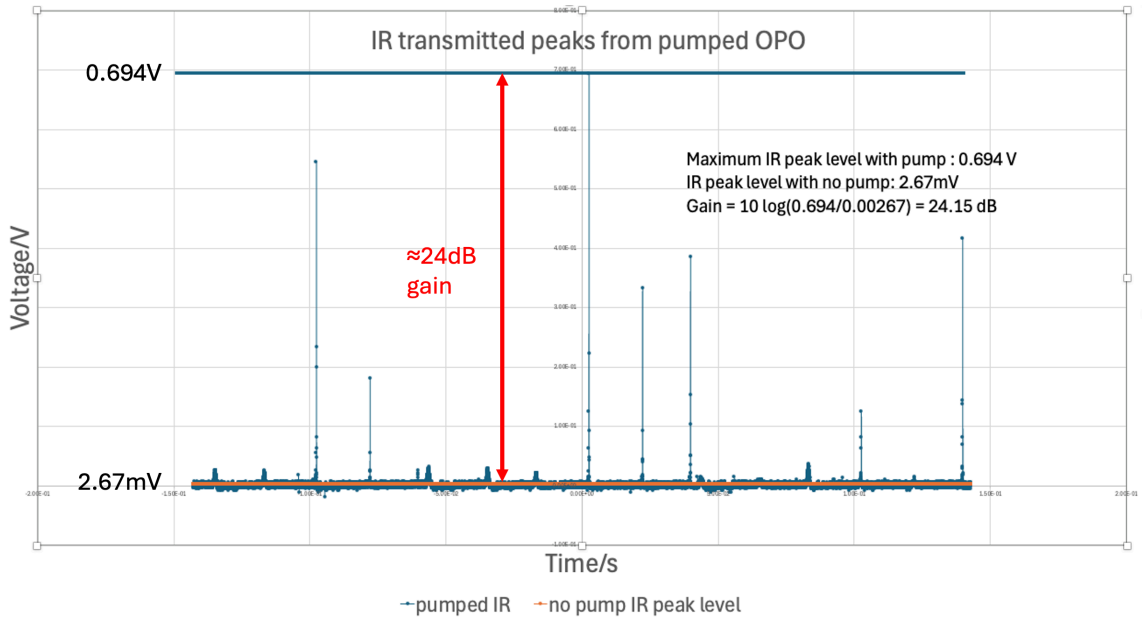


Figure 2.14: Data for measured ZZZ 24 dB gain. Maximum IR peak level with pump: 0.694 V. IR peak level with no pump: 2.67 mV. Gain = 10 log(0.694/0.00267) = 24.15 dB. The no pump IR level is marked in orange on the plot. The reason the amplified peaks have different heights is because we're scanning both cavity length and pump phase, maximum height only occurs when pump is completely in phase with input IR seed beam. These result were recorded at crystal temperature = 32.5729°C using a Moku:Lab device by Liquid Instruments.

2.3.4 Summary and Discussion

In this section I presented my work on building a new OPO source and characterizing it. My goal was to get a record of squeezing and my work has been a series of successful steps towards that.

- I was able to successfully model, build and optimize OPO performance over a range of different parameters.
- I was able to demonstrate triply resonant operation in the nondegenerate (YZY, type-II) and degenerate (ZZZ, type-0) cases.
- I was able to observe phase-sensitive amplification at large gain, a necessary

requirement for observing squeezing.

- I was able to observe lasing in the ZZZ OPO when getting it above threshold.

As mentioned in the chapter introduction, the type-0 OPO can be used to generate single-mode squeezed states, which are a necessary ingredient for cat state generation, which can in turn be used to make GKP states (useful for error correction)[33]. The triply resonant type-II OPO can be used to generate two-mode squeezed states and separable (by polarization), entangled photon pairs. Two-mode squeezed states can be used to generate cubic phase states[22].

The gain in the doubly resonant case is higher than the triply resonant case because the gain(in dB) is proportional to the nonlinear coupling coefficient d, which is greater in the ZZZ case than the YZY.

Compared to the setup in [23] where they observed 15 dB of squeezing in a doubly resonant OPO, our setup has a stand-alone back OPO mirror instead of being directly on the back end of crystal. This added step could potentially add absorption or scattering losses, but it was measured in previous experiments to be negligible. They use a 9.3 mm long PPKTP crystal while we use a 10 mm long, which means we could get even higher gain assuming the non-linear coupling coefficient d is the same (which they do not mention). Otherwise, our setups are similar. This is why I believe we could already have similar levels of squeezing since they measured ≈ 24 dB anti-squeezing. Measuring the squeezing though would require a balanced-homodyne detection (BHD) with precise control over the phase-lock between the local oscillator and OPO signal. In the paper they say their main set-back for measuring higher squeezing was photodetector efficiency in the BHD. We have a similar efficiency in our lab photodetectors and so I also believe we could measure similar levels of squeezing. I did not continue with that endeavor because our laser broke down. I am confident future students can make use of the OPO I built and achieve this result in our lab.

Chapter 3

Photon Number Resolving Detection (PNRD)

The nature of quantum mechanics dictates a fundamental wave-particle duality for physical systems, which was first recognized by Einstein through the understanding that light is composed of individual energy quanta known as photons [49]. The ability to accurately measure photons has led to checking the validity of the notion of 'spooky action at a distance' [50] and tremendous technological advancement in quantum communication [51], quantum metrology [52, 53, 54], and quantum computation [55, 56]. Much of this progress relies on the ability to measure single photons, such as through the use of avalanche photodiodes (APDs)[57]; however, the ability to resolve arbitrary numbers of photons beyond simply distinguishing vacuum from non-vacuum is highly desirable for many quantum information applications [58, 59, 60, 56]. The process of projecting a subset of modes of an entangled state onto the Fock-basis can allow for engineering non-Gaussian quantum states with negative Wigner functions [61, 62, 63] — a requirement for any quantum speed-up in continuous-variable quantum information [64].

In this chapter I will start with the theoretical description of photon number resolving detectors, positive-operator-valued-measures (POVMs). Next I will discuss a segmented single-photon avalanche-photodiode (SPAD) detector and its use as a PNRD. Finally I will discuss the transition-edge sensor (TES) and how my group and

I managed to use it to resolve up to 100 photons, breaking the previous world record of (~ 16) [29].

3.1 Detector positive-operator-valued-measures (POVMs)

If asked to write down a quantum operator describing a detector measuring the number of photons in a given pulse of light, the first thing that would come to mind is writing down an operrator of the form: $|n\rangle\langle n|$, a projection operator in the photon number basis (Fock basis).

Now, let's say our detector reports a single click for each photon it detects, and that it reported k clicks. In that scenario, our detector would be exactly described by: $|k\rangle\langle k|$ for that measurement. Explicitly saying: the state I was measuring was $|k\rangle$ which has k photons.

But, what if the number of photons incident on the detector was actually n, where n>k? This is entirely possible and very likely. Photons could be lost due to a number of reasons such as losses along the beam path to the detector or imperfections in the detector itself affecting its efficiency.

What if instead m photons where actually incident on the detector, where m<k? Where could the extra counts come from? These are called dark counts, and are due to the physics of the detector. We can clearly see now how it is incorrect to conclude that our measurement operator is $|k\rangle\langle k|$ and that our incident quantum state was $|k\rangle$ when registering k clicks on the detector. Our initial guess is only valid in the ideal case where there are no losses and dark counts. How then can we describe our measurement/detector?

This is where the positive-operator-valued-measure (POVM) formalism comes into play. It is a more general way to describe measurements, of which the projective (also known as *von Neumann*) measurements are a subset [65]. Each measurement outcome k is associated with a Hermitian operator, that is a POVM element, $\hat{\Pi}_k$. These POVM elements are complete ($\sum_k \hat{\Pi}_k = \hat{1}$), and the complete set $\{\hat{\Pi}_k\}$ is known as a POVM.

For phase insensitive detectors, such as photon counting detectors, the POVM element $\hat{\Pi}_k$ can be written as:

$$\hat{\Pi}_k = \sum_{n=0}^{\infty} P(k|n) \left|n\right\rangle \left\langle n\right| . \tag{3.1}$$

Where P(k|n) is the conditional probability of registering k clicks for n input photons. We can quickly see that if our detector is ideal, meaning that it reports k clicks if and only if k photons are input on the detector, we get:

$$\hat{\Pi}_k = \sum_{n=0}^{\infty} \delta_{n,k} \left|n\right\rangle \left\langle n\right| = \left|k\right\rangle \left\langle k\right| \tag{3.2}$$

which agrees with our initial intuition.

Now, let us consider the case of photon loss due to detector inefficiency. For a detector of efficiency $\eta \leq 1$, the conditional probability P(k|n) is given by:

$$P(k|n) = \binom{n}{k} \eta^k (1-\eta)^{n-k}. \tag{3.3}$$

We can make sense of the above formula by considering that if we do measure k clicks for n input photons where k<n, then for sure k photons made it through, and n-k photons were lost. The probability to measure a photon successfully is η and to lose

a photon is 1- η. Now we can understand the η^k and $(1-\eta)^{n-k}$ terms. Finally, because we have no way to tell which of the k photons out of n get registered by the detector, we account for that by the binomial term. From now on we shall refer to the conditional probability P(k|n) as P_l(k|n) where the l is for lossy.

Next, let us model the case of dark counts, on top of detector inefficiency, where m extra photons from the environment are incident on our detector in addition to the n photons from our input state, while registering k clicks. Assuming a probability of $P_d(m)$ for having m dark photon counts, we can modify Eq.(3.3) as:

$$\begin{aligned} P_{ld}(k|n) &= P_l(k|n)P_d(0) + P_l(k-1|n)P_d(1) + P_l(k-2|n)P_d(2) + ...P_l(0|n)P_d(k) \\ &= \sum_{j=0}^{k} P_l(k-j|n)P_d(j). \end{aligned} \tag{3.4}$$

where P_l(k-j|n) is given by Eq.(3.3).

Thus, we can write the POVM elements for a lossy PNR detector as:

$$\hat{\Pi}_k = \sum_{n=0}^{\infty} \binom{n}{k} \eta^k (1-\eta)^{n-k} \left|n\right\rangle \left\langle n\right| \tag{3.5}$$

and the POVM elements of a lossy PNR detector with dark counts as:

$$\hat{\Pi}_k = \sum_{n=0}^{\infty} \sum_{j=0}^{k} \binom{n}{k-j} \eta^{k-j} (1-\eta)^{n-k+j} P_d(j) \left|n\right\rangle \left\langle n\right| \tag{3.6}$$

Depending on the detector we have, we can use the best suited POVM definition. In the case of single-photon avalanche photodiodes (SPADs), we shall model all three cases in the following section. As for the transition edge sensor (TES), it has a very low dark count of less than 1 Hz, so we can neglect them and get away with using

Eq.(3.5).

Finally, we define the purity of a POVM element for outcome k as:

$$Purity(\Pi_k) = \frac{Tr(\Pi_k^2)}{Tr(\Pi_k)^2} \tag{3.7}$$

The purity satisfies the following condition:

$$\frac{1}{D} \leq Purity(\Pi_k) \leq 1 \tag{3.8}$$

where D is the dimension of the Hilbert space associated with the POVM element Π_k, i.e. the number of projectors with non-zero probabilities in that element. Thus, the closer the purity is to 1, the closer the POVM element is to a projection operator, the better it is as a measurement operator (i.e. determining what was the corresponding input state).

3.2 Single-photon avalanche-photodiodes (SPADs)

Single photon avalanche photodiodes (SPADs) are a type of avalanche photodiodes (APDs) that are designed in such a way that the absorption of at least one photon triggers an avalanche amplifying the output current pulse, which can then be easily detected. This way, a SPAD is essentially a 'click' detector, capable of distinguishing between zero and non-zero input photon states. There are several approaches to building a photon number resolving (PNR) detector out of SPADs like measuring the initial current generated in the SPAD before the avalanche fully develops [66], or as in the case we shall examine here, designing a segmented detector in such a away that the input photons are distributed on all the available SPADs minimizing the probability of a single SPAD ever seeing more than one photon[27].

In [27], the segmented detector is essentially a wave guide with SPADs attached along its length. The material choices and dimensions are designed such that photons get siphoned off the input light pulse one photon at a time. Such an arrangement is outlined in Fig [3.1].

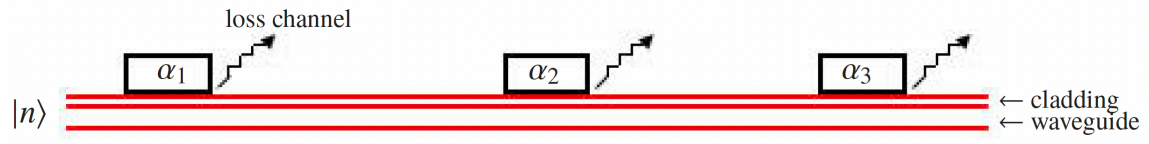


Figure 3.1: Figure taken from [27].Principle sketch of a segmented detector. Guided photons are detected alongside propagation by SPADs which frustrate total internal reflection. The quantum efficiency (QE) of SPAD #j is α_j^2. The design goal is to avoid detection losses, which are distinct from the nonunity of α_j^2, and keep all undetected photons in the waveguide for further detection.

Such a detector can be modeled, as done in [27], as a series of beamsplitters with transmissivities and reflectivities chosen such that each SPAD sees only one photon. This can be seen in Fig.[3.2]

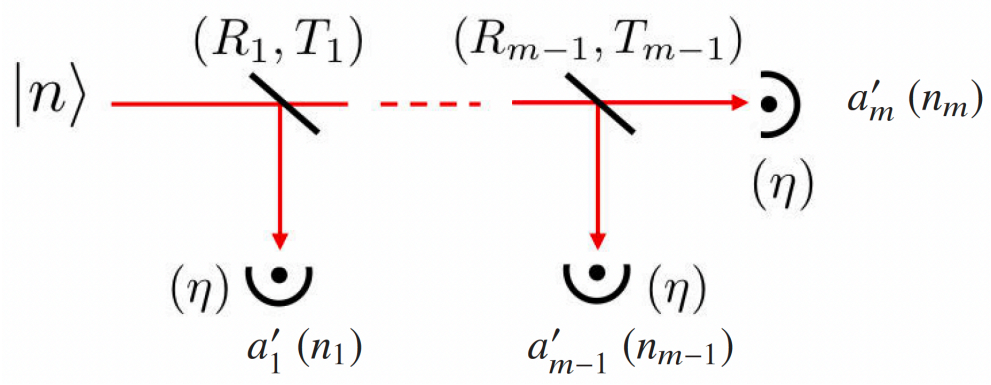


Figure 3.2: Figure taken from [27]. Model of a PNR segmented photodetector with $\mathrm{R}_j + T_j \equiv \mathrm{r}_j^2 + t_j^2 = 1, \forall \mathrm{j} \in [1,\mathrm{m}]$. a'_i are the annihilation operators for each detection mode i.

It is worth noting that $\alpha_j^2 < 1$, as shown in Fig. 3.1, is concerned with how much is actually absorbed by each SPAD #j assuming nothing is lost, and is different from one detector to the next. For $\alpha_j^2 < 1$, any light not absorbed by the SPAD goes back into the waveguide. As for $\eta < 1$, this is used to model lost photons in each 'beam split' and is the same on all detectors.

We would now like to assess our segmented SPAD detector and calculate the associated POVM purity for 3 cases: 1) lossless with no dark counts 2) lossy with no dark counts 3) lossy with dark counts. We want to see how the purity changes for different number of detectors, quantum efficiencies and dark counts.

Our initial approach could be to calculate the purities directly using the equations in the previous sections, and that is what was done in [27]. The problem with this approach is that it is computationally heavy and thus limits the number of SPADs we can simulate in our model. To solve this problem, instead of using the POVM element definition in the previous section, we use that defined in [67] which is exact and not an approximation. The POVM element there is given by:

$$\Pi_k =: \frac{N!}{k!(N-k)!}(e^{-(\eta\frac{\hat{n}}{N}+\nu)})^{N-k}(\hat{1} - e^{-(\eta\frac{\hat{n}}{N}+\nu)})^k : \tag{3.9}$$

Here N is the total number of detectors, k is the number of clicks, η is the quantum efficiency, ν represents the dark counts and : : is the normal ordering operator. We can rearrange this equation to get:

$$\Pi_k =: \frac{N!}{k!(N-k)!} e^{-\nu N} (e^{(\eta \frac{\hat{n}}{N} + \nu)} - \hat{1})^k e^{-\eta \hat{n}} : \tag{3.10}$$

Next, we Taylor expand the exponential in the middle parenthesis, subtract the first term (identity), and recognize that the parenthesis are repeated k times, for the k different detectors that saw at least one photon. We get:

$$\Pi_k =: \frac{N!}{k!(N-k)!} e^{-\nu N} \sum_{m_1..m_k \geq 1} \frac{(\eta \frac{\hat{n}}{N} + \nu)^{\sum_i m_i}}{m_1!...m_k!} e^{-\eta \hat{n}} : \tag{3.11}$$

3.2.1 POVM element Purity(Π_k) for different cases

Case 1: Lossless with no dark counts $\nu = 0$, $\eta = 1$

Setting $\nu = 0$ and $\eta = 1$ in Eq. 3.11 and following the procedure in the Appendix [67], we get their Eq.(A10) for the POVM elements:

$$\Pi_k = \frac{N!}{k!(N-k)!} \sum_{n=k}^{\infty} \frac{1}{N^n} \left[\partial_x^n (e^x - 1)^k |_{x=0} \right] |n\rangle \langle n| \tag{3.12}$$

For convenience, we define the coefficient D_{nk} as

$$D_{nk} = \partial_x^n (e^x - 1)^k |_{x=0} \tag{3.13}$$

We calculate the trace as follows:

$$
\begin{aligned}
Tr(\Pi_k) &= \sum_{i=0}^{\infty} \langle i| \Pi_k |i\rangle \\
&= \frac{N!}{k!(N-k)!} \sum_{i=0}^{\infty} \sum_{n=k}^{\infty} \frac{1}{N^n} D_{nk} \langle i| |n\rangle \langle n| |i\rangle \\
&= \frac{N!}{k!(N-k)!} \sum_{i=0}^{\infty} \sum_{n=k}^{\infty} \frac{1}{N^n} D_{nk} \langle i| |n\rangle \delta_{n,i} \\
&= \frac{N!}{k!(N-k)!} \sum_{n=k}^{\infty} \frac{1}{N^n} D_{nk} \langle n| |n\rangle \\
&= \frac{N!}{k!(N-k)!} \sum_{n=k}^{\infty} \frac{1}{N^n} D_{nk}
\end{aligned} \tag{3.14}
$$

and $\mathrm{Tr}(\Pi_k^2)$ is given by:

$$
\begin{aligned}
Tr(\Pi_k^2) &= \sum_{i=0}^{\infty} \langle i| \Pi_k \Pi_k |i\rangle \\
&= \Big(\frac{N!}{k!(N-k)!}\Big)^2 \sum_{n,m=k}^{\infty} \sum_{i=0}^{\infty} \frac{1}{N^{n+m}} D_{mk} D_{nk} \langle i| |m\rangle \langle m| |n\rangle \langle n| |i\rangle \\
&= \Big(\frac{N!}{k!(N-k)!}\Big)^2 \sum_{n,m=k}^{\infty} \sum_{i=0}^{\infty} \frac{1}{N^{n+m}} D_{mk} D_{nk} \delta_{i,m} \delta_{m,n} \delta_{n,i} \\
&= \Big(\frac{N!}{k!(N-k)!}\Big)^2 \sum_{n=k}^{\infty} \Big(\frac{1}{N^n} D_{nk}\Big)^2
\end{aligned} \tag{3.15}
$$

Plugging Eq. 3.14 and Eq. 3.15 into Eq. 3.7 we get:

$$
Purity(\Pi_k) = \frac{\sum_{n=k}^{\infty} \Big(\frac{1}{N^n} D_{nk}\Big)^2}{\Big(\sum_{n=k}^{\infty} \frac{1}{N^n} D_{nk}\Big)^2} \tag{3.16}
$$

Using Eq. 3.16 we can generate the following plot:

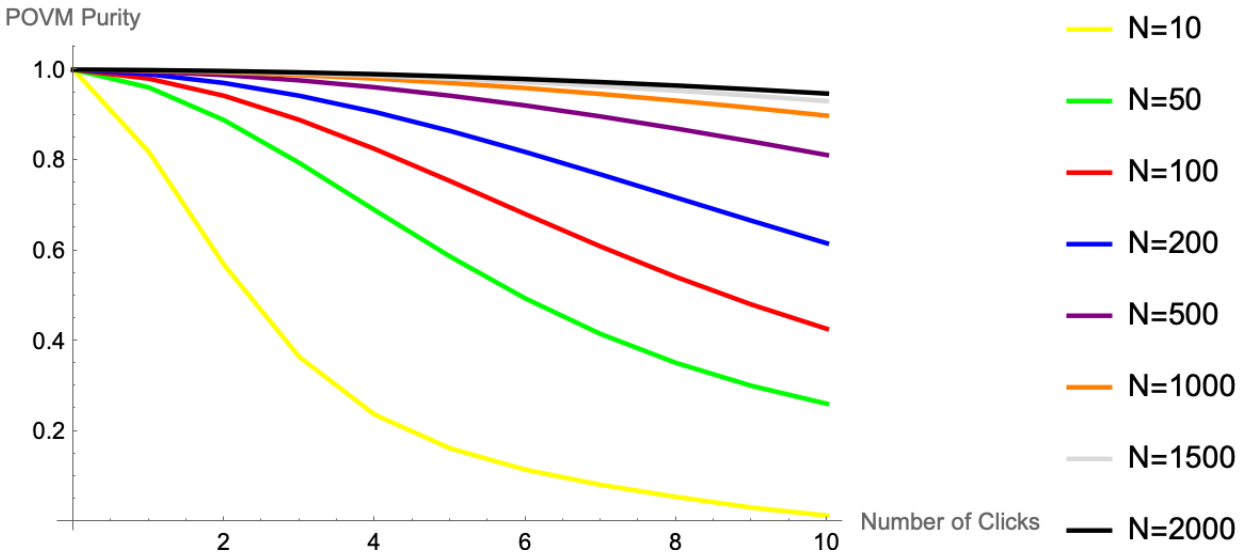


Figure 3.3: POVM element Purity(Π_k) vs click number k for different number of detectors N, with no losses or dark counts. This is a reproduction of Fig.[8] in [27].

Case 2: Lossy with no dark counts $\nu = 0$, $\eta \neq 1$

Setting $\nu = 0$ but keeping η in Eq. 3.11 we get:

$$\Pi_k =: \frac{N!}{k!(N-k)!} \sum_{m_1..m_k \geq 1} \frac{1}{N^{\sum_i m_i}} \frac{(\eta\hat{n})^{\sum_i m_i}}{m_1!...m_k!} e^{-\eta\hat{n}} : \tag{3.17}$$

We now make the substitution $\sum_i m_i = n$ and add a sum over n while keeping the m summations with the condition $\sum_i m_i = n$ for every term in the n summation. The n sum starts from k because each m_i is at least 1.

$$\begin{aligned} \Pi_k &= \frac{N!}{k!(N-k)!} \sum_{n=k}^{\infty} \sum_{m_1..m_k \geq 1} \frac{1}{N^n} \frac{1}{m_1!...m_k!} : (\eta\hat{n})^n e^{-\eta\hat{n}} : \\ &= \frac{N!}{k!(N-k)!} \sum_{n=k}^{\infty} \frac{\eta^n}{N^n n!} \left[\sum_{m_1..m_k \geq 1} \frac{n!}{m_1!...m_k!} \right] : \hat{n}^n e^{-\eta\hat{n}} : \end{aligned} \tag{3.18}$$

where in the second line we multiplied and divided by n!.

Let's take a closer look at the operators inside the normal ordering, we have:

$$
\begin{aligned}
:\hat{n}^n e^{-\eta\hat{n}}: &=: (\hat{n})^n \sum_{s=0}^{\infty} \frac{(-\eta\hat{n})^s}{s!} : \\
&= \sum_{s=0}^{\infty} \frac{(-\eta)^s}{s!} : \hat{n}^{s+n} : \\
&= \sum_{s=0}^{\infty} \frac{(-\eta)^s}{s!} : (a^\dagger a)^{s+n} : \\
&= \sum_{s=0}^{\infty} \frac{(-\eta)^s}{s!} (a^\dagger)^{s+n} a^{s+n} \\
&= (a^\dagger)^n \left[\sum_{s=0}^{\infty} \frac{(-\eta)^s}{s!} (a^\dagger)^s a^s \right] a^n \\
&= (a^\dagger)^n \left[\hat{1} - \eta a^\dagger a + \frac{\eta^2}{2} (a^\dagger)^2 a^2 - ... \right] a^n \\
&= (a^\dagger)^n \left[\sum_{s=0}^{\infty} (1-\eta)^s \left|s\right\rangle \left\langle s\right| \right] a^n \\
&= (a^\dagger)^n \hat{O} a^n
\end{aligned}
$$

Where $\hat{O}$ is what we will call the sum in the bracket.

We can easily verify that $\hat{O}$ acts in the following way:

$$
\begin{aligned}
&\hat{O} \left|m\right\rangle = (1-\eta)^m \left|m\right\rangle \\
&\left\langle m\right| \hat{O} \left|m\right\rangle = (1-\eta)^m \\
&\left\langle k\right| \hat{O} \left|m\right\rangle = (1-\eta)^m \delta_{k,m} \\
&\left\langle m\right| (a^\dagger)^n \hat{O} a^n \left|m\right\rangle = \frac{m!}{(m-n)!} (1-\eta)^{m-n}
\end{aligned}
\tag{3.19}
$$

As for the bracket in Eq. 3.18, it is exactly the same braket in the Appendix of [67]. And so we directly replace it with the following:

$$\left[\sum_{m_1..m_k\geq 1}\frac{n!}{m_1!...m_k!}\right]\rightarrow\left[\partial_x^n(e^x-1)^k|_{x=0}\right]=D_{nk} \tag{3.20}$$

We can now rewrite the POVM elements Π_k as:

$$\Pi_k=\frac{N!}{k!(N-k)!}\sum_{n=k}^{\infty}\frac{\eta^n}{N^n n!}D_{nk}(a^\dagger)^n\hat{O}a^n \tag{3.21}$$

$\mathrm{Tr}(\Pi_k)$ is given by:

$$\begin{aligned}Tr(\Pi_k)&=\sum_{i=0}^{\infty}\langle i|\,\Pi_k\,|i\rangle\\&=\frac{N!}{k!(N-k)!}\sum_{i=0}^{\infty}\sum_{n=k}^{\infty}\frac{\eta^n}{N^n n!}D_{nk}\,\langle i|\,(a^\dagger)^n\hat{O}a^n\,|i\rangle\\&=\frac{N!}{k!(N-k)!}\sum_{n,i=k}^{\infty}\frac{\eta^n}{N^n n!}D_{nk}(1-\eta)^{i-n}\frac{i!}{(i-n)!}\end{aligned} \tag{3.22}$$

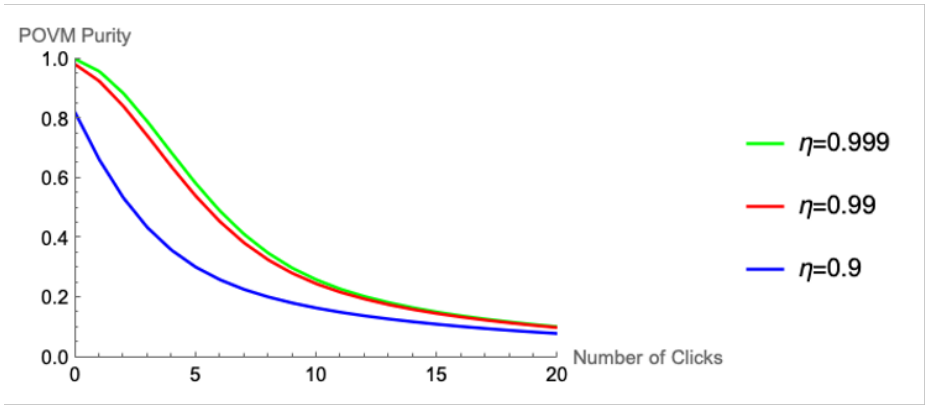
and $\mathrm{Tr}(\Pi_k^2)$ is given by:

$$
\begin{aligned}
Tr(\Pi_k^2) &= \sum_{i=0}^{\infty} \langle i| \, \Pi_k \Pi_k \, |i\rangle \\
&= \Big(\frac{N!}{k!(N-k)!}\Big)^2 \sum_{n,m=k}^{\infty} \sum_{i=0}^{\infty} \frac{\eta^{m+n}}{N^{n+m} m! n!} D_{mk} D_{nk} \, \langle i| \, (a^\dagger)^m \hat{O} a^m (a^\dagger)^n \hat{O} a^n \, |i\rangle \\
&= \Big(\frac{N!}{k!(N-k)!}\Big)^2 \sum_{n,m,i=k}^{\infty} \frac{\eta^{m+n}}{N^{n+m} m! n!} D_{mk} D_{nk} \sqrt{\frac{i!}{(i-m)!}} \sqrt{\frac{i!}{(i-n)!}} \\
&\quad \langle i-m| \, (\hat{O} a^m (a^\dagger)^n \hat{O} \, |i-n\rangle \\
&= \Big(\frac{N!}{k!(N-k)!}\Big)^2 \sum_{n,m,i=k}^{\infty} \frac{\eta^{m+n}}{N^{n+m} m! n!} D_{mk} D_{nk} \sqrt{\frac{i!}{(i-m)!}} \sqrt{\frac{i!}{(i-n)!}} \\
&\quad (1-\eta)^{i-m} (1-\eta)^{i-n} \, \langle i-m| \, (a^m (a^\dagger)^n \, |i-n\rangle \\
&= \Big(\frac{N!}{k!(N-k)!}\Big)^2 \sum_{n,m,i=k}^{\infty} \frac{\eta^{m+n}}{N^{n+m} m! n!} D_{mk} D_{nk} (1-\eta)^{i-m} (1-\eta)^{i-n} \\
&\quad \sqrt{\frac{i!}{(i-m)!}} \sqrt{\frac{i!}{(i-n)!}} \sqrt{\frac{i!}{(i-m)!}} \sqrt{\frac{i!}{(i-n)!}} \\
&= \Big(\frac{N!}{k!(N-k)!}\Big)^2 \sum_{n,m,i=k}^{\infty} \frac{\eta^{m+n}}{N^{n+m} m! n!} D_{mk} D_{nk} \frac{(1-\eta)^{2i-m-n} (i!)^2}{(i-m)!(i-n)!}
\end{aligned} \tag{3.23}
$$

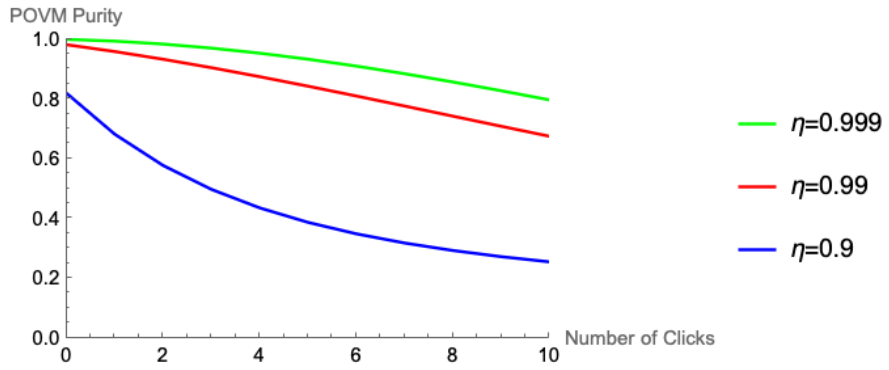
Substituting Eq. 3.22 and Eq. 3.23 into Eq. 3.7 we get:

$$
Purity(\Pi_k) = \frac{\sum_{n,m,i=k}^{\infty} \frac{\eta^{m+n}}{N^{n+m} m! n!} D_{mk} D_{nk} \frac{(1-\eta)^{2i-m-n} (i!)^2}{(i-m)!(i-n)!}}{\Big(\sum_{n,i=k}^{\infty} \frac{\eta^n}{N^n n!} D_{nk} (1-\eta)^{i-n} \frac{i!}{(i-n)!} \Big)^2} \tag{3.24}
$$

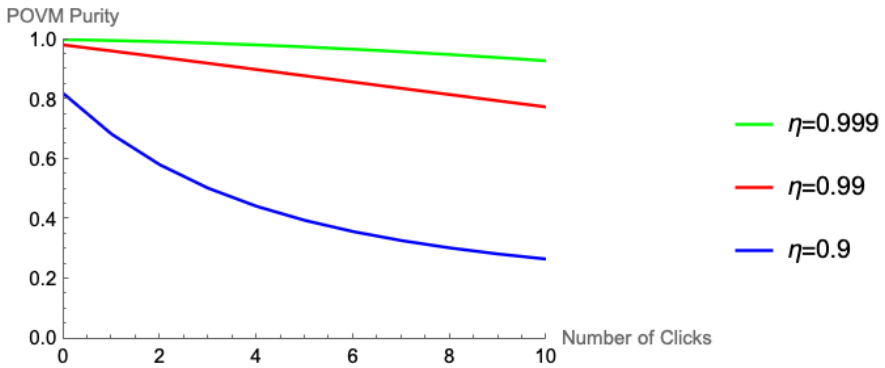
Plotting Eq. 3.24 we find:



(a) $N = 50$



(b) $N = 500$



(c) $N = 2000$

Figure 3.4: POVM element Purity(Π_k) vs click number at different quantum efficiencies η for different values of N. (a) $N = 50$, (b) $N = 500$, (c) $N = 2000$.

Table 3.1: Number of SPADs N required to reach 90 and 99% POVM purities versus loss per SPAD $L = 1-\eta$, for different click numbers. We take the maximum tolerable loss per detector to be $L_{\max} \sim 1/N \,|_{L=0\%}$. This corresponds to the probability of losing 1 photon out of N, which we do not want to occur. We can see how for high purity the number of SPADs needed is in the thousands. This would require integrated optics, but that's feasible.

Click number	purity	L	N	$L_{\max}$	purity	L	N	$L_{\max}$
3	90%	0%	113	1%	99%	0%	1193	0.1%
		0.01%	113			0.01%	1295	
		0.1%	121			0.1%	5793	
		1%	433					
5	90%	0%	279	0.36%	99%	0%	2980	0.03%
		0.01%	283			0.01%	3382	
		0.1%	314					
10	90%	0%	1050	0.1%	98%	0%	4000	0.025%
		0.01%	1100			0.01%	5000	

Case 3: Lossy with dark counts $\nu \neq 0$, $\eta \neq 1$

Again, we start from Eq. 3.11. After multiplying by n!/n!, using the substitution in Eq. 3.20, moving ν outside the parentheses and rearranging we get:

$$\Pi_k = \frac{N!}{k!(N-k)!} e^{-\nu N} \sum_{n=k}^{\infty} \frac{\nu^n}{n!} D_{nk} : (\frac{\eta \hat{n}}{N\nu} + 1)^n e^{-\eta \hat{n}} : \tag{3.25}$$

Let's take a closer look at the operators inside the normal ordering, we have:

$$
\begin{aligned}
:(\frac{\eta\hat{n}}{N\nu}+1)^n e^{-\eta\hat{n}}: &=: \sum_{q=0}^{n}\binom{n}{q}\Big(\frac{\eta\hat{n}}{N\nu}\Big)^q e^{-\eta\hat{n}}: \\
&=: \sum_{q=0}^{n}\binom{n}{q}\Big(\frac{\eta}{N\nu}\Big)^q \hat{n}^q \sum_{s=0}^{\infty}\frac{(-\eta)^s}{s!}\hat{n}^s: \\
&= \sum_{q=0}^{n}\sum_{s=0}^{\infty}\binom{n}{q}\Big(\frac{\eta}{N\nu}\Big)^q \frac{(-\eta)^s}{s!}:\hat{n}^{q+s}: \\
&= \sum_{q=0}^{n}\sum_{s=0}^{\infty}\binom{n}{q}\Big(\frac{\eta}{N\nu}\Big)^q \frac{(-\eta)^s}{s!}(a^\dagger)^{q+s}a^{q+s} \\
&= \sum_{q=0}^{n}\binom{n}{q}\Big(\frac{\eta}{N\nu}\Big)^q (a^\dagger)^q\Big[\sum_{s=0}^{\infty}\frac{(-\eta)^s}{s!}(a^\dagger)^s a^s\Big]a^q \\
&= \sum_{q=0}^{n}\binom{n}{q}\Big(\frac{\eta}{N\nu}\Big)^q (a^\dagger)^q\hat{O}a^q
\end{aligned}
$$

Substituting back in Eq. 3.25 we get:

$$
\Pi_k = \frac{N!}{k!(N-k)!}e^{-\nu N}\sum_{n=k}^{\infty}\frac{\nu^n}{n!}D_{nk}\sum_{q=0}^{n}\binom{n}{q}\Big(\frac{\eta}{N\nu}\Big)^q (a^\dagger)^q\hat{O}a^q \tag{3.26}
$$

Taking the trace of this equation is very similar to what we did in Eq. 3.22, we now have:

$$
\begin{aligned}
Tr(\Pi_k) &= \sum_{i=0}^{\infty}\langle i|\,\Pi_k\,|i\rangle \\
&= \frac{N!}{k!(N-k)!}e^{-\nu N}\sum_{n=k}^{\infty}\frac{\nu^n}{n!}D_{nk}\sum_{q=0}^{n}\binom{n}{q}\Big(\frac{\eta}{N\nu}\Big)^q\sum_{i=0}^{\infty}\langle i|\,(a^\dagger)^q\hat{O}a^q\,|i\rangle \\
&= \frac{N!}{k!(N-k)!}e^{-\nu N}\sum_{n=k}^{\infty}\sum_{q=0}^{n}\sum_{i=0}^{\infty}\frac{\nu^n}{n!}D_{nk}\binom{n}{q}\Big(\frac{\eta}{N\nu}\Big)^q\frac{i!}{(i-q)!}(1-\eta)^{i-q}
\end{aligned} \tag{3.27}
$$

where when going to the last line we used Eq. 3.19.

$\mathrm{Tr}(\Pi_k^2)$ is given by:

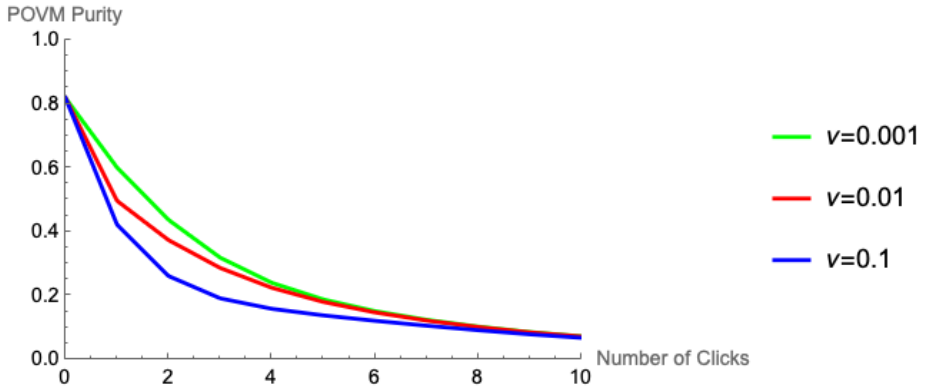
$$\begin{aligned} Tr(\Pi_k^2) &= \sum_{i=0}^{\infty} \langle i| \, \Pi_k \Pi_k \, |i\rangle \\ &= \left(\frac{N!}{k!(N-k)!} e^{-\nu N}\right)^2 \sum_{n=k}^{\infty} \sum_{m=k}^{\infty} \frac{\nu^{m+n}}{m!n!} D_{mk} D_{nk} \\ &\quad \sum_{s=0}^{m} \sum_{q=0}^{n} \binom{m}{s} \binom{n}{q} \left(\frac{\eta}{N\nu}\right)^{s+q} \sum_{i=0}^{\infty} \langle i| \, (a^\dagger)^s \hat{O} a^s (a^\dagger)^q \hat{O} a^q \, |i\rangle \\ &= \left(\frac{N!}{k!(N-k)!} e^{-\nu N}\right)^2 \sum_{n,m=k}^{\infty} \sum_{s=0}^{m} \sum_{q=0}^{n} \sum_{i=0}^{\infty} \frac{\nu^{m+n}}{m!n!} D_{mk} D_{nk} \\ &\quad \binom{m}{s} \binom{n}{q} \left(\frac{\eta}{N\nu}\right)^{s+q} \frac{(1-\eta)^{2i-s-q} (i!)^2}{(i-s)!(i-q)!} \end{aligned} \tag{3.28}$$

where when going to last line we used the same process as in Eq. 3.23 to evaluate the expectation value.

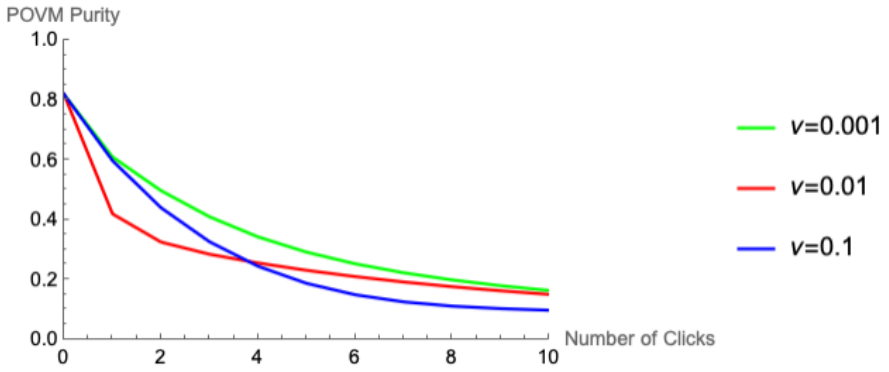
Finally, substituting Eq. 3.27 and Eq. 3.28 into Eq. 3.7 we get:

$$Purity(\Pi_k) = \frac{\sum_{n,m=k}^{\infty} \sum_{s=0}^{m} \sum_{q=0}^{n} \sum_{i=0}^{\infty} \frac{\nu^{m+n}}{m!n!} D_{mk} D_{nk} \binom{m}{s} \binom{n}{q} \left(\frac{\eta}{N\nu}\right)^{s+q} \frac{(1-\eta)^{2i-s-q} (i!)^2}{(i-s)!(i-q)!}}{\left(\sum_{n=k}^{\infty} \sum_{q=0}^{n} \sum_{i=0}^{\infty} \frac{\nu^n}{n!} D_{nk} \binom{n}{q} \left(\frac{\eta}{N\nu}\right)^{q} \frac{i!}{(i-q)!} (1-\eta)^{i-q}\right)^2} \tag{3.29}$$

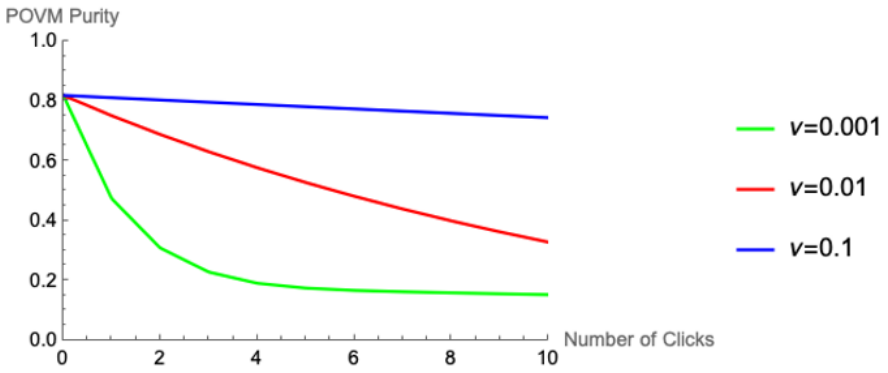
Practically, when computing the results using Eq. 3.29 we would have to place an upper limit instead of ∞ in the sums inside the equation. A value of 20 was used in all following figures except figures 3.5(a) and 3.6(a) where greater accuracy was needed to correctly describe the behavior. Below are the results.



(a) $N = 16$

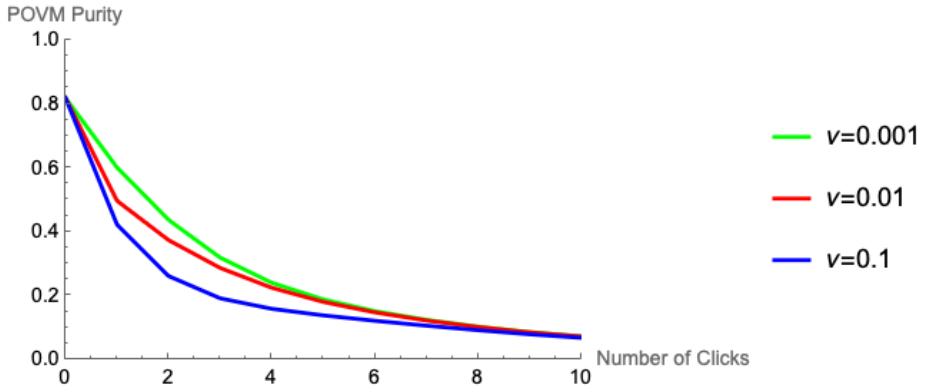


(b) $N = 50$

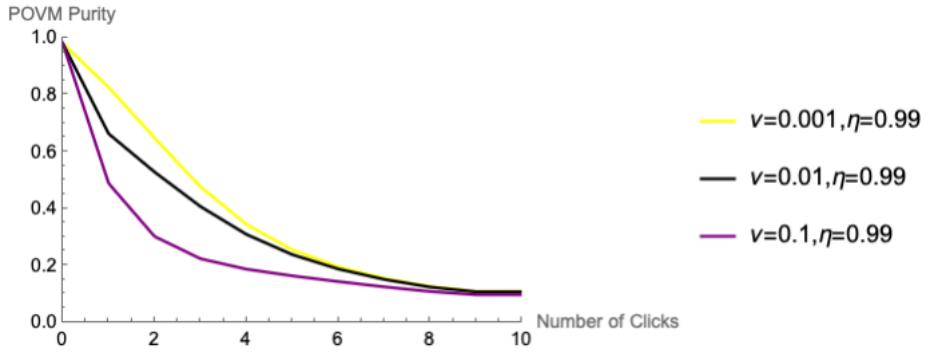


(c) $N = 2000$

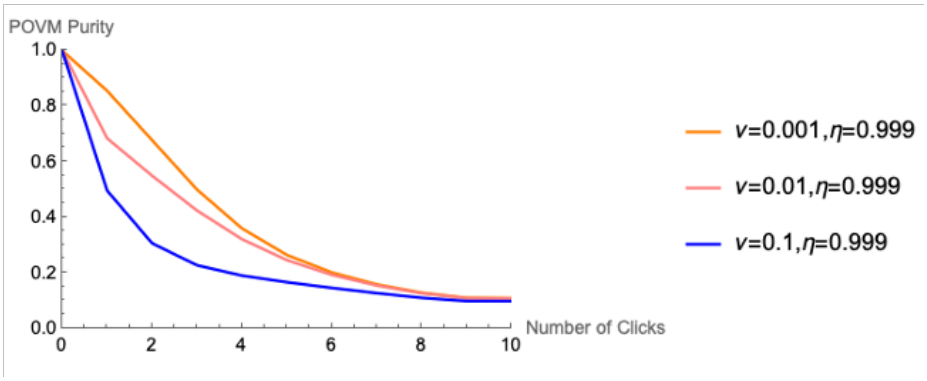
Figure 3.5: POVM element Purity(Π_k) vs click number at quantum efficiency η=0.9 for different values of ν and N. (a) $N = 16$, (b) $N = 50$, (c) $N = 2000$.



(a) $\eta = 0.9$

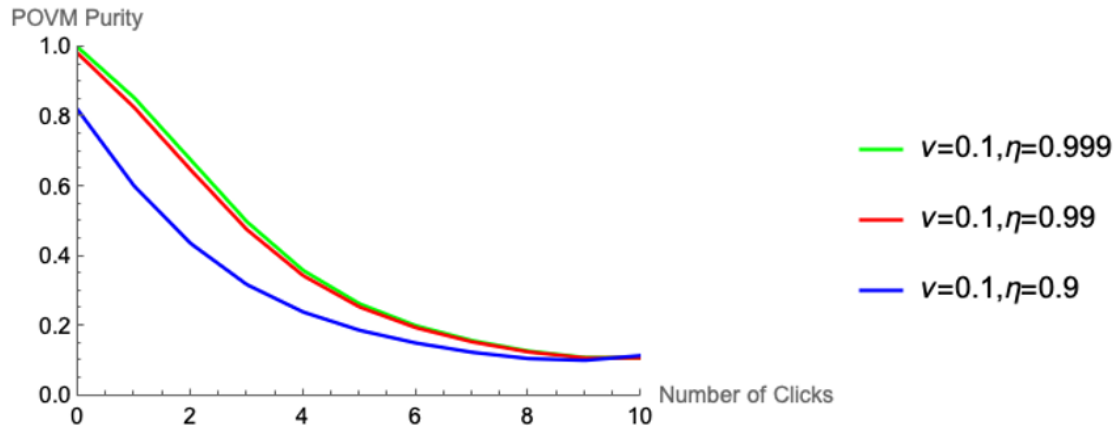


(b) $\eta = 0.99$

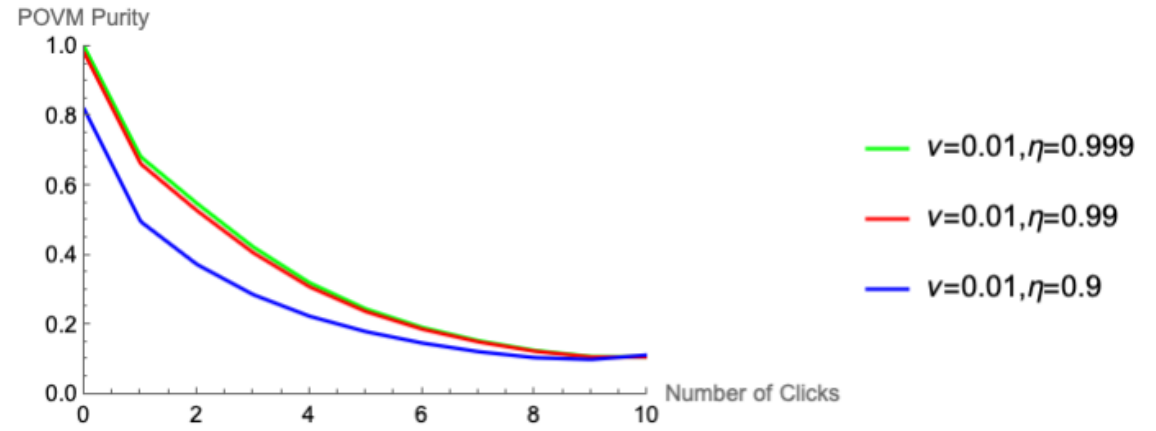


(c) $\eta = 0.999$

Figure 3.6: POVM element Purity(Π_k) vs click number at N=16 for different quantum efficiencies η and different ν's. (a) $\eta = 0.9$, (b) $\eta = 0.99$, (c) $\eta = 0.999$.



(a) $\nu = 0.1$



(b) $\nu = 0.01$

Figure 3.7: POVM element Purity(Π_k) vs click number at N=16 for different quantum efficiencies η and different ν's. (a) $\nu = 0.1$, (b) $\nu = 0.01$.

3.2.2 Summary

In this section I presented my work on efficiently modeling a segmented PNR detector based on SPADs. My goal was to produce new results previously unattainable due to computational complexity and I was able to achieve that.

- I was able to successfully model a segmented PNR detector based on SPADs using less computationally demanding mathematical functions (derivatives of exponentials rather than factorials).
- I was able to generate new results guiding commercial applications, namely: How many detectors are needed, for a given loss coefficient, to achieve a particular POVM purity. This will guide detector design by calculating how many detectors will be needed on-chip for successful implementation for different applications.

3.3 Transition-Edge Sensor (TES)

The transition-edge sensor (TES), which is based on a calorimeter formed from a superconducting wafer held just below the critical temperature, has arisen as a viable PNRD with quantum efficiency approaching unity and entirely negligible dark counts [68, 69, 70]. Previous results with TES systems show the ability to measure non-classical systems with high mean-photon numbers [71, 72]; however, these experiments were based on methods requiring extensive post-processing that give generally good estimates of photon-number measurements but relatively low distinguishability between individual photon counts above 10 photons [73]. For demanding applications requiring photon-number resolution, even a single photon discrepancy destroys quantum correlations. Current methods demonstrate the potential to accurately count photons in the low double-digits($\sim$ 16) [29], but certain proposals necessitate considerably higher detection events for conditional state preparation. One particularly salient example is the preparation of a cubic-phase state to complete a universal gate set for continuous-variable quantum computation [21]. In order for the numerical approximations used in this formalism to hold, one must detect a large number of photons — simulations suggest 50 or more [22]. The detection scheme we demonstrate here now easily surpasses this previously unreachable milestone.

The Transition Edge Sensor (TES) serves as a photon-number-resolving detector (PNRD) by leveraging the highly temperature-sensitive resistance of a superconductor close to its phase transition point. In our setup, these TESs are constructed from superconducting tungsten wafers, functioning at a critical temperature around 100 mK. When a photon hits the chip, its absorbed thermal energy disrupts the superconducting state in a localized area, creating a small region with measurable resistance. Around this critical temperature, the superconductor's resistivity goes almost linearly with temperature, as shown in Fig. 3.8(a). Our detectors were optimized to maximize

absorption at the specific wavelength we targeted, achieving quantum efficiencies exceeding 90% at 1064 nm. However, it's worth noting that other TES systems have recorded efficiencies as high as $\eta = 0.98$ [69], with indications that values beyond $\eta > 0.99$ [74] might be attainable.

Each TES chip is wired to an induction loop, set up in parallel with a reference resistor, and supplied with a biasing current, as depicted in Fig. 3.8(b). When a photon gets absorbed by the detector, the chip's resistivity linearly increases, which reduces the current passing through the inductor. This change is detected and amplified by the highly sensitive Superconducting Quantum Interference Device (SQUID) magnetometers, converting it into a classical voltage signal that we can measure. That signal then gets an additional external amplification before being fed into an Ethernet-based flash analog-to-digital converter (EFADC)—a device built on a field-programmable gate array (FPGA)—which pulls out essential signal details in real time.

To ensure optimal performance, the SQUIDs require precise biasing to achieve maximum sensitivity. During sensitivity tests with an external input, the SQUID fringe must be distinctly visible and attain its maximum amplitude, as illustrated in Fig. 3.8(c). This is accomplished by carefully adjusting the SQUID bias setting on the cryostat. Modifying the 'flux bias' (FB) enables us to establish the baseline position along the SQUID fringe, which should be aligned with the steepest segment of the slope to maximize responsivity. For more details on TES detectors, including their design and various applications, information is available in Ref.[70]. The detectors utilized in this study were provided by the Sae Woo Nam group at the National Institute of Standards and Technology (NIST).

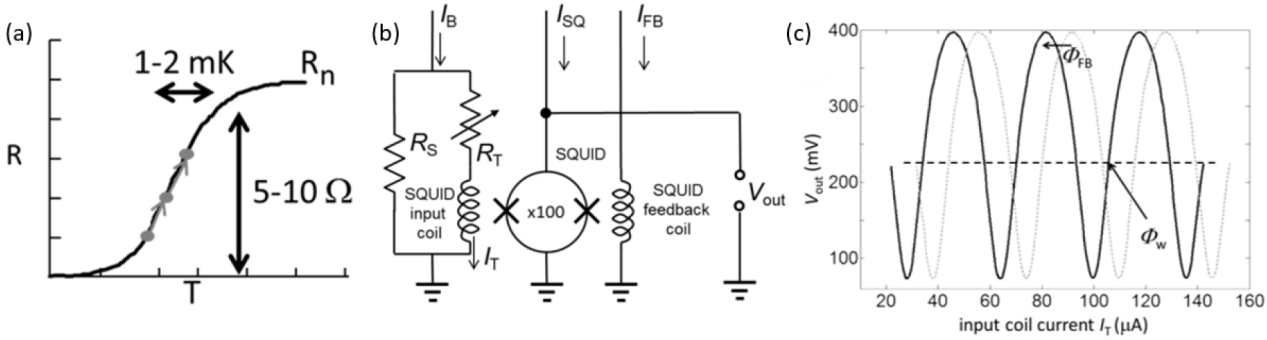


Figure 3.8: Figure taken from [70]. (a) Resistivity of TES as temperature increases near the superconducting phase transition. (b) Readout circuit with SQUID magnetometer for detecting changes in resistance. (c) SQUID fringe tuned such that all SQUID signals (SQUID input coil signal and SQUID feedback coil signal) are in-phase and constructively interfere.

3.3.1 Experimental Considerations

Pulsing

It is worth highlighting that the TES struggles to effectively handle continuous wave (CW) laser input. Beyond its notably slow cool-down period ($\geq 20\ \mu$s), the TES lacks a defined 'reset time,' meaning it remains perpetually capable of registering additional signals. When CW light strikes the detector, there's a constant chance of detecting an event at any moment, and if multiple events overlap within a specific time frame, this can result in pile-ups that make distinguishing photon numbers challenging [54, 75]. Despite these challenges, low-flux CW light remains viable for use with the TES, particularly in heralding experiments where pile-ups are infrequent [54, 76]. To circumvent the pile-up issue, we adopted a controllable pulsed method, enabling us to adjust the interval between pulses so the TES can fully cool back to its base temperature before the arrival of the next laser pulse.

In our 100 photon detection experiment, the coherent state sent to the TES is generated by pulsing a continuous-wave 1064 nm laser using an acousto-optical modulator (AOM) as an optical switch. The pulse duration is set to be less than 100 ns, which

is well-within the rising-edge time of the detection signal. The pulses are sent at a repetition rate of 12.5 kHz to ensure that the detector has re-cooled and thermal noise is at a minimum. This rate can be increased to 50 kHz without incurring substantial ill-effects. Each split pulse -split by beamsplitters, as shown in Fig. 3.15(a)- is coupled to a TES channel through standard single-mode optical fiber. Details on TES operation within a cryostat can be found in Refs. [70, 54]. In this work, we additionally filter the output signal to remove the DC component and implement a low-noise external amplifier to bring the signal to within a 500 mV range, floor-to-peak, as will be explained in the data acquisition subsection.

External amplification and filtering

This subsection (external amplification and filtering) discusses the external amplifier circuit board after the TES and before the EFADC acquisition device. Miller Eaton, my colleague at the time, designed the amplifier and I helped physically build it by soldering the components on the board. The following is an excerpt from his PhD dissertation included for completeness[33]:

> The magnitude of the analog output signal from the TES is dependent on several factors including bias and temperature in addition to the number of photons actually absorbed. Even for large PNR signals, this voltage remains on the order of 0-25 mV. Because the EFADC digitizes a 0-500 mV range with 12-bit accuracy, the best peak differentiation will occur if the input signal is designed to occupy the majority of the available voltage input range. In order to do this, we designed an amplifier circuit based on the ultra-lownoise OPA818 op-amp.
>
> In order to design the circuit to properly amplify the photon peaks and reduce noise, it is useful to first examine the frequency-domain spectrum

of the signal. This is shown in Fig. 3.9. From this plot, we see that the signal drops off quickly beyond 1.4 MHz, but there is a substantial contribution at low frequency, even down to 1 kHz. This contribution can be attributed to the slow cooling tail that trails after each event. This portion of the signal will be important to the area calculation so should not be excluded. However, there is a DC offset that one would like to suppress, so some highpass filtering would also be helpful.

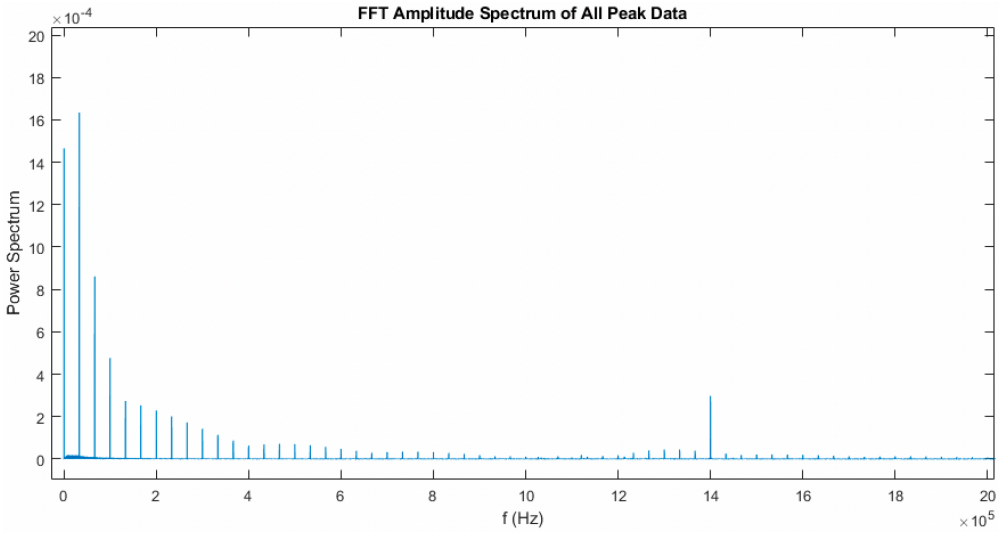


Figure 3.9: FFT data of TES signal. Figure from [33].

To test possible filtering frequencies, low and high-pass filtering was applied to the data in post-processing at several test frequencies as shown in Fig. 3.10. Both panels of this figure show the original data (blue) compared to the data filtered by the given frequency (red). It can be seen that the test high-pass filter at 40 kHz in Fig. 3.10(a) performs poorly as several features are qualitatively quite different; this shows that the low-frequency peaks in the power spectrum are components of the signal, and important to be kept.

The high-pass filter in Fig. 3.10(b), however, seems to perform quite well. The filtered data gives similar quality peaks but smooths the fast noise.

This indicates that the 1.4 MHz peak on the power spectrum may be noise unrelated to the signal. However, it was eventually decided that this 1.4 MHz component may also relate to the initial peak height, as the rise time can be quite fast depending on the bias, and 1 MHz Fourier components are expected for a signal with a rise time of 1 μs.

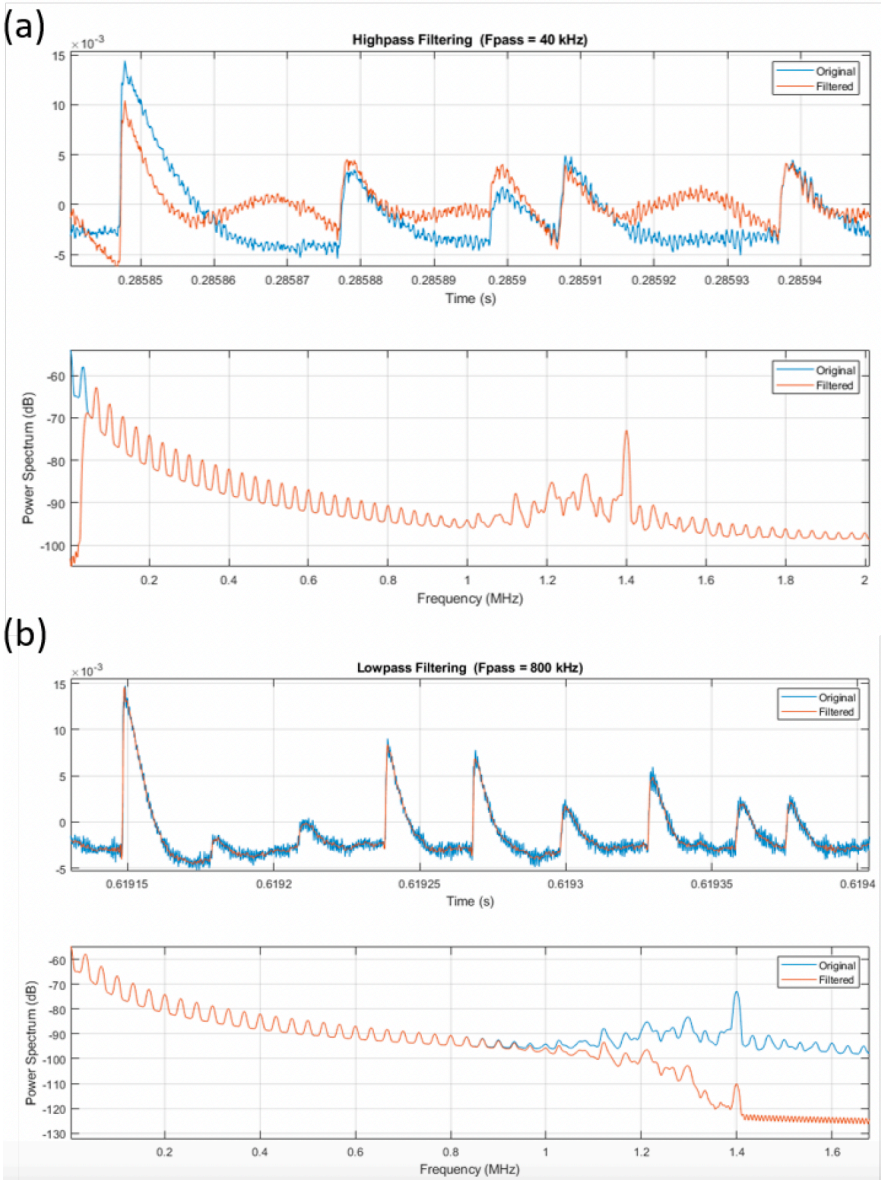


Figure 3.10: TES signal (blue) compared to a filtered signal (red) for a highpass filter applied at 40 kHz (a) and a low-pass filter applied at 800 kHz (b). The top panel of each shows the comparison of the signal in time while the bottom compares the power spectrum in the frequency domain. Figure from [33].

The final circuit design is shown in Fig. 3.11, where the top panel shows the simplified circuit diagram and the picture shows the modified demo board for the op-amp use. First, an active high-pass filter with a cutoff frequency of 145 Hz is used to remove the DC component of the signal and provide a gain of 20. At the end of the circuit, a low-pass filter with cutoff frequency of 3.2 MHz is used to clean any residual noise from the op-amp or other high-frequency noise from the TES signal.

The demo board can be turned into the amplifier described by replacing R2 with a 10 kW resistor, removing R3 entirely, replacing R4 with a 500 W resistor, adding a 1 nF capacitor at R7 (not shown in picture), and replacing R9 with a 2.2 mF capacitor. After these modifications, the frequency response was measured as shown in Fig. 3.12

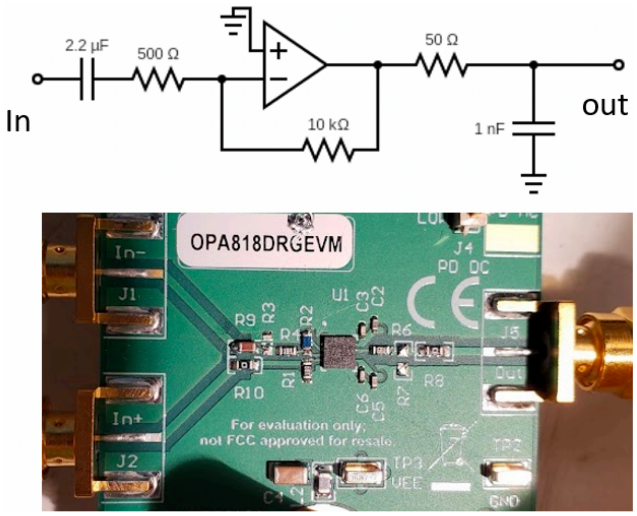


Figure 3.11: Circuit used to amplify the TES output signal into the 0-500 mV range. The circuit is an active high-pass filter with corner of 145 Hz, gain of 20, and low-pass filter at 3.2 MHz. The modified OPA818 demo board is also shown. Figure from [33].

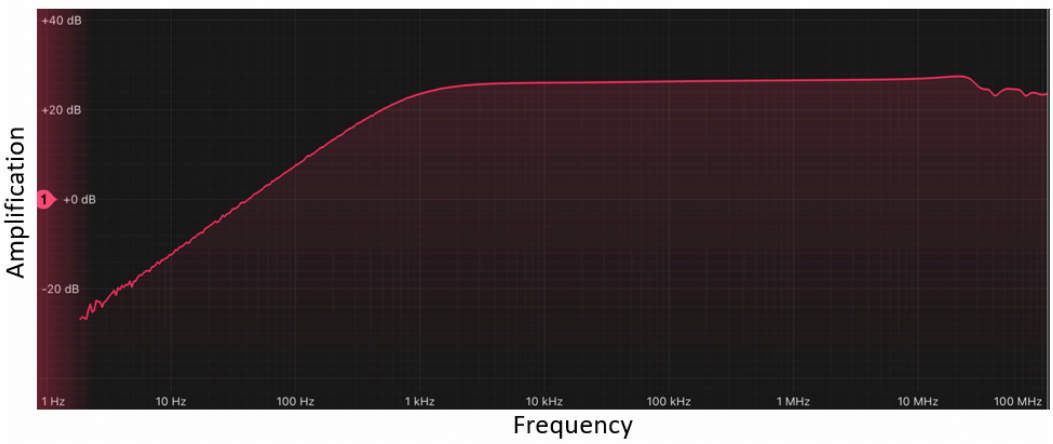


Figure 3.12: Frequency response of the OPA818 amplifier circuit. Figure from [33].

Data acquisition

The amplified output signal is sent to a custom-built Ethernet-based flash analog-to-digital converter (EFADC) capable of collecting and processing TES signals for up to 8 channels. The device is based on a field-programmable gate array (FPGA) which samples a signal with 12-bit resolution at a rate of 250 MHz. The internal memory and processing speed allows the device to collect up to 32 µs worth of signal points, perform rudimentary calculations on the data to determine key parameters, and transfer the calculated parameters to a hard disk all before the next signal pulse arrives.

The EFADC is triggered by an external pulse signal corresponding to the arrival time of each coherent state pulse. If the incoming signal rises above a user-defined noise threshold, the EFADC begins integrating waveform until the signal falls below a second threshold that can be set to account for hysteresis. The integrated signal area, maximum peak height, signal duration, timestamp of signal start, and timestamp of signal maximum are all recorded. All parameters can be used for additional signal characterization in post-processing, but we find that pulse area is sufficient to achieve large photon-number resolution.

The interface between the TES, the EFADC, and the lab computer is shown in Fig. 3.13. Upon receiving a trigger signal within a voltage range of 2-4 V, the EFADC starts data collection for each pulse. For this setup to work properly, the trigger should be the same signal used to pulse the laser, switching the acousto-optic modulator on and off. The EFADC 50 Ohm input impedance and it converts analog inputs in the range 0-500 mV into digital signals. Should the input surpass 500 mV, the EFADC reports the peak value until the input drops below this limit. This is useful in photon number resolution, as the peak amplitude minimally affects the total area, thus occasionally allowing the input to exceed the saturation threshold may be beneficial. This point will be further explained in the next section. Additionally, the EFADC possesses a user-adjustable DAC offset that is set with trial and error for each channel to maintain baseline noise near zero on the digital output. The DAC also inverts the analog signal before digitization, thus the actual input should be peaks in the range from 0 to -500 mV. The DAC offset provides a means to mitigate minor input signal voltage offsets.

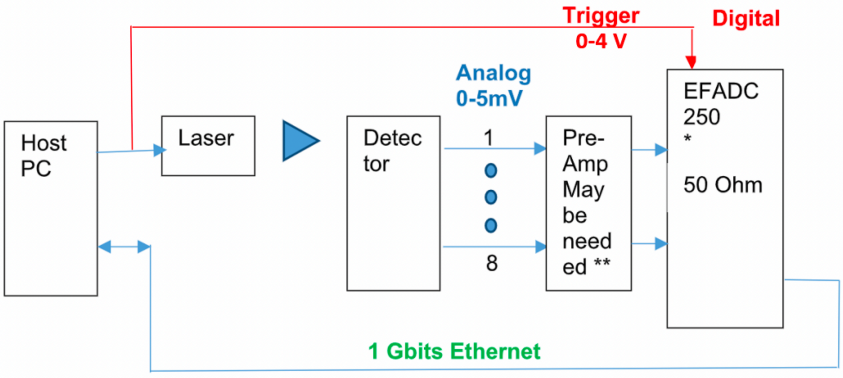


Figure 3.13: Diagram of data collection. An external trigger is synced to pulse the laser and prepare the EFADC to look for TES output pulse data. Each pulse is temporarily stored while calculations are performed on the hardware, then key parameters are permanently stored.

Once it receives a signal, the EFADC's internal firmware is configured to compute and provide a range of key parameters, such as the peak height, area, trigger timestamp, the timestamp of the peak relative to the trigger, and various other parameters. These

computations rely on multiple user-defined input parameters. Comprehensive details regarding the EFADC data acquisition system's operation, including the structure of the output data, are available in the firmware documentation on the QFQI group's Dropbox or in the Github repository of Miller's dissertation[33]. The rest of this section is based on that documentation. However, the core functionality can be understood by referring to Fig. 3.14.

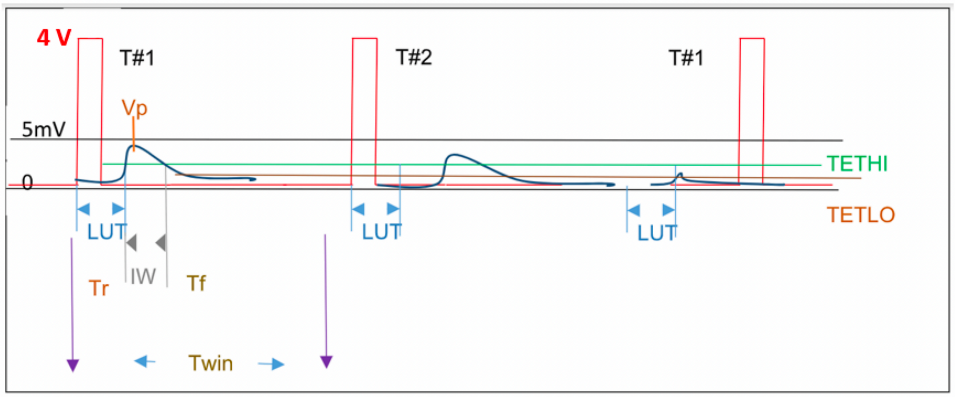


Figure 3.14: A basic depiction of the response of the EFADC firmware. For an incoming trigger signal (red), the firmware decides whether to acquire the signal (blue) based on user-defined controls. Further details can be found in the main text.

The user first programs trigger thresholds (TET) such that the device will only integrate the signal if it first crosses the upper threshold, TETHI, and it will continue to calculate the pulse parameters until either the signal drops below the lower threshold, TETLO, or the signal continues beyond the maximum duration specified by the user.

After the device receives a trigger, if the signal rises above TETHI for a user-specified number of ADC samples (NSAT), and if this occurs within a certain number of samples from the trigger define by the lookup time (LUT), the device will behave as follows:

- A Y user-programmable number of samples (PedNumOfAdcSamp) starting at the Trigger time will be averaged to be reported as a Pedestal for this trigger. Y is restricted to be 1,2,4, or 8. If any of these ADC samples is above TETHI, the

Pedestal quality bit will set to TRUE. If an ADC sample within PedNumOfAdcSamp is greater than the user-programmable value (MAXPED), MaxPedDetect bit is set to TRUE.

- If a pulse started within PedNumOfAdcSamp, PulseInPed is set to TRUE

- The samples (including the Pedestal samples) in that channel will be summed until a sample drops below TETLO (the final sample below TETLO). In other words, the samples within the integration window (IW) will be summed. If an ADC sample is either above or below the limits set by the input signal, then either an Overflow (Ov) or underflow (Uv) bit will be set to TRUE and recorded in the output file. The sum is terminated either when the EFADC receives a new trigger or if the value for Twin is reached. Twin is a user-programmable quantity that determines how long, in ADC samples, the sum should continue as measured from the start of the trigger.

- Twin must be less than the minimum time between pulses. If Twin is greater than the time between pulses, the second pulse will not be recognized, i.e., if more than one pulse occurs within Twin, only the parameters of the first pulse will be processed.

- The time that the 1st sample is above TETHI (Tr) and the time that the 1st sample falls below TETLO (Tf) will be reported. This time is relative to the rising edge of the trigger signal.

- The peak ADC sample (Vp) and the time (Tp) will be reported.

- If after a Trigger signal, no NSAT number of samples is larger than TETHI within the specified LUT, only the time of the trigger is stored in the output file.

- The difference between TETHI and TETLO is essentially hysteresis. As such the user should not set TETHI and TETLO to the same value. The difference should be set to be equal to or greater than the baseline noise of the signals.

Of the three triggers shown in Fig. 3.14, only T#1 has data to report. T#2 does not

have data to report because samples cross TETHI after LUT time. Similarly, T#3 does not have data to report because no or not enough sample(s) cross TETHI. It should be noted that all quantities, whether it be a measure of voltage or time, are stored in terms of ADC samples. For example, if one wishes to specify a time of 800 ns for LUT, the user would set LUT = 200 since the device performs one sample every 4 ns.

Efficiency calibration

Transition-edge sensors have managed to reach up to 98% quantum efficiency (QE) [69], but it is important to characterize the precise response of our detection system at 1064 nm. The power in a given pulse sent to each TES detector is on the order of several pW, so care must be taken to accurately calibrate the QE. First, we constructed and characterized a high-amplification photodetection circuit with a low-power sensitivity threshold at approximately 200 pW. Calibration for this detector was based on a Scientech pyroelectric calorimeter and a series of precision attenuators. The home-build photodetector was then used in conjunction with the attenuators to calibrate each TES channel individually. Laser-light was split at a 95:5 beamsplitter where the stronger portion was sent to the photodetector and the weaker portion was further attenuated and sent to the TES. This calibrated attenuation included the effects of imperfect fiber coupling so the TES quantum efficiency could be directly measured.

For each detector, 10^6 pulses were sent simultaneously to the photodetector and the TES channel under test. The mean photon number was extracted from the PNRD and compared with the classical signal power to determine the QE. We measured a QE of $97(^{+3}_{-5})\%$ for Channel 1, $93(\pm5)\%$ for Channel 2, and $91(\pm5)\%$ for Channel 3. The 5% uncertainly originates from the absolute error on the Scientech pyroelectric calorimeter, uncertainty on splitting ratio, and error on the attenuation calibration.

All channels used were thus measured to have a QE above 90%.

3.3.2 Resolution of 100 Photons

In our published paper[77], we extend the resolving capabilities of individual TES detectors to a maximum of 37 photons per detection channel with on-the-fly signal processing. We then multiplex three detectors into a system capable of resolving 0-100 photons with detector quantum efficiencies above 90%. Furthermore, we illustrate the utility of our scheme toward quantum cryptography applications by creating a quantum random number generator (QRNG). The need for random numbers arises in many applications including cryptography, simulation, and games of chance. Pseudo-random number generators (PRNG) are not truly random and can, for example, lead to erroneous results in Monte Carlo simulations [78]. The stochastic nature of quantum mechanics leads to true randomness, but many current implementations sample random events from a non-uniform distribution which can lead to bias that must be corrected classically [79, 80]. Our method to implement a QRNG is based on sampling the photon statistics of a coherent state and is fundamentally unbiased, robust to experimental and environmental noise, and invulnerable to eavesdropping. Details on the quantum random number generation can be found in the next chapter.

The detection system used here is constructed by splitting a laser pulse equally across three paths and sending each to a TES as shown in Fig. 3.15(a).

In order to resolve absorbed photon number, information to distinguish different outputs must be extracted from the signal received by the FPGA. An example signal is depicted in Fig. 3.15(b). Traditionally, peak height has been used for an indicator as the magnitude of the voltage is proportional to the energy absorbed for low-photon numbers [70]. However, this technique limits individual detector resolution due to the saturation of the peak magnitudes beyond several photons, so recently, alterna-

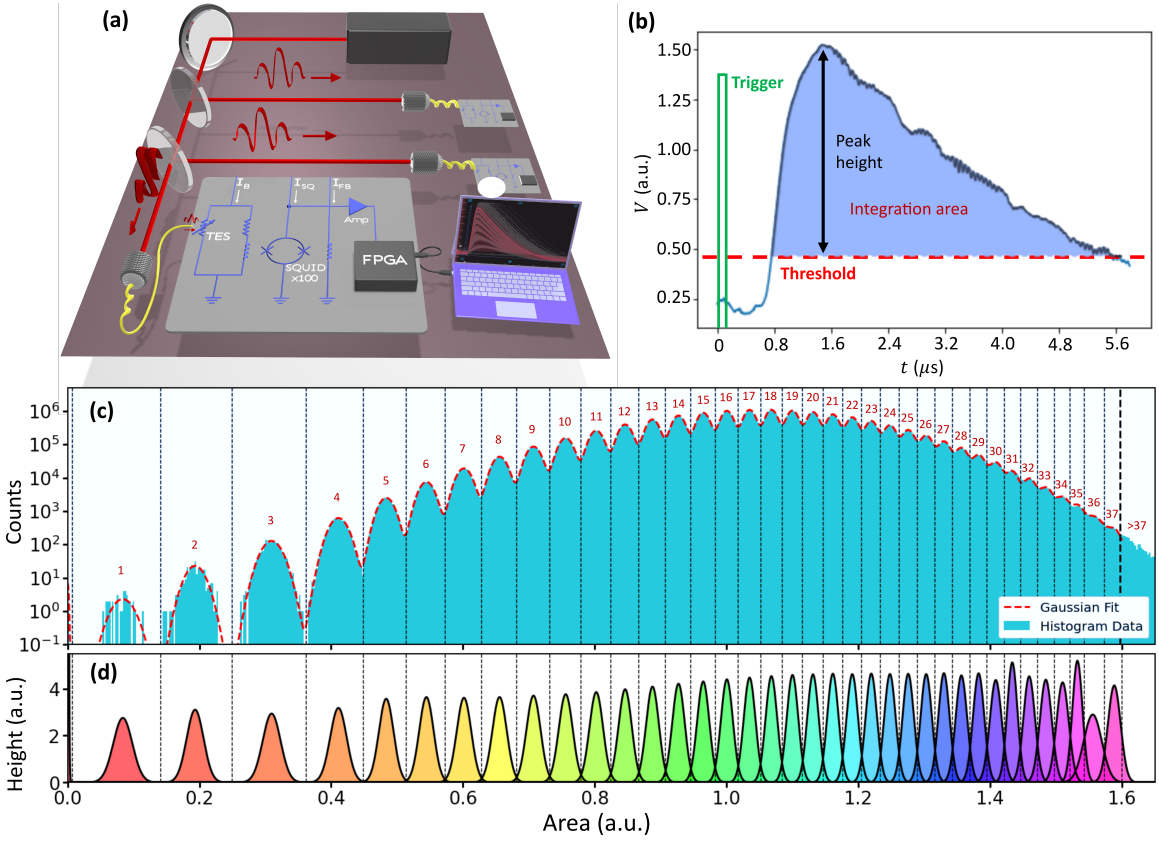


Figure 3.15: (a) Experimental setup. A pulsed sources is evenly split into three segments and each is coupled to a TES detector channel. (b) Example event (blue) following the pulse trigger (green). Pulse parameters including area and height are recorded if the signal passes a specified threshold. (c) Histogram of measured signal areas of 10^8 events for a single TES channel where a sum of Gaussians (dashed red line) is used to fit the data to determine binning for photon-number resolution. Bins are set at the intersection of between the normalized Gaussians as shown in (d).

tive methods have been explored for extracting useful information [29]. Although the maximum voltage of the peak saturates, the electrical resistance of the TES continues to change as it re-cools back to the superconducting state, suggesting useful information is contained beyond the peak as the cooling time will also depend on the energy absorbed. Integrating the signal in the region above a pre-defined noise threshold yields information about both the maximum voltage and the time to cool the TES; this peak area thus allows the resolution of many more photons than height alone.

For a single TES channel, the histogram of areas for 10^8 measurement events of a pulsed coherent state is shown in Fig. 3.15(c). As the pulse area monotonically increases with absorbed energy, the distinctly separated bins correspond exactly to quanta of energy detected and can be used to inform the number of photons measured. The location of these bins can be determined by fitting the obtained histogram to a sum of Gaussian functions (red dotted line in the figure), where the intersection of each normalized Gaussian gives the location of the bin edge. The reason for a Gaussian distribution within each bin is due to variations in the peak areas resulting from electronic and thermal noise on the cooling tail of signal peaks. The Gaussian fitting breaks down for large areas beyond the black dashed line in Fig. 3.15(c) indicating the photon-number can no longer be accurately determined for this detector. The number of events beyond the detector resolution across all three TES channels accounts for less than 0.3% of events.

The normalized Gaussian fits to the histogram are displayed in the bottom panel, Fig. 3.15(d), where it can be seen that the overlap of neighboring Gaussian peaks is quite small for the majority bins, indicating a high confidence in correctly determining the true photon number for a given area measurement. The confidence rate decreases with photon number but remains above 90% for photon numbers from 0-20 in Fig. 3.15(d). A plot of the experimentally measured probability distribution for a large coherent state with $\bar{n} = 57$, which allows use to make full use of our PNRD and

clearly resolve out to 100 photons is shown in Fig. 3.16.

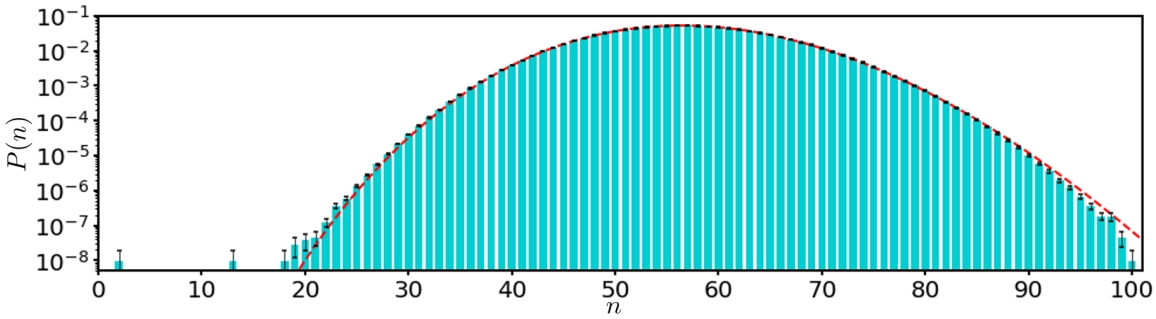


Figure 3.16: Experimental photon number distribution obtained by splitting a coherent state of mean photon number $\bar{n} = 57$ across three TES channels over 10^8 events. The red dashed line indicates the theoretical Poissonian distribution with a mean of 57. Error bars shown are of one SD and are obtained from finite sampling and photon-number binning errors.

If one is willing to post-select and slightly reduced count rates, the accuracy of a given photon-number assignment can be substantially increased by defining regions of uncertainty near the bin edges. If an event area is recorded in this uncertainty region, then the event is discarded and not considered in the statistics. Provided the regions of uncertainty are scaled in terms of the fitted Gaussian widths, σ_n, then the measured probability distribution will not deviate from the true distribution and the accuracy of individual photon-number assignment will increase. If the regions of uncertainty are defined beyond $\pm\sigma_n$, then 32% of the data is discarded, but the confidence rates increase to 99% or higher for the first 20 photons. If area events are only kept within $\pm\frac{1}{2}\sigma_n$ of each peak, then confidence rates further increases to 99% out to 31 photons. The area histograms, Gaussian fits, and quantitative overlap errors for each of the three detection channels are given in the Extended Data section.

Extended Data

Further analyses of experimental data are shown in the figures below. The effect of error-rate reduction through binning modifications is shown in Fig. 3.17 with the

normalized Gaussian fitting for all three TES channels displayed in Fig. 3.18. Specific error rates for different photon-number measurements on each channel based on different histogram binning is shown in Fig. 3.19.

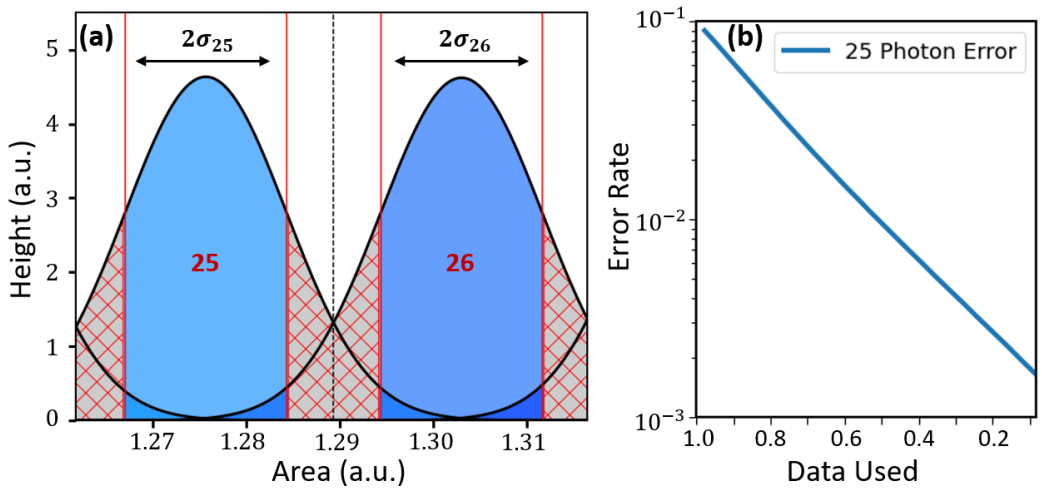


Figure 3.17: Error-rate reduction on photon-number resolution through post-selection of data. (a) By excluding data points with measured areas further from the center of each bin, the portion of overlap from neighboring Gaussians can be substantially reduced. The location of the new binning thresholds must be the same fraction of the Gaussian peak width, σ_n, for each bin. Here, $2\sigma_n$ is chosen. (b) Error rate to incorrectly characterize a true 25 photon event as a function of the proportion of measurement data kept.

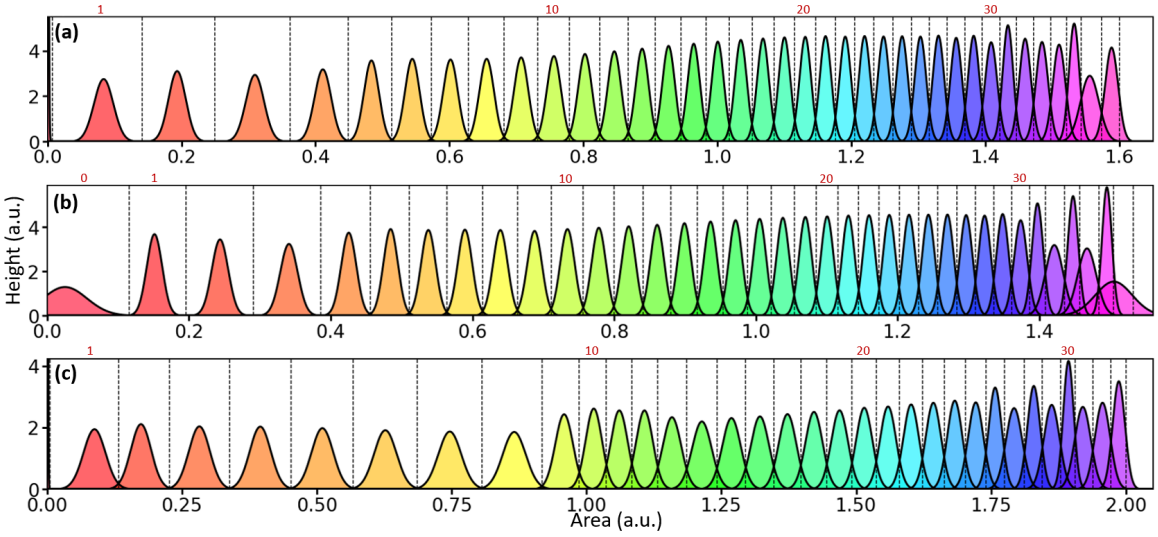


Figure 3.18: Normalized Gaussian fits for the histogrammed areas measurements TES channel 1 (a), 2 (b), and 3 (c). Note that for channels 1 and 3, the FPGA thresholds are set above the electronics noise such that zero photon events have a measured area of zero. For channel 2, electronics noise can drift slightly above the set voltage threshold so that small, non-zero areas are recorded for zero photon events.

Channel 1

n	$Error_{all}$	$Error_{2\sigma}$	$Error_{1\sigma}$
0	<1E-5 %	<1E-5 %	<1E-5 %
1	0.00323%	<1E-5 %	<1E-5 %
2	0.00337%	<1E-5 %	<1E-5 %
3	0.00606%	<1E-5 %	<1E-5 %
4	0.12408%	0.00005%	<1E-5 %
5	0.40158%	0.00038%	0.00003%
6	0.76496%	0.00163%	0.00015%
7	1.18980%	0.00640%	0.00072%
8	1.59754%	0.01444%	0.00176%
9	1.99698%	0.02717%	0.00355%
10	2.46313%	0.04999%	0.00712%
11	2.92733%	0.08202%	0.01249%
12	3.38050%	0.12056%	0.01897%
13	3.82676%	0.17018%	0.02819%
14	4.26184%	0.22828%	0.03883%
15	4.76323%	0.31062%	0.05509%
16	5.29303%	0.41246%	0.07629%
17	5.84855%	0.54010%	0.10365%
18	6.43810%	0.69847%	0.13860%
19	7.02718%	0.88229%	0.18133%
20	7.67397%	1.11349%	0.23902%
21	8.33058%	1.37321%	0.30043%
22	9.06531%	1.72533%	0.39977%
23	9.71082%	2.04220%	0.48005%
24	10.39516%	2.44039%	0.59682%
25	10.98424%	2.79816%	0.69679%
26	11.60429%	3.19400%	0.82521%
27	12.02390%	3.54259%	0.89904%
28	12.99672%	4.21978%	1.16603%
29	13.22495%	4.51885%	1.15847%
30	14.95028%	5.70299%	1.87684%
31	11.81587%	3.57955%	0.75042%
32	14.34333%	5.46466%	1.61618%
33	16.29129%	7.33867%	2.19949%
34	19.02733%	9.67386%	3.56896%
35	16.03542%	15.29955%	2.69396%
36	28.15765%	17.54685%	9.97878%
37	23.28622%	2.50462%	0.37663%

Channel 2

n	$Error_{all}$	$Error_{2\sigma}$	$Error_{1\sigma}$
0	0.16505%	0.00904%	0.00443%
1	0.05360%	<1E-5 %	<1E-5 %
2	0.00422%	<1E-5 %	<1E-5 %
3	0.01519%	<1E-5 %	<1E-5 %
4	0.24684%	0.00022%	0.00002%
5	0.69270%	0.00138%	0.00013%
6	1.08336%	0.00453%	0.00048%
7	1.35976%	0.00844%	0.00093%
8	1.74642%	0.01792%	0.00215%
9	2.24348%	0.03934%	0.00548%
10	2.67735%	0.06201%	0.00886%
11	3.17022%	0.10150%	0.01555%
12	3.74374%	0.15965%	0.02598%
13	4.32444%	0.23883%	0.04093%
14	4.91033%	0.33929%	0.06098%
15	5.50332%	0.46070%	0.08641%
16	6.14017%	0.61542%	0.12057%
17	6.76565%	0.80202%	0.16266%
18	7.43999%	1.02582%	0.21652%
19	8.12803%	1.28837%	0.28310%
20	8.80006%	1.59444%	0.36344%
21	9.44801%	1.91218%	0.44474%
22	10.13576%	2.27646%	0.54859%
23	10.78673%	2.68344%	0.66457%
24	11.43643%	3.10811%	0.79199%
25	12.12337%	3.58303%	0.93612%
26	12.82011%	4.10727%	1.09553%
27	13.56510%	4.72383%	1.29533%
28	14.36295%	5.40639%	1.55068%
29	14.76240%	5.94518%	1.61591%
30	17.22925%	7.81656%	2.74031%
31	15.42488%	11.06632%	2.09260%
32	27.31078%	16.69295%	9.17559%
33	15.25798%	12.39242%	4.12422%
34	32.96108%	22.82930%	14.26695%
35	12.37675%	9.35277%	7.95803%
36	54.07997%	45.62961%	40.43541%

Channel 3

n	$Error_{all}$	$Error_{2\sigma}$	$Error_{1\sigma}$
0	0.00016%	<1E-5 %	<1E-5 %
1	1.48394%	0.05080%	0.00971%
2	1.58273%	0.02465%	0.00281%
3	0.43777%	0.00032%	0.00003%
4	0.37926%	0.00016%	0.00001%
5	0.39887%	0.00019%	0.00001%
6	0.44089%	0.00028%	0.00002%
7	0.48277%	0.00037%	0.00003%
8	1.07570%	0.01913%	0.00414%
9	4.86415%	0.75226%	0.18864%
10	10.00977%	2.39729%	0.57133%
11	12.99089%	4.23998%	1.16158%
12	12.23206%	3.74354%	0.94267%
13	11.71984%	3.28820%	0.87955%
14	12.14633%	3.56774%	1.00551%
15	11.98636%	3.48938%	0.89375%
16	12.31270%	3.71189%	0.98322%
17	12.53381%	3.90230%	1.03879%
18	12.89334%	4.16052%	1.11179%
19	13.33620%	4.53110%	1.25031%
20	13.63416%	4.80738%	1.31482%
21	14.23810%	5.29031%	1.50045%
22	14.71015%	5.74825%	1.63897%
23	15.35154%	6.36062%	1.86422%
24	15.79179%	6.91107%	1.98914%
25	17.62951%	8.32499%	2.88164%
26	15.86059%	8.39646%	1.95142%
27	21.31844%	11.52445%	4.87493%
28	16.24228%	9.37796%	2.18805%
29	24.01478%	14.02259%	6.54019%
30	16.13940%	13.40093%	2.90600%
31	28.29595%	19.30811%	9.57075%
32	23.68172%	15.52840%	6.19073%
33	22.26482%	7.99003%	2.11533%

Figure 3.19: Error rates for all detection channels depending on binning. Error percentages indicate the probability to incorrectly count a measurement that was a true n photon event. $Error_{all}$ includes all areas and uses the Gaussian intersections to place bins. $Error_{2\sigma}$ discards area events occurring outsides of a 2σ width centered around each Gaussian in the histogram fit. The thrown-out events account for 32% of all measurements. The $Error_{1\sigma}$ discards area events occurring outsides of a 1σ width centered around each Gaussian in the histogram fit. This removes 62% of the measured data but drastically reduces counting errors.

3.3.3 Summary

In this section I presented my work on improving photon number resolving capability by optimizing the use of our TES detector. My goal was to break the previous record of resolving ≈ 16 photons and I have achieved that, successfully resolving up to 100 photons.

- I was able to successfully calibrate and operate the TES detector taking into account different experimental considerations.
- In collaboration with my colleagues in the group and collaborators at Jefferson Lab, I was able to successfully set up the new custom-made FPGA-based EFADC data acquisition device allowing us to achieve the new record performance.

A natural question that may arise is why did we not use the POVM treatment here to assess confidence in our measured number of photons with the TES? While the POVM treatment would be more rigorous, we believe that the error from the Gaussian fit overlap is enough for the purposes we are seeking here.

Chapter 4

PNRD Applications

In this chapter I will discuss two applications of photon number resolving detectors. The first is quantum random number generation and the second is Fock state interferometry.

4.1 Quantum random number generation (QRNG)

The need for random numbers arises in many applications ranging from cryptography to simulation. Typically, pseudo random number generators (PRNG) are used due to their easy implementation and high generation rates. These are algorithmic methods that take a small input string as the 'seed' and produce outputs following a uniform distribution, mimicking randomness, but the outputs are reproducible if the seed is known. While that is sometimes useful, unpredictability is a prerequisite for most applications. Alternatively, true random number generators (TRNGs) are devices that rely on measuring some unpredictable or at least difficult to predict physical processes as a source of randomness. Quantum random number generators (QRNG) are considered a subset of TRNG whose source of randomness is truly stochastic quantum phenomena.

The prototypical photonic QRNG is based on sending a single photon to a balanced beamsplitter and placing detectors on the output to determine whether the photon was transmitted or reflected [81, 82]. This is a truly random coin-flip in the ideal

case, but it comes with limitations, such as the need for on-demand single photons, a perfectly balanced beamsplitter, and ideal detectors. Other optical techniques, such as homodyne measurements to detector random vacuum fluctuations [83] or a variation on the first method where weak light is spread across a sensor array [84] can also be used, but these methods also suffer from physical limitations and noise that lead to randomness with bias. The randomness achieved is not sampled from a uniform distribution and therefore systematic bias must be removed with classical algorithms [85, 86]. Beyond reducing data and requiring vulnerable classical schemes, systems with inherent bias are at risk to quantum hacking [87], where an adversary can effectively change the calibrated bias and use this to their advanced to break encryption.

Here, we implement a QRNG making use of the inherent randomness present in the parity of the Poissonian distribution of a coherent state [88, 89]. When sampling the parity of the photon-number distribution, the inherent bias vanishes exponentially quickly with increasing coherent state intensity and asymptotically approaches a true coin flip. To generate the random numbers we simply convert a photon number detection to a binary output, where each even photon-number event is assigned an outcome of '0' and odd photon-numbers are assigned a '1'. This method is unaffected by experimental imperfections such as photon loss, detector inefficiency, phase and amplitude noise, and contamination by environmental noise, in the limit of large $\bar{n}$ as will be shown below.

For the parity operator given by $\hat{\Pi} = (-1)^{\hat{n}} = e^{i\pi\hat{n}}$ where $\hat{n} = \hat{a}^\dagger\hat{a}$ is the photon-number operator and the operators $\hat{a}^\dagger$ and $\hat{a}$ are the respective bosonic creation and annihilation operators, we can examine the expectation value of parity for a coherent state,

$$|\alpha\rangle = e^{-\frac{1}{2}\alpha^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,. \tag{4.1}$$

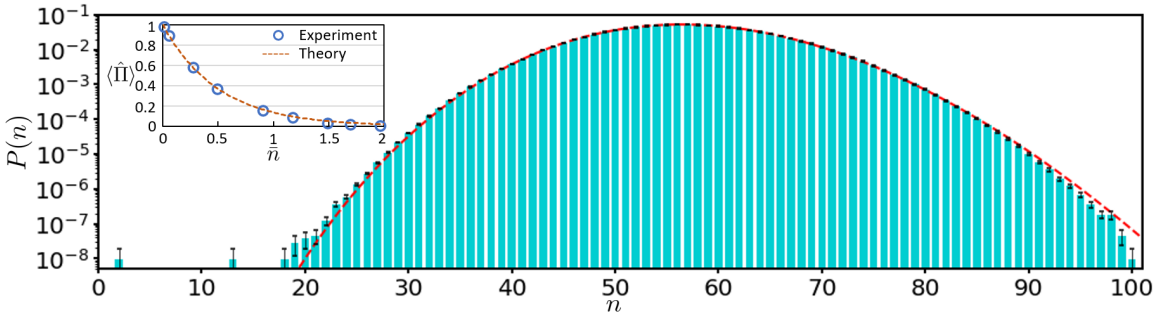


Figure 4.1: Experimental photon number distribution obtained by splitting a coherent state of mean photon number $\bar{n} = 57$ across three TES channels over 10^8 events. The red dashed line indicates the theoretical Poissonian distribution with a mean of 57. Error bars shown are of one SD and are obtained from finite sampling and photon-number binning errors. The plot inset shows the measured parity coherent states begins near one (vacuum) but tends to zero as the amplitude increases. The measured parity for the $\bar{n} = 57$ coherent state is $\langle\hat{\Pi}\rangle = -0.7 \times 10^{-4} \pm 1.0 \times 10^{-4}$.

If $\bar{n} = \langle\hat{n}\rangle$ is the mean photon number of the coherent state, then the expectation of parity is given by

$$\langle\hat{\Pi}\rangle = P_e - P_o = e^{-2\bar{n}}, \tag{4.2}$$

where P_e and P_o are the respective probabilities to detect either even or odd photon numbers.

In Fig. 4.1, we show the experimentally measured probability distribution for a large coherent state with $\bar{n} = 57$, which allows use to make full use of our PNRD and clearly resolve out to 100 photons. Although the theoretical parity of this state is $e^{-114} \sim 10^{-50}$, we cannot hope to reach this precision due to finite sampling. With 10^8 measurement events, we achieve a parity of zero to within uncertainty, with the measured value of $-0.7 \times 10^{-4} \pm 1.0 \times 10^{-4}$. Additionally, we first verify the parity of weaker coherent states as shown in the inset of Fig. 4.1. As expected, the parity of vacuum is 1, and we are clearly able to match the trend of $e^{-2\bar{n}}$ for increasing $\bar{n}$.

One unfortunate downside of a TES detection systems is the slow detector response leading to lower generation rates (12.5 kHz using mod 2 binning). Recent advances show that superconducting nanowire single-photon detectors (SNSPDs) have the po-

tential to be used as PNRDs that are orders of magnitude faster than TESs [90], but until this technology matures, we implement an alternative method to increasing random bit generation rates. As opposed to binning the photon number result by parity, a uniformly random distribution can also be obtained by taking the measurement result and binning according to photon-number modulo 2^d where $d \in \mathbb{Z}$. In this way, we can generate a bit string of size d for each measurement. As d increases, the residual bias of the QRNG still asymptotes to zero with increasing $\bar{n}$, but a larger coherent state amplitude is needed to achieve a similarly negligible bias. In this work with a maximum detection of 100 photons, we find that the residual bias for a coherent state with $\bar{n} = 57$ is equivalent for $d \in \{1, 2, 3\}$, so we use modulo 8 binning to generate random numbers.

We subject the $\sim 3 \times 10^8$ random bits generated by our protocol to a series of tests taken from the NIST suite of randomness tests [91]. The proportion (i.e. the percentage of tests that pass a given test) is plotted in Fig. 4.2 for each test, given a significance level of $\alpha = 0.01$. In computing the confidence interval for Fig. 4.2 (dashed blue lines), we do not make the standard approximation that the distribution of error about the binomially-weighted observation is given by that of a normal distribution, since our sample size is small enough that such an approximation will be unreliable. Instead we use the Wilson score (confidence) interval [92], which has been shown to be reliable for smaller sample sizes. The findings in Fig. 4.2 demonstrates that our measurements indicate randomness across all tests considered (all proportions lie above the lower confidence bound). We additionally show the results of randomness measures for binning with $d \in [1, 5]$ in the Extended Data.

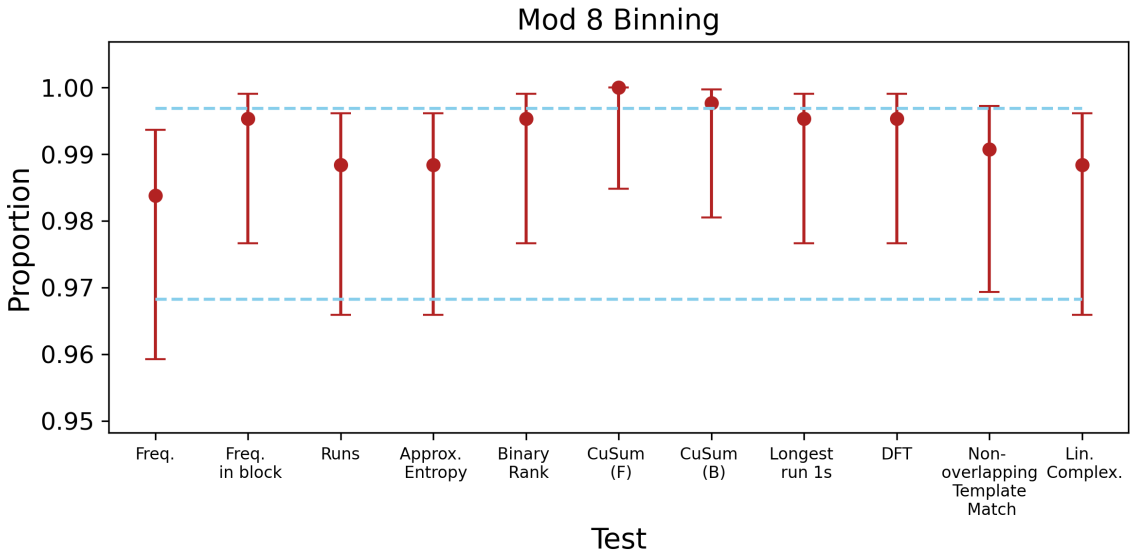


Figure 4.2: Randomness tests for the resultant bit strings from 10^8 events based on assigning three bits of information to each event by taking the measured photon number modulo 8. Data was broken into segments of 7.5×10^5 bits and each string was tested for randomness. The proportion (red markers), i.e. the percentage of trials that pass a test given a significance level of α=0.01, falls within the corresponding confidence interval for all tests considered indicating evidence of true randomness. The error bars for each proportion are computed from the Wilson score (confidence) interval of Eq. 4.26 where $n = 431$ is the total number of trials and n_s (n_f) are the number of successful (failed) trials for a significance level of $\alpha = 0.01$. Given repeated testing of the bit generation method, the error bars denote the probability range for which the proportion is likely to fall.

4.1.1 Robust nature of proposed method

Upon closer examination we can see how our method here proves to be quite robust against various sources of error. First, we can consider phase and amplitude fluctuations originating either from the laser or any other experimental instability. This can be modeled by assuming that a statistical mixture of coherent states impinges up the detector. We find that phase fluctuations have absolutely no bearing on the randomness and still lead to the same residual bias of $e^{-2\bar{n}}$, which we experimentally verify as shown in the Extended Data. Amplitude fluctuations similarly provide negligible impact. Suppose the coherent state has mean photon number of $\bar{n}$ and there is a small intensity fluctuation of δ. The expectation of parity becomes $e^{-2(\bar{n}\pm\delta)} \approx e^{-2\bar{n}}(1 \pm \delta)$ which tends to zero for sufficiently large $\bar{n}$.

Next, we can consider the effects of loss, detector inefficiency, and uneven splitting between the TES channels with imperfect beamsplitters. We can always model an inefficient detector by inserting a loss channel in the form of a beamsplitter of transmissivity η before a perfect detector and performing a partial trace over the unmeasured output port (Methods). As the coherent state, $|\alpha\rangle$, maps to the smaller coherent state, $|\sqrt{\eta}\alpha\rangle$, after this loss, an imperfect detector still measures a Poissonian photon-number distribution. Thus, in order to achieve quality randomness with low residual bias, the coherent state used must be chosen such that $\bar{n}' = \eta\bar{n}$ is sufficiently large. As for uneven splitting or differing detector efficiencies between channels, we can equivalently model the process of measuring a single coherent state distribution as the discrete convolution of three smaller coherent state distributions. As all beamsplitter outputs are still detected, changing the beamsplitter reflectivities just acts to redistribute the photons amongst the TES channels. Provided no single channel saturates, which is easily recognizable through monitoring areas measurements, sampling the summed output of all channels will still yield a Poissonian distribution.

An additional concern of any quantum mechanical experiment is that of unintentional coupling to the environment. One possible effect of such coupling is photon loss as addressed in the previous paragraph. Another effect is the addition of photons, such as coupling to an external thermal bath, or some malicious observer attempting to inject light. In place of measuring a coherent state, suppose that the detector is sent the density operator $\rho = \rho_\alpha \otimes \rho_{env}$, where $\rho_\alpha = |\alpha\rangle \langle\alpha|$ is the density operator for the coherent state and ρ_{env} is the density operator for some unknown quantum state, not necessarily pure, originating from the environment. The expectation value of parity for the whole system is given by $\langle e^{i\pi \sum \hat{n}_k} \rangle$, where subscript k denotes the different subsystems. This leads to an overall parity of

$$\langle \hat{\Pi} \rangle = e^{-2\bar{n}} \langle \hat{\Pi} \rangle_{env}, \tag{4.3}$$

where $\langle \hat{\Pi} \rangle_{env}$ is the parity of the environment alone and is bounded between 1 and -1. Thus environmental mixing will not degrade the quality of the QRNG.

As a final concern, consider an eavesdropper attempting to determine information about the random numbers. Suppose an eavesdropper uses a beamsplitter to sample the coherent light in an attempt to predict the random number measured by the user. Due to the nature of coherent states, the two beamsplitter outputs remain in a product state, hence are not correlated. Thus no information about the results at one output port can be used to determine the results at the other, preventing the eavesdropper from attaining useful information. This could be demonstrated by testing the random numbers generated by our three detection channels against each other (now each would have a lower $\bar{n}$ thus higher bias) for correlations. This robustness against eavesdropping is an advantage over simply sampling a Poisson noise distribution and splitting the classical signal afterwards, provided there is no technical noise. Other side-channel attacks, such as the insertion of different quantum

states by a nefarious party, can be readily mitigated as well. Although the QRNG method only utilizes higher order parity measurements, we still have access to the full photon-number distribution from the TES, which can be monitored to ensure that Poissonian statistics are still obtained. This rules out any external manipulation since replacing or interspersing the coherent state with a different state will yield a different distribution. Additionally, the TES waveform response can be concurrently monitored and frequently recalibrated to rule out signal manipulation. Finally, as a coherent state is simply a laser output, the source and detector can be fabricated in near proximity to one another and protected from any realistic attack through appropriate shielding.

Recently, there has been some emphasis on the use of Bell inequality violations to certify the quantum nature of a device and ensure private randomness [79, 93, 80]. Although this concept has merit, it requires closing all experimental loopholes to eliminate a local hidden variable theory before it can truly validate a black box as a quantum device. Furthermore, trust must be given at some point during any realistic experiment as the classical signal used to enact Bell measurements may themselves be spoofed. In our implementation, the quantum nature of the experiment is verified by the area histograms shown in Fig. 3.15(c). The origin of the separation between area measurements is the fundamental energy quantization of photons. An entirely classical signal would yield a single broad Gaussian peak centered about the average energy of the beam of light spanning a swath of areas due to classical noise fluctuations as opposed to the multiple Gaussian fits for each TES channel.

4.1.2 Theoretical background

Origin of randomness

The photon-number parity of a coherent state tends towards a uniform distribution as the energy of the state increases. For a coherent state given by $|\alpha\rangle = e^{-\frac{1}{2}\alpha^2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle$ and parity operator given by $\hat{\Pi} = (-1)^{\hat{n}} = e^{i\pi\hat{n}}$ where $\hat{n} = \hat{a}^\dagger\hat{a}$ is the photon-number operator. We can derive

$$\begin{aligned}
\langle\alpha|\hat{\Pi}|\alpha\rangle &= \langle\alpha| e^{i\pi\hat{n}} |\alpha\rangle \\
&= e^{-|\alpha|^2}\sum_{n,n'=0}^{\infty}\frac{\alpha^{*n'}\alpha^n}{\sqrt{n'!n!}}\langle n'| e^{i\pi\hat{n}} |n\rangle \\
&= e^{-|\alpha|^2}\sum_{n,n'=0}^{\infty}\frac{\alpha^{*n'}\alpha^n}{\sqrt{n'!n!}}e^{i\pi n}\langle n'|\,|n\rangle \\
&= e^{-|\alpha|^2}\sum_{n=0}^{\infty}\frac{(|\alpha|^2e^{i\pi})^n}{n!} \\
&= e^{-2\bar{n}}
\end{aligned}$$

where $\bar{n} = \langle\alpha|\,\hat{n}\,|\alpha\rangle = \alpha^2$.

From this we see that for large $\bar{n}$, the parity expectation value can be arbitrarily close to zero. To generate the random numbers we simply output '0' whenever we measure an even number or '1' whenever we measure odd.

Phase and amplitude fluctuations

First, we consider phase fluctuations. Suppose we do not have a pure coherent state, but a statistical mixture of coherent states with the same amplitude and a random phase,

$$\rho_{coh} = \frac{1}{2\pi}\int_0^{2\pi} d\phi\,|re^{i\phi}\rangle\langle re^{i\phi}|\,, \tag{4.4}$$

where $r = |\alpha| = \sqrt{\bar{n}}$. This yields

$$\begin{aligned}
\langle \hat{\Pi} \rangle &= \mathrm{Tr}[\rho_{coh} \hat{\Pi}] \\
&= \frac{1}{2\pi} \int_0^{2\pi} d\phi \sum_{n=0}^{\infty} \langle n | re^{i\phi} \rangle \langle re^{i\phi} | e^{i\pi \hat{n}} | n \rangle \\
&= \frac{1}{2\pi} \int_0^{2\pi} d\phi \sum_{n=0}^{\infty} e^{i\pi n} | \langle n | re^{i\phi} \rangle |^2 \\
&= \frac{1}{2\pi} \int_0^{2\pi} d\phi \sum_{n=0}^{\infty} (-1)^n \left| e^{-\frac{1}{2}\bar{n}} \sum_{i=0}^{\infty} \frac{(\sqrt{\bar{n}} e^{i\phi})^i}{\sqrt{i!}} \right|^2 \\
&= \frac{1}{2\pi} \int_0^{2\pi} d\phi \sum_{n=0}^{\infty} (-1)^n e^{-\bar{n}} \frac{\bar{n}^n}{n!} \\
&= e^{-2\bar{n}}
\end{aligned}$$

which shows that phase noise does not affect the parity expectation value. Second, we consider amplitude fluctuations. Changes in the amplitude of the coherent state amount to changes in the mean photon number $\bar{n}$. For a change δ in the mean photon number, the parity expectation value becomes $e^{-2(\bar{n} \pm \delta)}$ which is approximately $e^{-2\bar{n}}$ for small δ. This can be shown explicitly by following a calculation similar to the one above but for amplitude. Here we start by using $\rho_{coh} = \int_{\alpha_0 - \delta}^{\alpha_0 + \delta} d\alpha \, |\alpha\rangle \langle \alpha|$. Following the derivation we end with $\int_{\alpha_0 - \delta}^{\alpha_0 + \delta} d\alpha e^{-2|\alpha|^2}$ which can be calculated numerically, and goes to zero for $\delta \ll \alpha_0$.

Environmental noise

We now look at the expectation value of the parity operator on the whole system where $\rho = \rho_{coh} \otimes \rho_{env}$ with $\rho_{coh} = |\alpha\rangle \langle \alpha|$. Deriving the expectation value of the new parity operator, $e^{i\pi \sum \hat{n}_i}$, where subscript i denotes the different subsystems, we

obtain

$$\begin{aligned}\langle e^{i\pi\sum\hat{n}_i}\rangle &= Tr[e^{i\pi\hat{n}_1}\rho_{coh}\otimes e^{i\pi\hat{n}_2}\rho_{env}]\\ &= Tr[\langle\alpha|\, e^{i\pi\hat{n}_1}\,|\alpha\rangle\otimes e^{i\pi\hat{n}_2}\rho_{env}]\\ &= Tr[e^{-2\bar{n}}\otimes e^{i\pi\hat{n}_2}\rho_{env}]\\ &= e^{-2\bar{n}}\langle\hat{\Pi}\rangle_{env},\end{aligned}$$

where $\langle\hat{\Pi}\rangle_{env}$ is bounded between 1 and -1. For large enough $\bar{n}$, the whole expectation value goes to zero regardless of the form of ρ_{env}.

Loss and detector inefficiency

Consider an imperfect detector with quantum efficiency $\eta < 1$. This can be modeled by placing a fictitious 'loss beamsplitter' with reflection coefficient $r = \sqrt{1-\eta}$ and transmission coefficient $t = \sqrt{\eta}$ such that $r^2 + t^2 = 1$ in front of a perfect detector and performing a partial trace over the reflected mode. The beamsplitter operator acting on bosonic modes a and b is given by

$$\hat{B}_{ab} = e^{\theta(\hat{a}\hat{b}^\dagger - \hat{a}^\dagger\hat{b})}, \tag{4.5}$$

where $r = \cos\theta$, $t = \sin\theta$. Sending a coherent state, $|\alpha\rangle$, to an imperfect detector is then the same as sending the density operator

$$\rho = \mathrm{Tr}_b\left[\hat{B}_{ab}\left(|\alpha\rangle\langle\alpha|\right)_a\otimes\left(|0\rangle\langle 0|\right)_b\hat{B}^\dagger_{ab}\right] \tag{4.6}$$

$$= \mathrm{Tr}_b\left[\left(|\sqrt{\eta}\alpha\rangle\langle\sqrt{\eta}\alpha|\right)_a\otimes\left(|\sqrt{1-\eta}\alpha\rangle\langle\sqrt{1-\eta}\alpha|\right)_b\right] \tag{4.7}$$

$$= \left(|\sqrt{\eta}\alpha\rangle\langle\sqrt{\eta}\alpha|\right)_a \tag{4.8}$$

to a perfect detector. Thus, for coherent states, all measurements made with PNRDs having $\eta < 1$ can instead be treated as ideal detectors where the measured state is just a different coherent state.

Unbalanced splitting and efficiency

Suppose we send the coherent state $|\alpha\rangle$ to our three-detector system. Due to unbalanced splitting between different paths or small variations in detector efficiency, each TES may see a different signal. Together, the statistics of the photon number summed across all three channels will still be that of a coherent state but with potentially different effective amplitude.

For an input coherent state and vacuum in the unused beamsplitter ports, $|\alpha\rangle_a |0\rangle_b |0\rangle_c$, the beamsplitter system shown in Fig. 3.15(a) transforms the state to

$$\hat{B}_{ac}\hat{B}_{ab} |\alpha\rangle_a |0\rangle_b |0\rangle_c = |t_1 t_2 \alpha\rangle_a |r_1 \alpha\rangle_b |t_1 r_2 \alpha\rangle_c , \tag{4.9}$$

where r_k, t_k are the beamsplitter coefficients for beamsplitter k. Suppose now that the three detectors have quantum efficiencies η_a, η_b, and η_c. Using Eq. 4.6 for each mode, the effective state sent to three perfect detectors is then

$$|\psi\rangle = |\beta_a\rangle_a |\beta_b\rangle_b |\beta_c\rangle_c \tag{4.10}$$

$$= e^{-\frac{1}{2}|\beta_a\beta_b\beta_c|^2} \sum_{n_a=0}^{\infty}\sum_{n_b=0}^{\infty}\sum_{n_c=0}^{\infty} \frac{\beta_a^{n_a}\beta_b^{n_b}\beta_c^{n_c}}{\sqrt{n_a! n_b! n_c!}} |n_a\rangle_a |n_b\rangle_b |n_c\rangle_c \tag{4.11}$$

where

$$\beta_a = \sqrt{\eta_a} t_1 t_2 \alpha, \tag{4.12}$$

$$\beta_b = \sqrt{\eta_b} r_1 \alpha, \tag{4.13}$$

$$\beta_c = \sqrt{\eta_c} t_1 r_2 \alpha. \tag{4.14}$$

The probability to measure the total photon number summed across all detectors, $m = n_a + n_b + n_c$, is given by

$$P(m) = e^{-|\beta_a \beta_b \beta_c|^2} \sum_{n_a=0}^{m} \sum_{n_b=0}^{m-n_a} \frac{|\beta_a|^{2n_a} |\beta_b|^{2n_b} |\beta_c|^{2(m-n_a-n_b)}}{n_a! n_b! (m-n_a-n_b)!} \tag{4.15}$$

$$= e^{-|\beta_a \beta_b \beta_c|^2} \frac{\left(|\beta_a|^2 + |\beta_b|^2 + |\beta_c|^2\right)^m}{m!}, \tag{4.16}$$

which is the same probability distribution that would be obtained by measuring a coherent state of amplitude $\alpha' = \sqrt{|\beta_a|^2 + |\beta_b|^2 + |\beta_c|^2}$ with a single detector of efficiency $\eta = 1$.

4.1.3 Experimental considerations

Randomness characterization

Here we will follow the work detailed in [89] on how the photon-number counts were binned to generate multiplicatively longer bit sequences as well as how the bit sequence was tested for randomness. We start with the case of mod(2) binning, in which each detection event corresponds to an outcome of even(0) or odd(1), the measurement probabilities are given by

$$P^{(2)}_{0(1)} = \langle \hat{P}^{(2)}_{0(1)} \rangle = \tfrac{1}{2} \left(1 \pm e^{-2\bar{n}}\right) \quad \rightarrow \quad P^{(2)}_k = \tfrac{1}{2} \left(1 + (-1)^k e^{-2\bar{n}}\right), \tag{4.17}$$

where $\bar{n}$ is the average photon number of the coherent state and

$$\hat{P}_k^{(2)} = \sum_{m=0}^{\infty} |2m+k\rangle \langle 2m+k| , \tag{4.18}$$

are the even (k=0) and odd (k=1) projection operators. For large average photon numbers, the balancement between even/odd probabilities is maintained (i.e. $e^{-2\bar{n}} \to 0$). In terms of these projectors, the corresponding parity operator is given by $\hat{\Pi} = \hat{P}_0^{(2)} - \hat{P}_1^{(2)}$. Similarly, we can define projectors for the case of mod(4) binning

$$\hat{P}_k^{(4)} = \sum_{m=0}^{\infty} |4m+k\rangle \langle 4m+k| , \tag{4.19}$$

where each mod(2) bin is further broken down into bins containing every other even/odd photon count. For example, the $k = 0$ bin is comprised of the photon number counts $\{0, 4, 8, ...\}$ while the $k = 2$ bins counts $\{2, 6, 10, ..\}$ and likewise for the odd counts. In this sense, mod(4) binning is akin to a higher order parity measurement. It is clear then that the parity operator can be expressed as

$$\hat{\Pi} = \hat{P}_0^{(4)} + \hat{P}_2^{(4)} - \left(\hat{P}_1^{(4)} + \hat{P}_3^{(4)}\right) \equiv \hat{P}_0^{(2)} - \hat{P}_1^{(2)}, \tag{4.20}$$

and the binning probabilities are in turn given by

$$\begin{aligned} P_k^{(4)} = \langle \hat{P}_k^{(4)} \rangle &= e^{-\bar{n}} \sum_{n=0}^{\infty} \frac{\bar{n}^{4n+k}}{(4n+k)!} \\ &= \frac{1}{4}\left(1 + 2e^{-\bar{n}} \cos\left(\bar{n} - \tfrac{k\pi}{2}\right) + (-1)^k e^{-2\bar{n}}\right). \end{aligned} \tag{4.21}$$

The length of the bit sequence can then be made longer by taking the remainders and mapping them to the dual-bit values according to $\{0, 1, 2, 3\} \to \{00, 01, 10, 11\}$. This same form of mapping holds for higher modulo binning. Note the largest biasing term in Eq. 4.21 is larger than the mod(2) biasing term by a square root. This implies

a trade-off when binning the data: larger bit sequence generation comes at the cost of requiring a higher coherent state average photon number. This procedure can be generalized for mod(Q) where the projectors are given by

$$\hat{P}_k^{(Q)} = \sum_{m=0}^{\infty} |Qm+k\rangle \langle Qm+k| , \tag{4.22}$$

and the corresponding parity operator can in turn be constructed as

$$\hat{\Pi} = \sum_{k=0}^{Q-1} (-1)^k \hat{P}_k^{(Q)} \equiv \hat{P}_0^{(2)} - \hat{P}_1^{(2)}. \tag{4.23}$$

The tested data is based off of 107911769 photon-number counts from a coherent source of average photon number $\bar{n} \approx 57$. For a trial size of 7.5×10^5, this corresponds to $n = \{143, 287, 431, 575, 719\}$ trials for mod$\{2, 4, 8, 16, 32\}$, respectively. We subject this data to a suite of randomness tests outlined by NIST SP800-22 [91] in order to demonstrate that the generated bit sequence is truly random. We note that our methodology for determining randomness is the same employed in testing the randomness of bit sequences generated using the protocols of the NIST encryption standard competition finalists, detailed in Soto *et al.* [94], utilized in the verification of new randomness tests by Doğanaksoy *et al.* [95] and implemented in the cryptographically-secure Intrinsic ID Zign software-based RNG [96]. In Fig. 4.4 we plot the results of these tests for mod$\{2, 4, 16, 32\}$. Note the mod(8) result can be found within the main body text. Due to the large number of tests available for judging whether a sequence is random or not, there is no 'complete' or systematic approach to proving randomness. Instead, one relies on providing sufficient evidence that a given sequence is indeed random. For each trial, a series of tests are performed and a P-value is obtained for each test corresponding to the probability that a perfect random number generator would produce a sequence *less* random than the sequence being tested. If this P-value is greater than the chosen significance level of $\alpha = 0.01$

(1%), the test is considered passed (successful) and the trial is accepted as random. The proportion is then defined as the ratio of successful trials to the total number of trials (i.e. the success rate). Included in our analysis is the confidence interval (CI), i.e. the range of estimation for the success rate of a particular test given a 99% confidence level. Typically, the CI for a set of Bernoulli trials with a success rate of $\hat{p}$ can be fairly approximated by that of the normal distribution

$$\mathrm{CI} \approx \hat{p} \pm z\sqrt{\frac{\hat{p}\,(1-\hat{p})}{n}}, \tag{4.24}$$

where n is the total number of trials and z is the $1-\frac{\alpha}{2}$ quantile probit function (i.e. the inverse cumulative distribution function for the normal distribution). However, this approximation to the binomial distribution, which is more representative of a set of Bernoulli trials, is only valid when the number of trials is on the order of $n \gtrsim 10^4$ and/or where the success rates are sufficiently far away from the boundary values of $0, 1$. This proves to be an insufficient approximation for our data. We instead turn to the asymmetric Wilson score approximation [92] to the normal distribution given by

$$\mathrm{CI}_{\mathrm{ws}} = \frac{n}{n+z^2}\left(\hat{p} + \frac{z^2}{2n}\right) \pm \frac{zn}{n+z^2}\sqrt{\frac{\hat{p}\,(1-\hat{p})}{n} + \frac{z^2}{4n^2}}. \tag{4.25}$$

The Wilson score confidence interval, $\mathrm{CI}_{\mathrm{ws}}$, for a 99% confidence level are represented by horizontal dashed blue lines in Figs. 4.2, 4.4 and 4.5. In addition, we plot for each test the equivalent definition of the $\mathrm{CI}_{\mathrm{ws}}$

$$\mathrm{CI}_{\mathrm{ws}} = \frac{n_s + \frac{1}{2}z^2}{n+z^2} \pm \frac{z}{n+z^2}\sqrt{\frac{n_s n_f}{n} + \frac{z^2}{4}}, \tag{4.26}$$

where $n_s, n_f = n - n_s$ are the number of successful and failed trials, respectively. The success rate is then given by $\hat{p} = n_s/n$. This measure provides a range for each test in which the mean proportion is likely to fall given repeated testing of the bit

generation method (i.e. more trials performed) and are represented by red error bars in Figs. 4.2, 4.4 and 4.5. Sufficient evidence of randomness exists if the proportion lies above the lower bound of the $\mathrm{CI}_{\mathrm{ws}}$ for all tests considered. By this criterion, we conclude that the generated bit sequence for the cases of mod$\{2, 4, 8\}$ binning are random while the generated bit sequence for mod$\{16, 32, ..\}$ binning are not random.

To further validate our results, we reiterate that for the case of a coherent state with average photon number $\bar{n} \approx 57$, we expect the balancement of binning probabilities to hold for up to mod(8) binning. Higher modulo binning will introduce larger degrees of bias into the binning probabilities, as seen in Eq. 4.21. An approximate trend is that the largest biasing term in the binning probabilities for the case of mod(Q) binning is $\propto \exp\left(-\frac{4\bar{n}}{Q}\right)$, such that if one wanted to maintain the same degree of bias as the mod(2) binning case, one would need a coherent state with an average photon number $\frac{1}{2}Q$ times larger. For a static $\bar{n}$, higher mod binning will subsequently result in a generated bit sequence that does not display randomness as there will be a significant amount of bias in the higher-modulo binning probabilities. For reference, the impact of bias on the randomness of the bit sequence is reflected in Fig. 4.4, where as predicted the mod(16) and mod(32) binning cases show evidence that the generated bit sequence is *not* random since for both cases several test proportions fall outside of the $\mathrm{CI}_{\mathrm{ws}}$. Even more specifically, only a few tests fail for the mod(16) case and most fail for the mod(32), reflecting that more bias is introduced as a function of the modulo binning size. Likewise, this also further strengthens the argument that the mod$\{2, 4, 8\}$ cases result in a random bit sequence, as our experimental data align perfectly with theoretical predictions.

Phase randomization

Fig. 4.5 in the Extended Data shows the randomness tests for data where phase noise has been introduced to the coherent state. This is achieved by driving a mirror-mounted piezoelectric actuator (PZT) to change the optical path length over a range of one wavelength, or 1064 nm. The PZT was driven with a 100 Hz triangle-wave function, which was chosen to be much slower than the pulse repetition rate to ensure all phases over the range from 0 to 2π where equally represented amongst the entire data set.

Extended Data

Further analyses of experimental data are shown in the figures below. Theoretical residual bias for photon-number measurements modulo d with an upper limit of 100 resolveable photons are shown in Fig. 4.3, and full characterization of the randomness tests on all data is shown in Figs. 4.4 and 4.5.

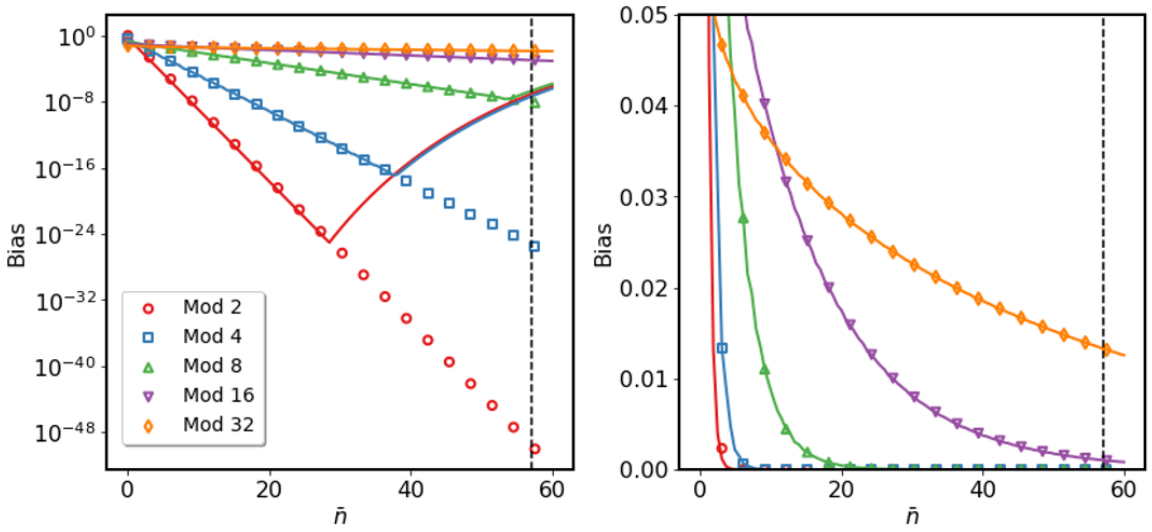


Figure 4.3: Residual bias based on modulo binning of a photon number distribution for coherent state of mean photon number $\bar{n}$. Markers indicate the theoretical deviation from a uniformly random distribution if one had infinite photon-number resolving capability while solid lines give the expected bias with a truncation of the photon number distribution beyond 100 photons. The vertical dashed line indicates a coherent state with $\bar{n} = 57$ such as used in this experiment where the residual bias for mod 2, mod 4, and mod 8 binning are the same. The two plots are identical with the plot at left showing log scale.

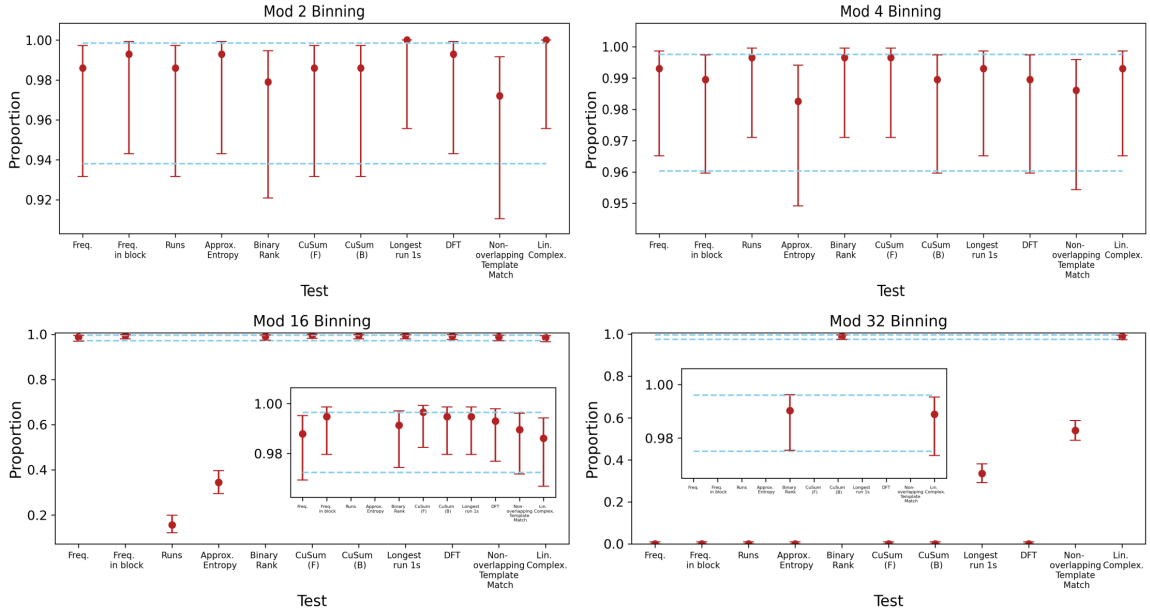


Figure 4.4: Randomness tests for the resultant bit strings based on how the measured data is binned (Mod 8 data shown in the main text). Mod 2, Mod 4, and Mod 8 tests all indicate randomness, while some tests begin to fail for Mod 16 and Mod 32. This is expected due to the non-zero residual biases for a coherent state distribution with mean photon number $\bar{n} = 57$ and a PNRD limit of 100 photons. The error bars for each proportion are computed from the Wilson score (confidence) interval of Eq. 4.26 where $n = \{143, 287, 575, 719\}$ is the total number of trials for mod$\{2, 4, 16, 32\}$ binning, respectively, and n_s (n_f) are the number of successful (failed) trials for a significance level of $\alpha = 0.01$. Given repeated testing of the bit generation method, the error bars denote the probability range for which the proportion is likely to fall.

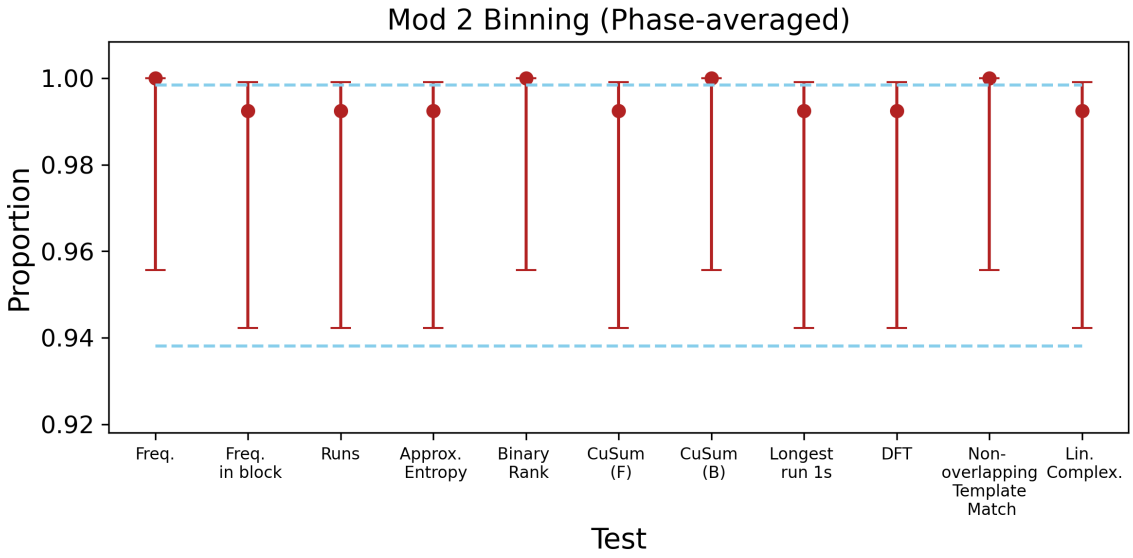


Figure 4.5: Randomness tests for bit strings obtained from modulo 2 binning the sampled photon number from a mixture of coherent states with randomized phase. All tests pass indicating phase stability has no bearing on the quality of QRNG. The error bars for each proportion are computed from the Wilson score interval of Eq. 4.26 where $n = 143$ is the total number of trials and n_s (n_f) are the number of successful (failed) trials for a significance level of $\alpha = 0.01$. Given repeated testing of the bit generation method, the error bars denote the probability range for which the proportion is likely to fall.

4.1.4 Summary

In this section I have presented my work on implementing a quantum random number generator. My goal was to demonstrate a use case of our newly achieved 100 photon resolution capability and I have successfully achieved that.

- I was able to theoretically model the QRNG and show where the randomness comes from and how it is robust to various potential impediments.
- I was able to successfully experimentally generate truly random numbers that passed the NIST randomness tests.

4.2 Fock State Interferometry (FSI)

The ability to distinguish between apriori-known phase shifts has many applications including M-ary Phase Shift Keying (MPSK), a digital modulation scheme that conveys M messages by modulating the optical phase of a probe signal [97] and quantum reading with binary phase-encoded memory pixels [98, 99]. One technique to perform such a measurement is using Fock state interferometry (FSI), a Mach-Zehnder interferometer whose inputs are Fock states and whose outputs are measured using photon number resolving detection (PNRD).[30]. Such a setup is outlined in Fig. 4.6. It is recommended that the reader reviews [30] for a more detailed explanation of the FSI method. Below is a breif overview.

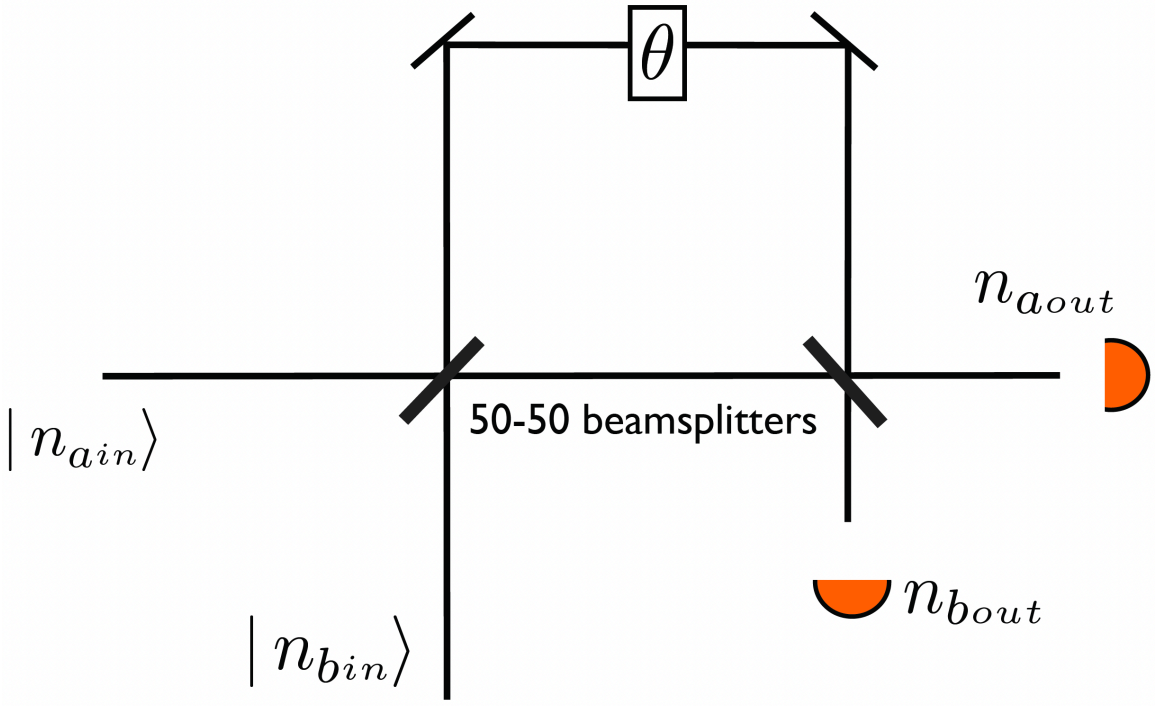


Figure 4.6: Figure from [30]. Phase discrimination by Fock-state interferometry. The Fock state $|n_a\rangle_a |n_b\rangle_b$ is input into a Mach-Zehnder interferometer of phase difference θ and the interferometer's output is measured by photon-number- resolving detectors.

Classically, with coherent state inputs for instance, the phase measurement sensitivity cannot exceed the beamsplitter shot-noise level $\Delta\theta_{cl} \sim \langle N\rangle^{-\frac{1}{2}}$[100], where θ is the

phase difference between the arms of an interferometer and $\langle N \rangle$ is the total average number of photons in the interferometer. The classical limit, however, doesn't give the ultimate phase precision, which is fixed by the Heisenberg number-phase Heisenberg inequality [101] and bounded by the Heisenberg limit (HL): $\Delta\theta_{Hl} \sim \langle N \rangle^{-1}$.

FSI can yield enhanced interferometry performance and break the classical limit in cases less general than the estimation of an unknown phase, namely the discrimination of two or more predetermined phase shifts [30]. In this section I will highlight the results in [30] examining the ideal (lossless) case and provide an analysis of the lossy situation.

4.2.1 Lossless FSI

Schwinger representation

Shahrokhshahi et al. in [30] use the Schwinger representation to model the interferometer setup, which was first demonstrated by Yurke et al in [102]. The analysis in [30] goes as follows:

Any linear passive lossless optical device with two input and two output ports can be described by a 2×2 SU(2) matrix:

$$U = \begin{pmatrix} \cos\frac{\beta}{2} e^{i(\alpha+\gamma)/2} & \sin\frac{\beta}{2} e^{i(\alpha-\gamma)/2} \\ -\sin\frac{\beta}{2} e^{-i(\alpha+\gamma)/2} & \cos\frac{\beta}{2} e^{-i(\alpha+\gamma)/2} \end{pmatrix} \tag{4.27}$$

where α, β and γ are the Euler angles. U operates on the two-dimensional vector $(a, b)^T$, whose components are the annihilation operators for the two input fields at each port of the system.

The homomorphism from SU(2) to the rotation group in three dimensions, SO(3),

allows us to visualize the action of two-mode optical devices, such as beam splitters and phase shifters, as rotations in 3D space. The general rotation in Eq. 4.27 is mathematically equivalent to the rotation of the following tridimensional vector $\vec{J}$ in 3D space:

$$J = \begin{pmatrix} J_x \\ J_y \\ J_z \end{pmatrix} = \frac{1}{2} \begin{pmatrix} a^\dagger b + b^\dagger a \\ -i(a^\dagger b - b^\dagger a) \\ a^\dagger a - b^\dagger b \end{pmatrix}. \tag{4.28}$$

Components J_x, J_y and J_z follow the canonical commutation relations for quantum angular momentum operators

$$[J_k, J_l] = i\hbar\varepsilon_{klm} J_m \tag{4.29}$$

where $k, l, m \in \{x, y, z\}$, and ε_{klm} is the Levi-Civita symbol. So $\vec{J}$ can be deemed a quantum angular momentum, or effective spin.

The magnitude of the angular momentum J^2 is

$$J^2 = J_x^2 + J_y^2 + J_z^2 = \frac{a^\dagger a + b^\dagger b}{2}\left(\frac{a^\dagger a + b^\dagger b}{2} + 1\right) \tag{4.30}$$

$$J^2 = \frac{N}{2}\left(\frac{N}{2} + 1\right) \tag{4.31}$$

where

$$N = N_a + N_b = a^\dagger a + b^\dagger b \tag{4.32}$$

is the total photon number operator.

Fock states $|n_a\rangle |n_b\rangle$ are therefore also eigenstates of J^2 and J_z,

$$|j\mu\rangle_z = |n_a\rangle_a |n_b\rangle_b \tag{4.33}$$

with respective eigenvalues $j(j+1)$ and μ given by the total photon number and the

photon number difference

$$j = \frac{n_a + n_b}{2} \tag{4.34}$$

$$\mu = \frac{n_a - n_b}{2} \tag{4.35}$$

As an example, input state of the interferometer with $2j$ photons in mode a and vacuum in mode b is identical to, $|2j\rangle_a |0\rangle_b = |jj\rangle_z$ and the twin Fock state input which is required for Holland-Burnett interferometry [103] is $|j\rangle_a |j\rangle_b = |j0\rangle_z$.

A unitary operation on the quantum fields a and b can be viewed as the SO(3) rotation of the corresponding spin $\vec{J}$, Eq. 4.28. Any rotation of spin $\vec{J}$ can be described with the 3 Euler rotations:

$$\vec{J}^{\text{out}} = e^{i\alpha J_z} e^{i\beta J_y} e^{i\gamma J_z} \vec{J}^{\text{in}} e^{-i\gamma J_z} e^{-i\beta J_y} e^{-i\alpha J_z} \tag{4.36}$$

$$|\psi\rangle_{\text{out}} = e^{i\alpha J_z} e^{i\beta J_y} e^{i\gamma J_z} |\psi\rangle_{in} \tag{4.37}$$

respectively in the Heisenberg and Schrodinger pictures. In the Schwinger representation this arbitrary tridimensional rotation of the effective spin $\vec{J}^{\text{in}}$ is equivalent to the Euler angle parametrization of the SU(2) rotation of the two modes a and b basis, Eq. 4.27. The SO(3) Euler matrix is

$$\begin{pmatrix} c_\alpha c_\beta c_\gamma - s_\alpha s_\gamma & -c_\gamma s_\alpha - c_\alpha c_\beta s_\gamma & c_\alpha s_\beta \\ c_\alpha s_\gamma + c_\beta c_\gamma s_\alpha & c_\alpha c_\gamma - c_\beta s_\alpha s_\gamma & s_\alpha s_\beta \\ -c_\gamma s_\beta & s_\beta s_\gamma & c_\beta \end{pmatrix} \tag{4.38}$$

where $c_{(\alpha/\beta,\gamma)} = \cos(\alpha/\beta, \gamma)$, $s_{(\alpha/\beta,\gamma)} = \sin(\alpha/\beta, \gamma)$. The Mach-Zehnder Interferometer (MZI) consists of two 50/50 beam splitters, and a phase shifter. The effect of MZI is equivalent to a $(-\pi/2)$ rotation around x axis, a θ rotation around z, and another

$\pi/2$ rotation around x, which yields a θ rotation around y

$$\vec{J}^{\text{out}} = e^{i\theta J_y} \vec{J}^{\text{in}} e^{-i\theta J_y} \tag{4.39}$$

$$|\psi_{\text{out}}\rangle = e^{i\theta J_y} |\psi_{in}\rangle \tag{4.40}$$

So the effect of MZI is equivalent to a single rotation of effective spin by θ around the y axis. We are interested on the effect of MZI on Fock states, the eigenstates of effective spin $\vec{J}$, $|j, \mu\rangle$. The probability function $P(\mu', \mu|\theta, j)$ for the input spin $|j, \mu\rangle$ to be measured after the interferometer as $|j, \mu'\rangle$ for fixed θ and J (the total photon number) can be described as a rotation matrix, which is a square matrix of dimension $2j + 1$ with general element

$$P(\mu', \mu|\theta, j) = |\langle j, \mu'|\psi_{\text{out}}\rangle|^2 \tag{4.41}$$

$$= |\langle j, \mu'|e^{i\theta J_y}|j\mu\rangle_z|^2 \tag{4.42}$$

$$= d^j_{\mu',\mu}(\theta)^2 \tag{4.43}$$

These rotation matrix elements can be expressed in terms of Jacobi polynomials

$$d^j_{\mu',\mu}(\theta) = \left[\frac{(j+\mu)!(j-\mu)!}{(j+\mu')!(j-\mu')!}\right]^{1/2} \left(\sin\frac{\beta}{2}\right)^{\mu-\mu'} \times \left(\cos\frac{\beta}{2}\right)^{\mu+\mu'} P_{j-\mu}^{(\mu-\mu',\mu+\mu')}(\cos\beta) \tag{4.44}$$

Phase discrimination

Let's start with binary phase discrimination where the unknown fixed phase θ can take one of two values: θ_1 and θ_2. We shall denote the estimated phase as $\hat{\theta}$. Four different scenarios can occur during the phase discrimination process. If the initial phase $\theta = \theta_{1,2}$ and the estimated phase $\hat{\theta} = \theta_{1,2}$, respectively, then we have success.

Else $\hat{\theta} = \theta_{2,1}$, and we have an error. A natural criterion to measure interferometer performance in the phase discrimination problem will then be the error probability, P_e, which we'll define later.

We consider a MZI with a $|j\mu\rangle$ input and whose phase θ can be either of two predetermined values $\theta_{1,2}$. We then perform a single J_z measurement of the photon number difference at the output ports, of result μ', and make a decision about the phase shift based on maximum likelihood algorithm: knowing the probability distribution $P(\mu', \mu|\theta)$ of the interferometer (Table 4.1), we compare both cases $\theta = \theta_1$ and $\theta = \theta_2$ for a given measurement outcome and assign the estimated phase shift $\hat{\theta}$ to the phase which is more likely to result in this specific outcome μ'. The algorithm is thus

$$\begin{aligned}
&\text{if } P(\mu', \mu|\theta_1) \geqslant P(\mu', \mu|\theta_2) \\
&\text{then} \begin{cases} P(\hat{\theta} = \theta_1|\theta = \theta_1) = P(\mu', \mu|\theta_1) & -\text{success} \\ P(\hat{\theta} = \theta_1|\theta = \theta_2) = P(\mu', \mu|\theta_2) & -\text{failure} \end{cases} \\
&\text{else} \begin{cases} P(\hat{\theta} = \theta_2|\theta = \theta_2) = P(\mu', \mu|\theta_2) & -\text{success} \\ P(\hat{\theta} = \theta_2|\theta = \theta_1) = P(\mu', \mu|\theta_1) & -\text{failure} \end{cases}
\end{aligned} \tag{4.45}$$

Table 4.1: Probability distribution $P(\mu', \mu|\theta)$. The possible measurement outcomes are denoted by μ' (columns) and possible phases by $\theta_{1,2}$ (rows). Each element of this array is the probability of measuring $\mu' \in [-j, j]$, given phase θ.

θ \ μ'	$-j$	$\cdots$	m	$\cdots$	j
θ_1	$P(-j, \mu\|\theta_1)$	$\cdots$	$P(m, \mu\|\theta_1)$	$\cdots$	$P(j, \mu\|\theta_1)$
θ_2	$P(-j, \mu\|\theta_2)$	$\cdots$	$P(m, \mu\|\theta_2)$	$\cdots$	$P(j, \mu\|\theta_2)$

For this procedure to be error free, one would need:

$$P(\hat{\theta} = \theta_{1,2}|\theta = \theta_{2,1}) = 0. \tag{4.46}$$

Of course, this is not the case in general, and the average error probability is given

by:

$$P_e = \sum_{i,j\neq i} P(\theta_i) P(\hat{\theta} = \theta_j | \theta = \theta_i). \tag{4.47}$$

The analytic expressions of probabilities are given by rotation matrix elements in the Schwinger representation, Eq. 4.43. Without loss of generality, we may elect to set $\theta_1 = 0$ as this entails

$$P(\mu', \mu|0) = d^j_{\mu',\mu}(0)^2 = \delta_{\mu',\mu} \tag{4.48}$$

and simplifies the situation. The problem will then reduce to discriminating $\theta_2 = \theta$ against $\theta_1 = 0$. Note that this is still different from general phase estimation – again classically-limited for a FSI – as we'll restrict θ to the values that will allow optimized performance.

Next, let's now turn to the extension of the previous problem to discriminating three phases $(0, \theta_1, \theta_2)$ – one of them being, again, set to zero for convenience and without loss of generality. Again, the error probability (P_e), is a natural criterion to assess the performance of the phase discrimination. For all phases equiprobable, the error probability is, from Eq. 4.47,

$$\begin{aligned} P_e = \frac{1}{3} [&P(0|\theta_1) + P(0|\theta_2) + P(\theta_1|0) \\ &+ P(\theta_1|\theta_2) + P(\theta_2|0) + P(\theta_2|\theta_1)] \end{aligned} \tag{4.49}$$

Information theory

A few definitions that will be used to benchmark our setup are:

The mutual information (MI), which is a measure of the amount of information that one random variable X contains about another random variable Y, is equivalent to the reduction in the uncertainty of one random variable due to the knowledge of the

other. It is given in this case by:

$$I(\theta;\hat{\theta}) = \log_2 M + \sum_{i,j} \frac{P(\hat{\theta}_j \mid \theta_i)}{M} \log_2 \frac{P(\hat{\theta}_j \mid \theta_i)}{\sum_k P(\hat{\theta}_j \mid \theta_k)} \tag{4.50}$$

where M is the number of possible optical phases, and $P(\hat{\theta}_j \mid \theta_i)$ is the conditional probability of measuring $\hat{\theta}_j$ given that θ_i occurred. Please note that Eq. 4.50 is different from Eq.(B16) in [30] by a sign difference. The error in [30] began starting from Eq.(B13). Eq. 4.50 is correct.

Next, the classical capacity of optical reading is the amount of bits of information that can be reliably encoded and read per pixel and is equivalent to the maximum attainable mutual information between the applied phase shifts θ and the measured phase shifts $\hat{\theta}$ for each pixel,

$$C(n_s) = \max I(\theta;\hat{\theta}), \tag{4.51}$$

where n_s is the average number of signal photons in the reading probe, here the interferometer arm that contains the phase shift.

Photon information efficiency (PIE) is then the number of bits read per signal photons:

$$\text{PIE} = \frac{C(n_s)}{n_s}. \tag{4.52}$$

4.2.2 Lossy FSI

Our aim now is to derive a formula for the probability of measuring an output $|j', \mu'\rangle$ on the other side of the FSI apparatus for an input state $|j, \mu\rangle$ taking into account losses. This is ultimately deriving the lossy equivalent of Eq. 4.43.

Adding beamsplitters before detectors vs using Krauss operators

There are two ways to go about modeling losses due to interaction with the environment in this case. The first seems conceptually straight forward: We assume that interaction is modeled as going through two beamsplitters before the two detectors at the end of our experiment with transmissivity η. The inputs at those beamsplitters would be our output state from the regular lossless FSI and vacuum(the environment). What we do next is calculate the output (now 4-mode) state and construct a density matrix from it. We then take the partial trace of the density matrix over the environment modes. What is left is our sub-system's density matrix after loss. Finally, we take the expectation value of the resulting density matrix in whatever state we like to get the probability of being in that particular state.

The other way to get the sub-system's density matrix after loss is to say that whatever the effect of loss is, it is modeled by some operator K that will transform our original density matrix into the lossy version.

The Krauss operator

Let us forget about the FSI setup for now and consider the following: We send a single-mode Fock state through some lossy region and want to get the output state. It's important to remember that losses come about because our state interacts with its environment. We model this loss by some operator K that will transform our input density matrix as:

$$\rho_{out} = \sum_k K_k \rho_{in} K_k^\dagger \tag{4.53}$$

where K_k is called a Krauss operator[104].

The summation index k here represents different possible final states of the 'environment' that we interacted with. We model the environment here as a simple harmonic oscillator in the number basis. Like the previous method, we start from vacuum, but end in some state k. From this we understand that k is the number of photons lost from our input state. The action of the operator K on the input mode is whatever action that remains after we evolve the environment (initially in vacuum) and project it onto its possible outcome state $\langle k|$ with our evolution operator. This can be written as:

$$K_k = \langle k|_b \, e^{itH_I} \, |0\rangle_b \tag{4.54}$$

where H_I is the interaction Hamiltonian of the input state with the environment. Subtitle a denotes input mode and subtitle b denotes environment mode. One of the simplest interactions that is sufficient to model loss in our case is a bilinear coupling, a product of the elementary system and environment coordinate operators [104]. This is given by:

$$H_I = \chi(a^\dagger b + b^\dagger a) \tag{4.55}$$

where χ is a coupling constant and a,b are the annihilation operators of the system and environment respectively.

Substituting Eq. 4.55 back into Eq. 4.54 we get:

$$K_k = \langle k|_b \, e^{i\chi t(a^\dagger b + b^\dagger a)} \, |0\rangle_b \tag{4.56}$$

This can be evaluated to give[104]:

$$K_k = \sum_n \sqrt{\binom{n}{k}} \sqrt{(1-\gamma)^{n-k}\gamma^k}\, |n-k\rangle \langle n| \tag{4.57}$$

where γ = 1-$cos^2(\chi t)$ is the probability of losing a single photon from the system during a time t. We can rewrite this in terms of transmissivity η using $\gamma + \eta = 1$ as:

$$K_k = \sum_n \sqrt{\binom{n}{k}} \sqrt{(1-\eta)^{k}\eta^{n-k}}\, |n-k\rangle \langle n| \tag{4.58}$$

We can directly use Eq. 4.58 as our Krauss operator, or we can work on it a bit more to get it in the form used in [105] which we'll do now.

$$\begin{aligned}
K_k &= \sum_n \sqrt{\binom{n}{k}} \sqrt{(1-\eta)^{k}\eta^{n-k}}\, |n-k\rangle \langle n| \\
&= \sum_n \sqrt{\frac{n!}{k!(n-k)!}} \eta^{\frac{n-k}{2}} (1-\eta)^{\frac{k}{2}} \frac{(a^\dagger)^{n-k}}{\sqrt{(n-k)!}} |0\rangle \langle 0| \frac{a^n}{\sqrt{n!}} \\
&= \sum_n \frac{1}{\sqrt{k!}} \frac{1}{(n-k)!} \eta^{\frac{n-k}{2}} (1-\eta)^{\frac{k}{2}} (a^\dagger)^{n-k} |0\rangle \langle 0| a^{n-k} a^k \\
&= (1-\eta)^{\frac{k}{2}} \Big(\sum_n \eta^{\frac{n-k}{2}} |n-k\rangle \langle n-k| \Big) \frac{a^k}{\sqrt{k!}}
\end{aligned} \tag{4.59}$$

We can replace the sum in the parenthesis with $\eta^{\frac{a^\dagger a}{2}}$. To see why, let's expand and compare the action of both operators on some state $|m\rangle$.

$$\begin{aligned}
\eta^{\frac{a^\dagger a}{2}} &= e^{\ln(\eta^{\frac{a^\dagger a}{2}})} \\
&= e^{a^\dagger a \ln(\sqrt{\eta})} \\
&= \sum_{i=0}^{\infty} \frac{(\ln\sqrt{\eta})^i}{i!} (a^\dagger a)^i
\end{aligned} \tag{4.60}$$

Now let's act by this on $|m\rangle$.

$$\sum_{i=0}^{\infty} \frac{(\ln \sqrt{\eta})^i}{i!} (a^\dagger a)^i |m\rangle = \sum_{i=0}^{\infty} \frac{(\ln \sqrt{\eta})^i}{i!} (m)^i |m\rangle$$
$$= \eta^{\frac{m}{2}} |m\rangle \tag{4.61}$$

Whereas :

$$\sum_n \eta^{\frac{n-k}{2}} |n-k\rangle \langle n-k| |m\rangle = \sum_n \eta^{\frac{n-k}{2}} |n-k\rangle \delta_{n-k,m}$$
$$= \eta^{\frac{m}{2}} |m\rangle \tag{4.62}$$

Making the substitution, we get the following formula for the operator K:

$$K_k = (1-\eta)^{\frac{k}{2}} \eta^{\frac{a^\dagger a}{2}} \frac{a^k}{\sqrt{k!}} \tag{4.63}$$

It's important to note that the authors have a typo in Eq.(24) in [105] in the power of the first term which we fixed here. To be sure, one can also look at Eq.(1) in [106].

Example: Beamsplitters vs Krauss operator

Let's look at an example where we want to calculate the probability of measuring a certain output $|m\rangle$ after sending in a state $|n\rangle$ through some lossy medium. We will calculate the losses using the two approaches outlined above.

Beamsplitters

The output of a beamsplitter of transmissivity η with a Fock state and vaccuum inputs is given by the well-known result [100]:

$$U_{BS}|n\rangle_a|0\rangle_{a'} = \sum_{k=0}^{n} \binom{n}{k}^{\frac{1}{2}} \eta^{\frac{k}{2}}(1-\eta)^{\frac{n-k}{2}}|k\rangle_b|n-k\rangle_{b'} \tag{4.64}$$

To get the corresponding density matrix representing our output state we must take the partial trace over mode b of the density matrix constructed by the previous equation. Tgis gives us:

$$\rho = \sum_{k=0}^{n} \binom{n}{k} \eta^k (1-\eta)^{n-k} \left|k\right\rangle \left\langle k\right| \tag{4.65}$$

To get the probability of measuring state $|m\rangle$ we just take the expectation value of ρ in that state:

$$\begin{aligned} P &= \langle m| \rho |m\rangle \\ &= \langle m| \sum_{k=0}^{n} \binom{n}{k} \eta^k (1-\eta)^{n-k} \left|k\right\rangle \left\langle k\right| |m\rangle \\ &= \langle m| \sum_{k=0}^{n} \binom{n}{k} \eta^k (1-\eta)^{n-k} \left|k\right\rangle \delta_{k,m} \\ &= \binom{n}{m} \eta^m (1-\eta)^{n-m} \end{aligned} \tag{4.66}$$

Krauss operator

We begin by substituting Eq. 4.63 in Eq. 4.53 with $\rho_{in} = |n\rangle \langle n|$:

$$\rho = \sum_k \frac{(1-\eta)^k}{k!} \eta^{\frac{a^\dagger a}{2}} a^k \left|n\right\rangle \left\langle n\right| (a^\dagger)^k \eta^{\frac{a^\dagger a}{2}} \tag{4.67}$$

Taking the expectation value we get:

$$\begin{aligned} P &= \left\langle m\right| \rho \left|m\right\rangle \\ &= \sum_k \frac{(1-\eta)^k}{k!} \left\langle m\right| \eta^{\frac{a^\dagger a}{2}} a^k \left|n\right\rangle \left\langle n\right| (a^\dagger)^k \eta^{\frac{a^\dagger a}{2}} \left|m\right\rangle \\ &= \sum_k \frac{(1-\eta)^k}{k!} \eta^m \frac{(m+k)!}{m!} \delta_{m+k,n} \\ &= (1-\eta)^{n-m} \eta^m \frac{n!}{m!(n-m)!} \\ &= \binom{n}{m} \eta^m (1-\eta)^{n-m} \end{aligned} \tag{4.68}$$

which matches the result in Eq. 4.66.

Lossy FSI probability formula

We begin by writing down our state $\left|\psi_{\text{lossless}}\right\rangle$ after coming out of the FSI apparatus but before detection and before applying losses as:

$$\begin{aligned} \left|\psi_{\text{lossless}}\right\rangle &= e^{i\theta J_y} \left|j, \mu\right\rangle \\ &= \sum_{x=-j}^{x=j} C_x(\theta) \left|j, x\right\rangle \end{aligned} \tag{4.69}$$

where :

$$
\begin{aligned}
|j,\mu\rangle &= |n\rangle_a |m\rangle_b \\
j &= \frac{n+m}{2} \\
\mu &= \frac{n-m}{2}
\end{aligned}
\tag{4.70}
$$

and

$$
C_x(\theta) = \langle j,x| \, e^{i\theta J_y} \, |j,\mu\rangle \tag{4.71}
$$

We can identify $C_x(\theta)$ as an element of what is known as Wigner's (small) d-matrix. The formula for that is given by:

$$
\begin{aligned}
C_x(\theta) = d^j_{x\mu}(\theta) = & \sqrt{(j+x)!(j-x)!(j+\mu)!(j-\mu)!} \times \\
& \sum_{s=\max(0,\mu-\mathrm{x})}^{\min(\mathrm{j}+\mu,\mathrm{j}-\mathrm{x})} \left[\frac{(-1)^{x-\mu+s} (\cos\frac{\theta}{2})^{2j+\mu-x-2s} (\sin\frac{\theta}{2})^{x-\mu+2s}}{(j+\mu-s!)s!(x-\mu+s)!(j-x-s!)} \right]
\end{aligned}
\tag{4.72}
$$

To account for losses, we use the equivalent of Eq. 4.53 but for two input modes:

$$
\rho_{\text{lossy}} = \sum_{p,q=0}^{2j} K_{p.a} K_{q,b} \rho_{\text{lossless}} K^\dagger_{q,b} K^\dagger_{p.a} \tag{4.73}
$$

where

$$
K_{p.a} = (1-\eta_a)^{\frac{p}{2}} \eta_a^{\frac{a^\dagger a}{2}} \frac{a^p}{\sqrt{p!}} \tag{4.74}
$$

Now we put everything together and evaluate the probability $P_{j'\mu',j\mu}$ of measuring

the output state as $|j', \mu'\rangle$ for an input state $|j, \mu\rangle$.

$$
\begin{aligned}
P_{j'\mu',j\mu}(\theta) &= \langle j', \mu'| \rho_{\text{lossy}} |j', \mu'\rangle \\
&= \sum_{p,q=0}^{2j} \langle j', \mu'| K_{p.a} K_{q,b} |\psi_{\text{lossless}}\rangle \langle \psi_{\text{lossless}}| K_{q,b}^{\dagger} K_{p.a}^{\dagger} |j', \mu'\rangle \\
&= \sum_{p,q=0}^{2j} \sum_{x,y=-j}^{j} C_x(\theta) C_y^*(\theta) \frac{(1-\eta_a)^p (1-\eta_b)^q}{p!q!} \langle j', \mu'| \eta_a^{\frac{a^\dagger a}{2}} a^p \eta_b^{\frac{b^\dagger b}{2}} b^q |j, x\rangle \times \\
&\langle j, y| (b^\dagger)^q \eta_b^{\frac{b^\dagger b}{2}} (a^\dagger)^p \eta_a^{\frac{a^\dagger a}{2}} |j', \mu'\rangle \\
&= \sum_{p,q=0}^{2j} \sum_{x,y=-j}^{j} C_x(\theta) C_y^*(\theta) \eta_a^{j'+\mu'} \eta_b^{j'-\mu'} \frac{(1-\eta_a)^p (1-\eta_b)^q}{p!q!} \langle j', \mu'| a^p b^q |j, x\rangle \times \\
&\langle j, y| (b^\dagger)^q (a^\dagger)^p |j', \mu'\rangle \\
&= \sum_{p,q=0}^{2j} \sum_{x,y=-j}^{j} C_x(\theta) C_y^*(\theta) \eta_a^{j'+\mu'} \eta_b^{j'-\mu'} (1-\eta_a)^p (1-\eta_b)^q \frac{(j'-\mu'+q)!}{q!(j'-\mu')!} \frac{(j'+\mu'+p)!}{p!(j'+\mu')!} \times \\
&\langle j' + \frac{p+q}{2}, \mu' + \frac{p-q}{2}| |j, x\rangle \langle j, y| |j' + \frac{p+q}{2}, \mu' + \frac{p-q}{2}\rangle \\
&= \sum_{p,q=0}^{2j} \sum_{x,y=-j}^{j} C_x(\theta) C_y^*(\theta) \eta_a^{j'+\mu'} \eta_b^{j'-\mu'} (1-\eta_a)^p (1-\eta_b)^q \binom{j'+\mu'+p}{p} \binom{j'-\mu'+q}{q} \times \\
&\delta_{j'+\frac{p+q}{2},j} \delta_{\mu'+\frac{p-q}{2},x} \delta_{\mu'+\frac{p-q}{2},y} \\
&= \sum_{p,q=0}^{2j} |C_{\mu'+\frac{p-q}{2}}(\theta)|^2 \eta_a^{j'+\mu'} \eta_b^{j'-\mu'} (1-\eta_a)^p (1-\eta_b)^q \binom{j'+\mu'+p}{p} \binom{j'-\mu'+q}{q} \delta_{j'+\frac{p+q}{2},j} \\
&= \sum_{p,q=0}^{2j} \delta_{j'+\frac{p+q}{2},j} (1-\eta_a)^p (1-\eta_b)^q \binom{j'+\mu'+p}{p} \binom{j'-\mu'+q}{q} \eta_a^{j'+\mu'} \eta_b^{j'-\mu'} \\
&\left| \sqrt{(j+\mu'+\frac{p-q}{2})!(j-\mu'-\frac{p-q}{2})!(j+\mu)!(j-\mu)!} \right. \\
&\left. \sum_{s=\max(0,\mu-\mu'-\frac{\mathrm{p-q}}{2})}^{\min(\mathrm{j+\mu,j-\mu'-\frac{p-q}{2}})} \left[\frac{(-1)^{\mu'+\frac{p-q}{2}-\mu+s} (\cos\frac{\theta}{2})^{2j+\mu-\mu'-\frac{p-q}{2}-2s} (\sin\frac{\theta}{2})^{\mu'+\frac{p-q}{2}-\mu+2s}}{(j+\mu-s!)s!(\mu'+\frac{p-q}{2}-\mu+s)!(j-\mu'-\frac{p-q}{2}-s!)} \right] \right|^2
\end{aligned}
\tag{4.75}
$$

For $\eta_a = \eta_b$ we have:

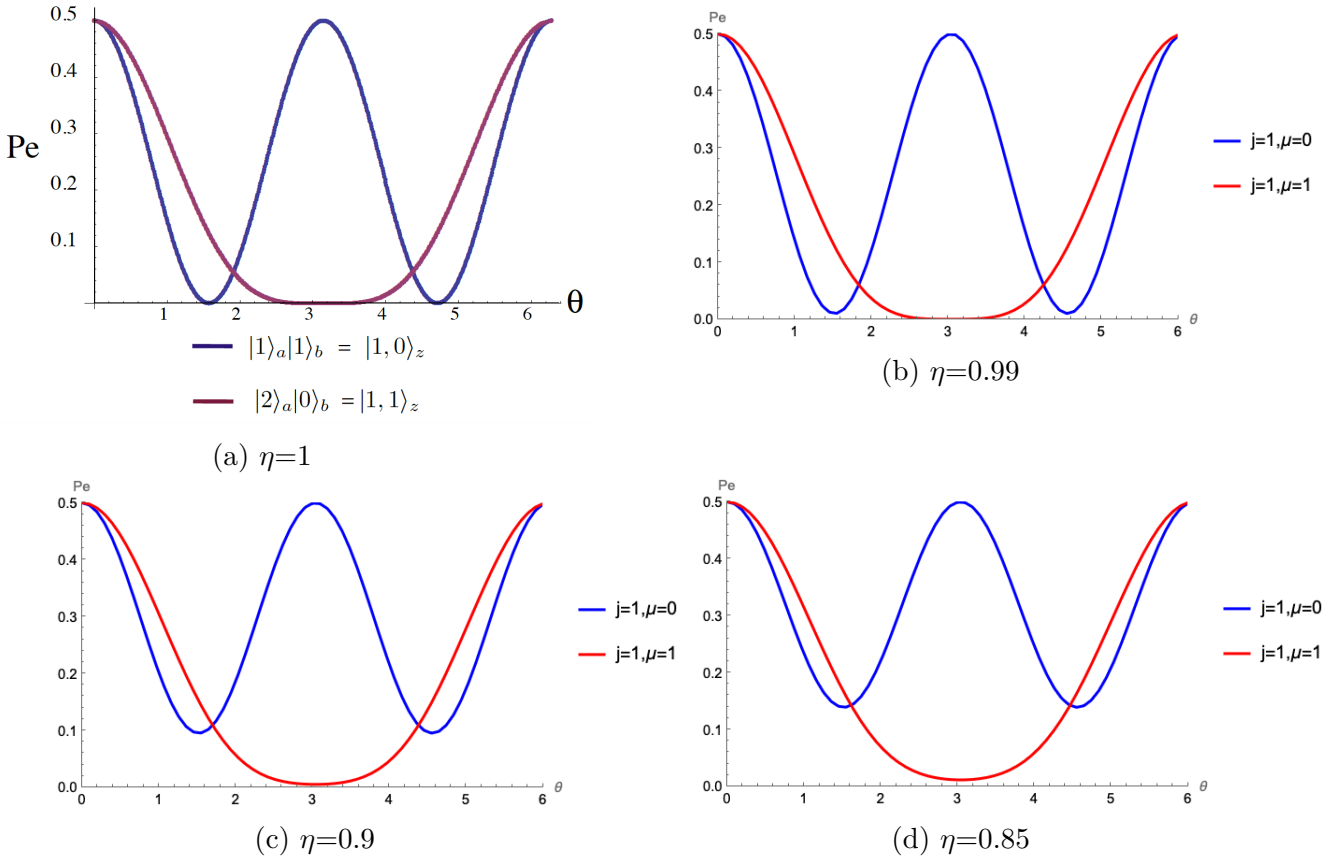
$$P_{j'\mu',j\mu}(\theta) = \sum_{p,q=0}^{2j} \delta_{j'+\frac{p+q}{2},j} \eta^{2j}(1-\eta)^{p+q} \binom{j'+\mu'+p}{p} \binom{j'-\mu'+q}{q} \left| \sqrt{(j+\mu'+\frac{p-q}{2})!(j-\mu'-\frac{p-q}{2})!(j+\mu)!(j-\mu)!} \right. \left. \sum_{s=\max(0,\mu-\mu'-\frac{p-q}{2})}^{\min(j+\mu,j-\mu'-\frac{p-q}{2})} \left[\frac{(-1)^{\mu'+\frac{p-q}{2}-\mu+s} (\cos\frac{\theta}{2})^{2j+\mu-\mu'-\frac{p-q}{2}-2s} (\sin\frac{\theta}{2})^{\mu'+\frac{p-q}{2}-\mu+2s}}{(j+\mu-s!)s!(\mu'+\frac{p-q}{2}-\mu+s)!(j-\mu'-\frac{p-q}{2}-s!)} \right] \right|^2 \tag{4.76}$$

It is important to remember when summing over possible j's and μ's to calculate the error probability - Eq. 4.47 - that $0 \leqslant j' \leqslant j$, $-j' \leqslant \mu' \leqslant j'$ and that j' moves in half-integer steps. Eq. 4.76 shall serve as the foundation for the following results.

4.2.3 Results

Let us now compare the performance of the lossy and lossless FSI models. The figures below are reproductions of the figures in [30] with different values of η accounting for loss. Figures 4.7, 4.8 and 4.9 show the error probability Pe(θ) vs θ for binary phase discrimination. Notice how Pe(θ) is zero at different values of θ depending on the input state, and how η affects different input states differently. Figure 4.10 compares Pe(θ) for discriminating between 0 and π radians, versus j (where 2j is the total photon number) at different values of η. Figures 4.11, 4.12 and 4.13 show the error probability Pe(θ) vs θ for ternary phase discrimination. Figure 4.14 is taken from [30] and shows the mutual information vs θ for different input states. Figure 4.15 is the lossy version of Fig. 4.14 with $\eta = 0.9$. Finally, figures 4.16 and 4.17 show the photon information efficiency vs the average number of signal photons n_s and the encoding

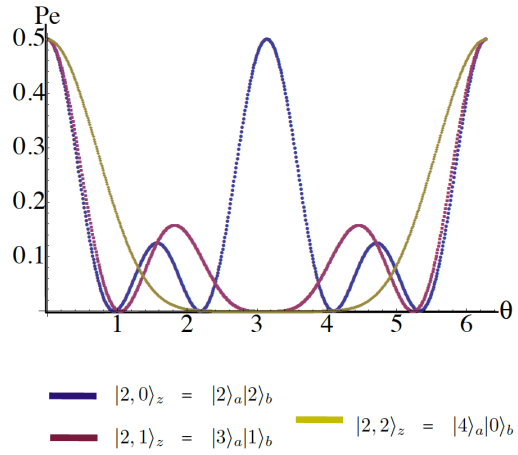
efficiency $C(n_s)$ respectively, at different values of η.



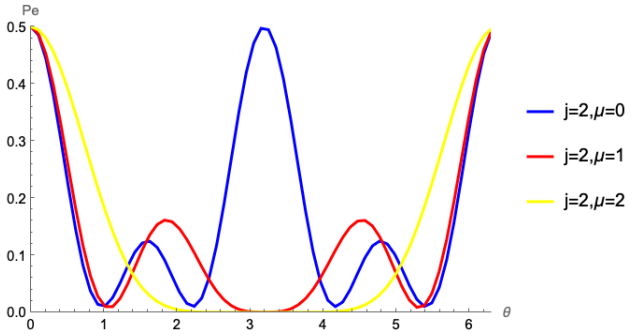
(a) η=1 (b) η=0.99

(c) η=0.9 (d) η=0.85

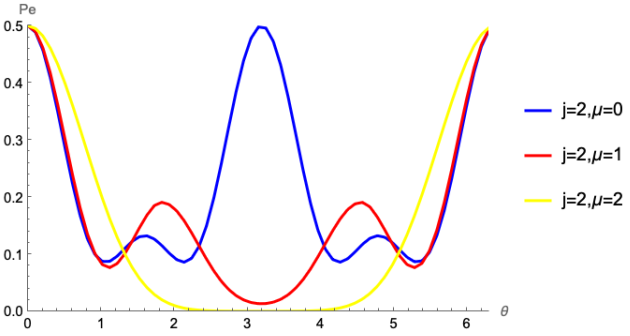
Figure 4.7: Error probability Pe(θ) for binary phase discrimination with a total photon number 2j = 2 at different values of η. Subfigure (a) is taken from [30] for reference. Notice how the input state $|2\rangle_a|0\rangle_b = |1,1\rangle_z$ is the most resilient to loss, maintaining a low error probability as we increase losses, suggesting it would be the best state to use experimentally.



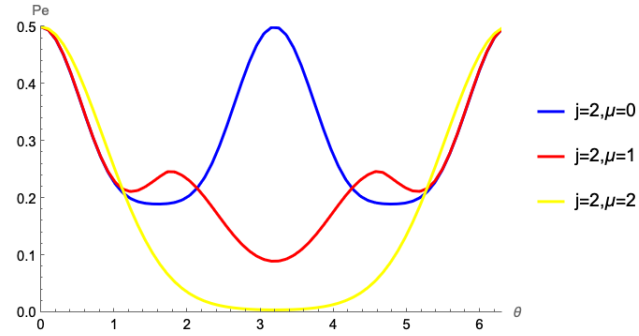
(a) η=1



(b) η=0.99

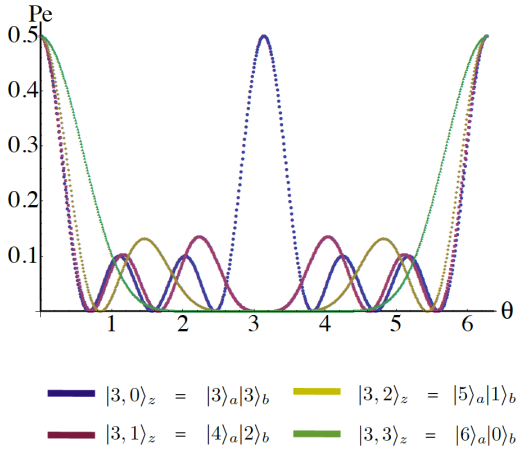


(c) η=0.9

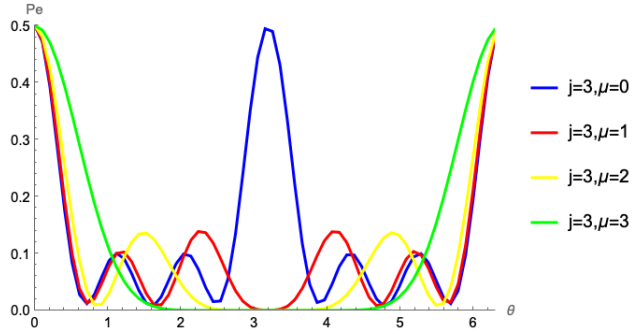


(d) η=0.7

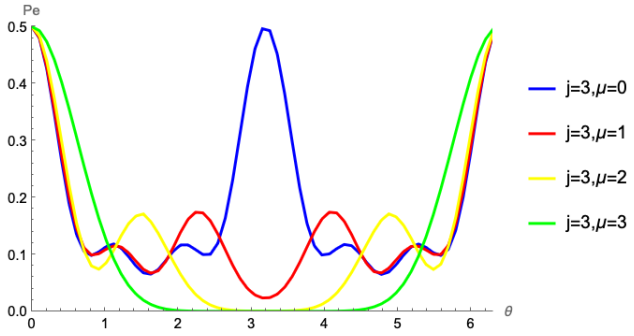
Figure 4.8: Error probability Pe(θ) for binary phase discrimination with a total photon number 2j = 4 at different values of η. Subfigure (a) is taken from [30] for reference. Notice how the input state $|4\rangle_a|0\rangle_b = |2,2\rangle_z$ is the most resilient to loss, maintaining a low error probability as we increase losses, suggesting it would be the best state to use experimentally.



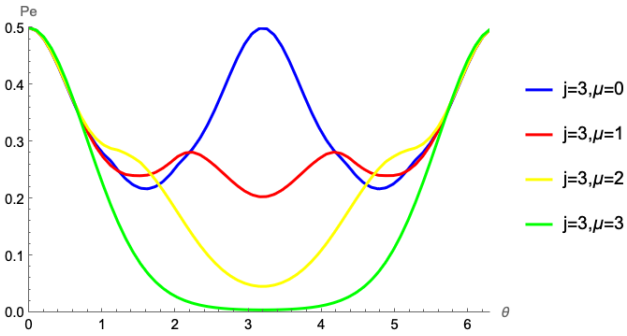
(a) η=1



(b) η=0.99

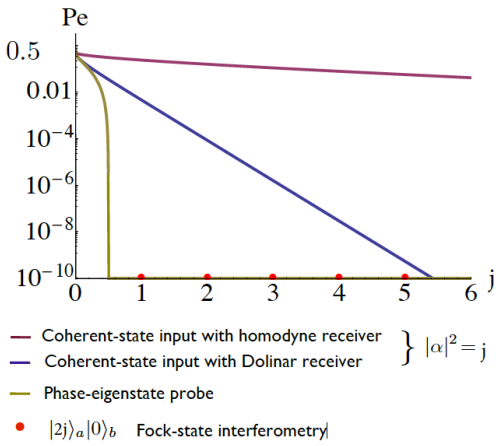


(c) η=0.9

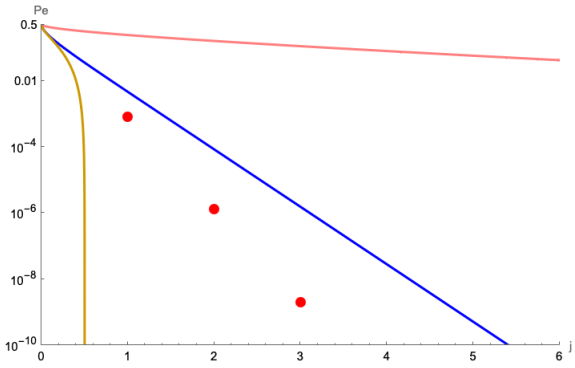


(d) η=0.55

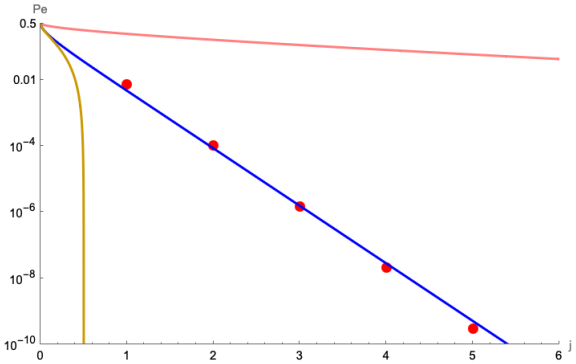
Figure 4.9: Error probability Pe(θ) for binary phase discrimination with a total photon number 2j = 6 at different values of η. Subfigure (a) is taken from [30] for reference. Notice how the input state $|6\rangle_a|0\rangle_b = |3,3\rangle_z$ is the most resilient to loss, maintaining a low error probability as we increase losses, suggesting it would be the best state to use experimentally.



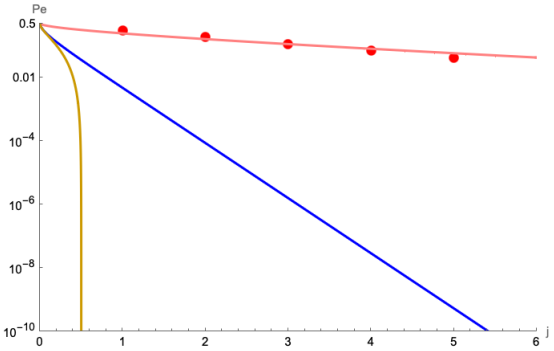
(a) η=1



(b) η=0.96

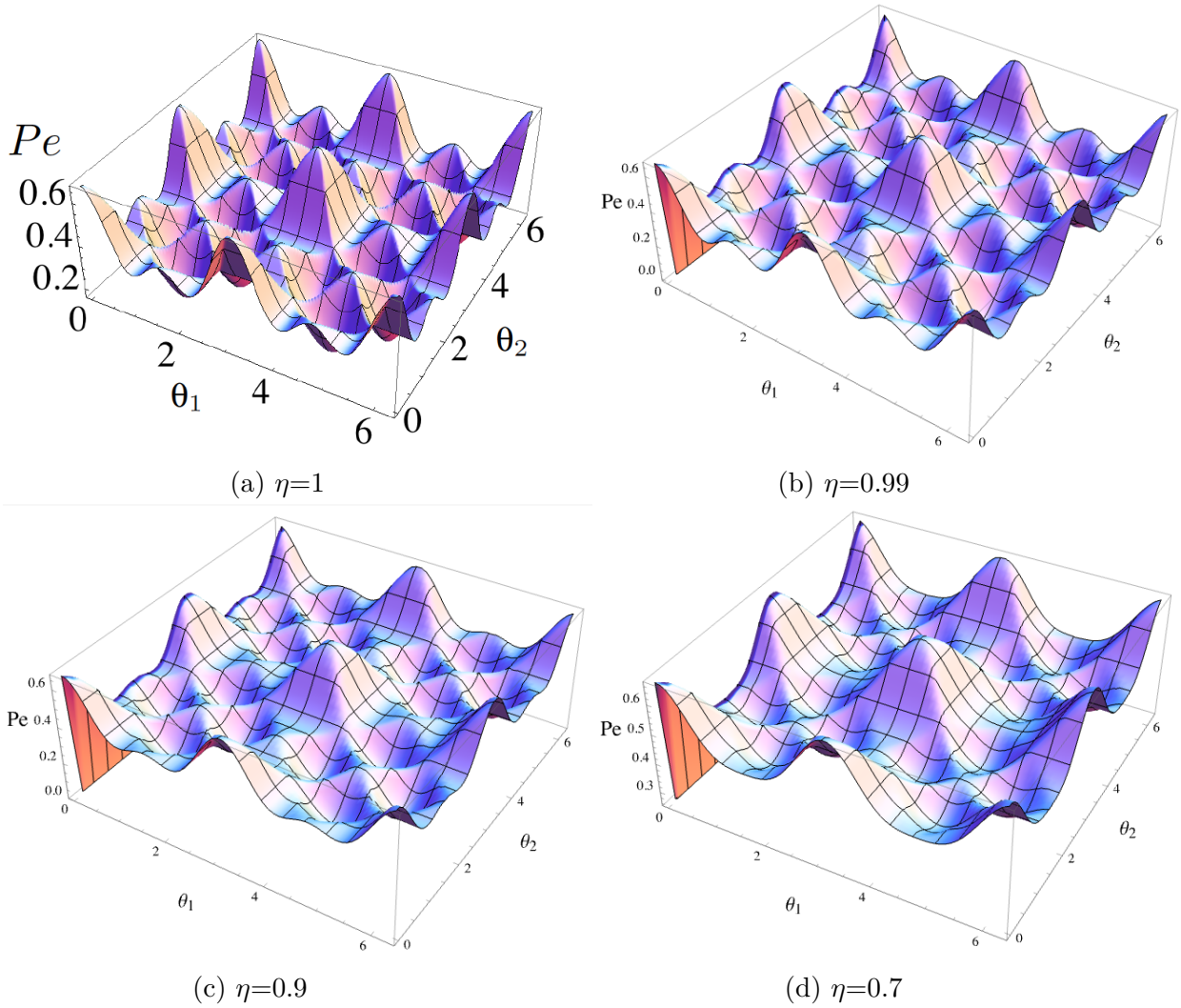


(c) η=0.88



(d) η=0.22

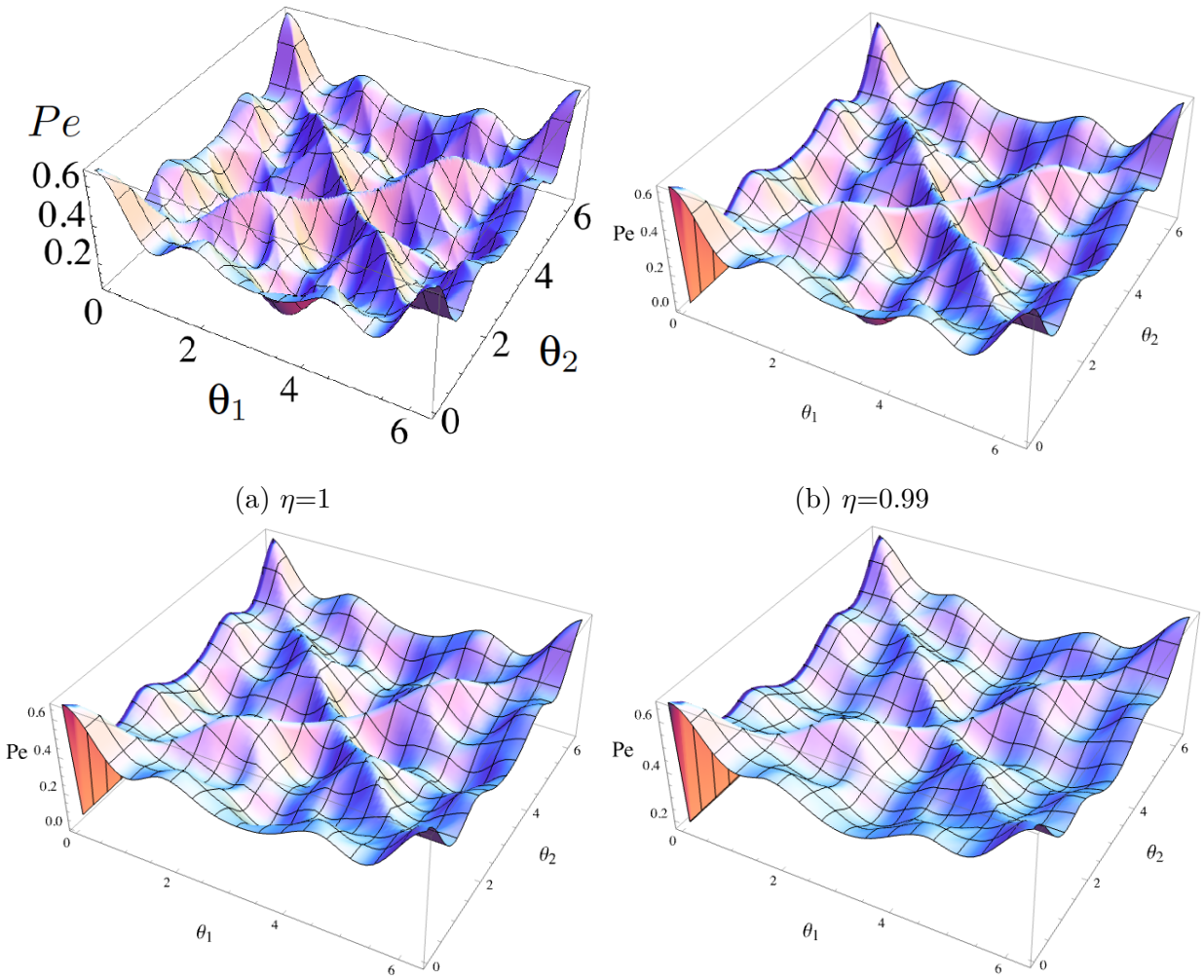
Figure 4.10: Error probability for discriminating between 0 and π radians, versus j (where 2j is the total photon number) at different values of η. Subfigure (a) is taken from [30] for reference. It compares FSI performance to other phase discrimination methods. Notice how one η goes below 0.88 the Dolinar receiver method outperforms FSI, and how below $\eta = 0.22$, the homodyne receiver method also outperforms FSI.



(a) η=1 (b) η=0.99

(c) η=0.9 (d) η=0.7

Figure 4.11: Error probability vs phase shifts θ_1 and θ_1 (in radians) for optical phase discrimination between three phase shifts $(0; \theta_1; \theta_2)$. MZI input is $|2\rangle_a |2\rangle_b = |2, 0\rangle_z$. This is calculated at different values of η. Subfigure (a) is taken from [30] for reference. Notice how the dips -corresponding to lower error- flatten as we increase loss.



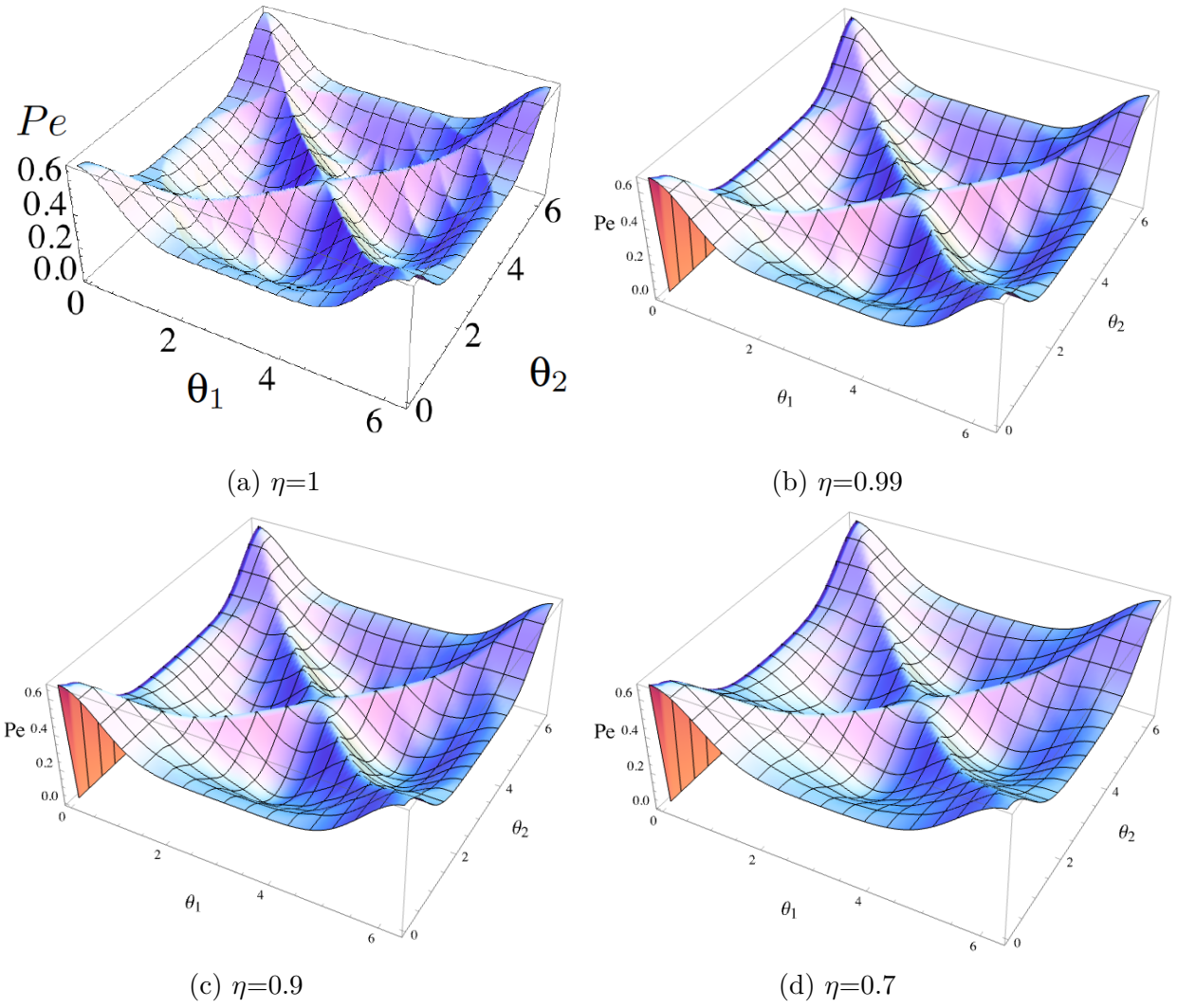
(a) η=1

(b) η=0.99

(c) η=0.9

(d) η=0.7

Figure 4.12: Error probability vs phase shifts θ_1 and θ_1 (in radians) for optical phase discrimination between three phase shifts (0; θ_1; θ_2). MZI input is $|3\rangle_a |1\rangle_b = |2,1\rangle_z$. This is calculated at different values of η. Subfigure (a) is taken from [30] for reference. Notice how the dips -corresponding to lower error- flatten as we increase loss.



(a) η=1

(b) η=0.99

(c) η=0.9

(d) η=0.7

Figure 4.13: Error probability vs phase shifts θ_1 and θ_1 (in radians) for optical phase discrimination between three phase shifts $(0; \theta_1; \theta_2)$. MZI input is $|4\rangle_a |0\rangle_b = |2,2\rangle_z$. This is calculated at different values of η. Subfigure (a) is taken from [30] for reference. Notice how the dips -corresponding to lower error- flatten as we increase loss.

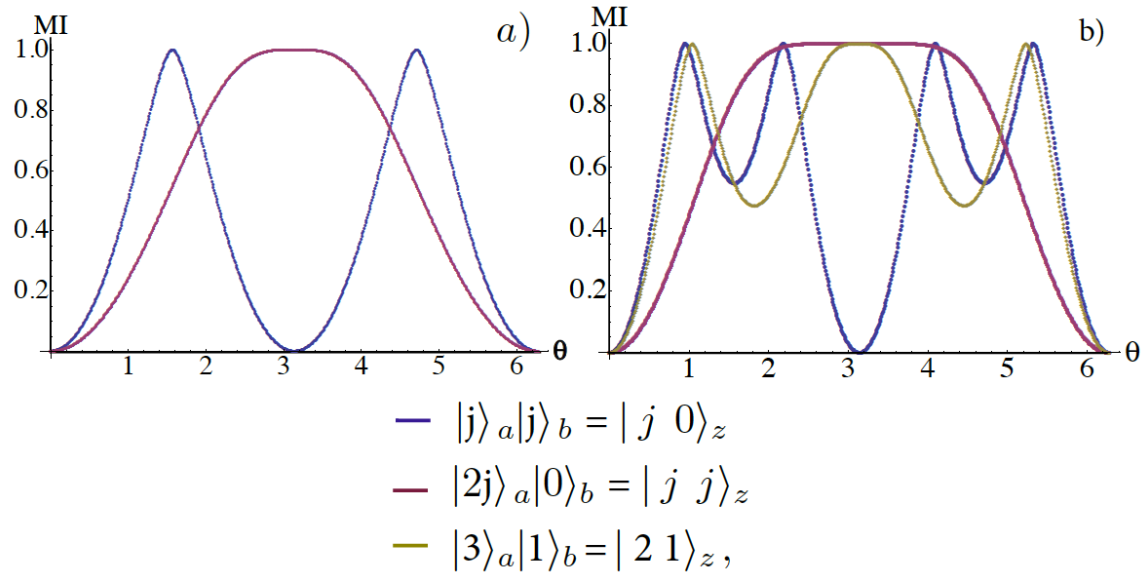


Figure 4.14: Figure taken from [30] with $\eta = 1$. Mutual information of optical reading. The binary information is encoded in optical phase shifts $(0; \theta)$; a), $n_s = \mathrm{j} = 1$; b), $n_s = \mathrm{j} = 2$.

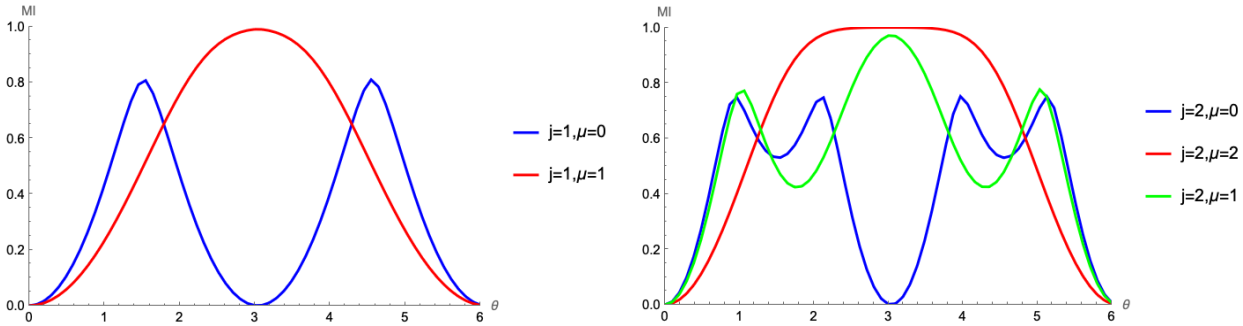
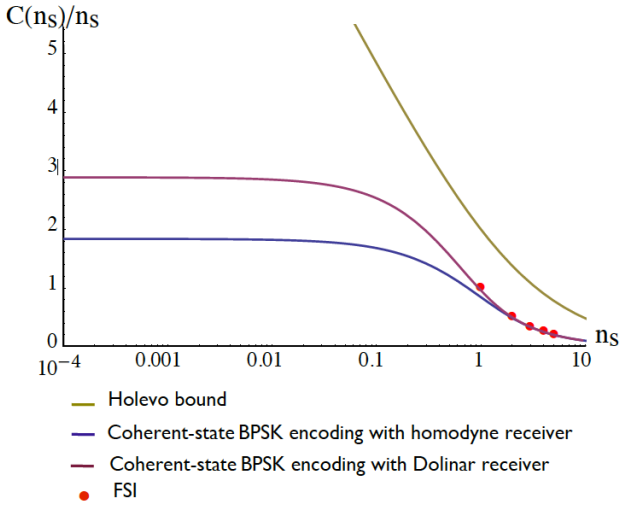
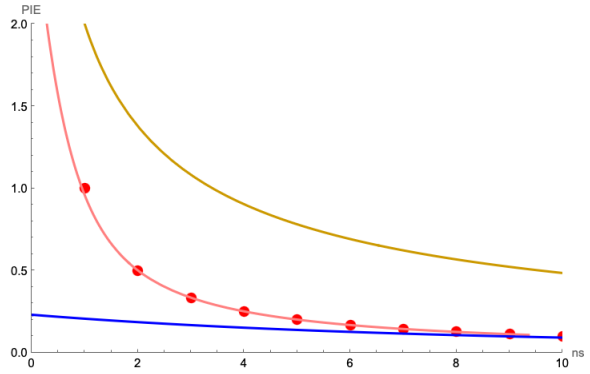


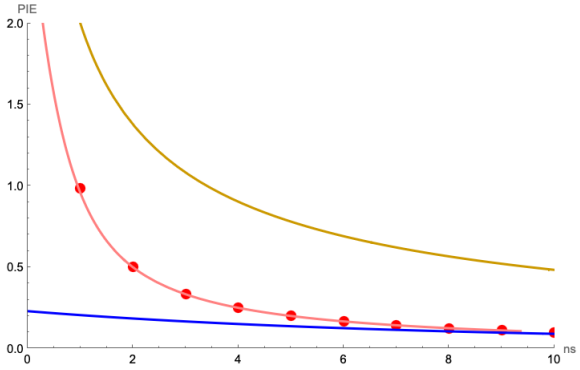
Figure 4.15: Lossy version of Fig. 4.14 with $\eta = 0.9$. Notice how the input states $|2\rangle_a|0\rangle_b = |1,1\rangle_z$ and $|4\rangle_a|0\rangle_b = |2,2\rangle_z$ are the most resilient to loss, maintaining a high MI as we add losses, suggesting it would be the best state to use experimentally.



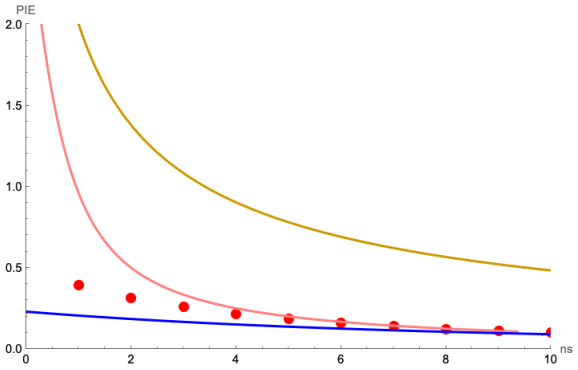
(a) η=1



(b) η=0.96

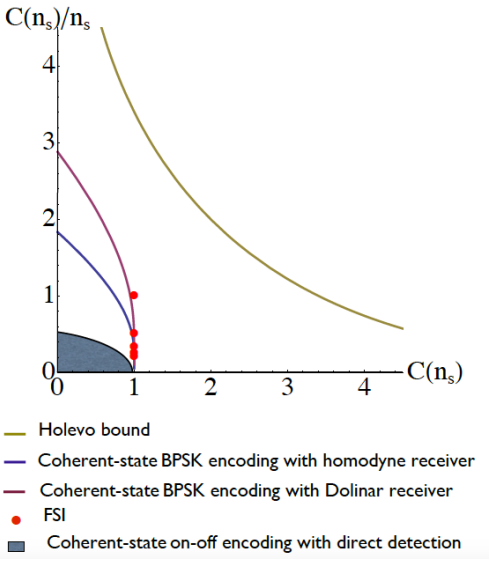


(c) η=0.88

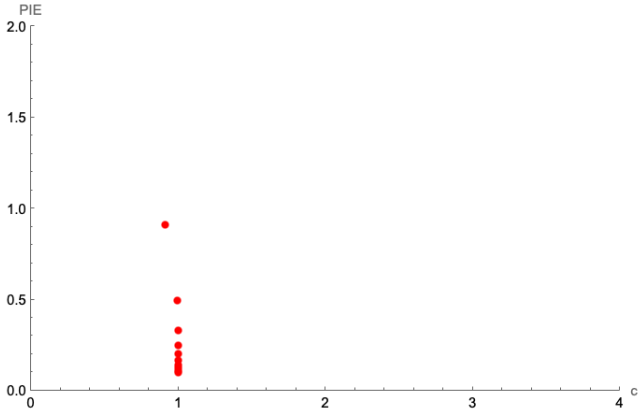


(d) η=0.22

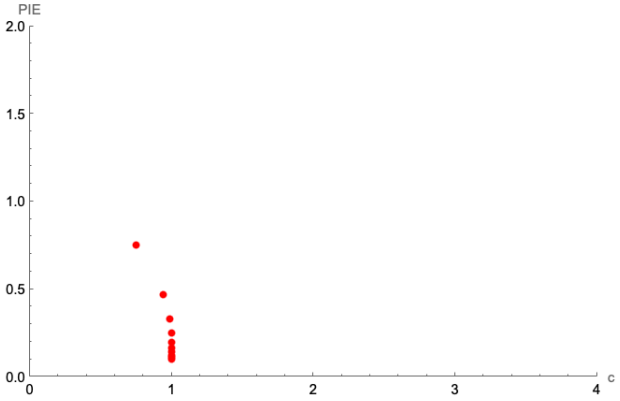
Figure 4.16: Photon information efficiency versus n_s at different values of η. Subfigure (a) is taken from [30] for reference. It compares FSI performance to other interferometry schemes.



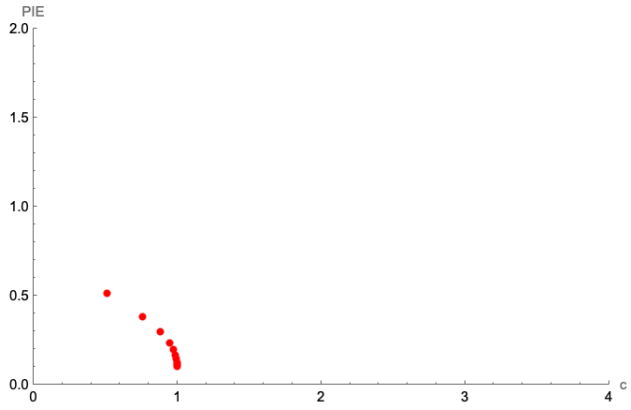
(a) η=1



(b) η=0.7



(c) η=0.5



(d) η=0.3

Figure 4.17: Photon information efficiency (bits per photon) vs the encoding efficiency (bits encoded per pixel) at different values of η. Subfigure (a) is taken from [30] for reference. It compares FSI performance to various input states and receivers. We are only concerned with comparing lossy to lossless FSI performance here.

4.2.4 Summary

In this section I presented my work on modeling a lossy Fock state interferometry setup. My goal was to develop the theory for the lossy case and assess its performance, and I have achieved that.

- I was able to successfully generalize the model to include losses, correctly reproducing the lossless results in the limit of no losses.
- I was able to show the viability of the Fock state interferometry setup for phase discrimination in the presence of losses with the right choice of input states.

Chapter 5

Conclusion

The general goal of this dissertation was to contribute to the advancement of the quantum computing endeavor. In particular, to contribute to completing the universal gate set for continuous variable quantum computing by implementing the cubic phase gate. Several proposals for implementing the cubic phase gate require high squeezing and/or high photon number resolving capability, two fronts on which significant progress was made in this dissertation.

In Chapter 2 I presented the work I have done building two triply resonant, nondegenerate (YZY) and degenerate (ZZZ), optical parametric oscillators achieving 6dB and 24dB of gain respectively—a necessary requirement to observe squeezing. These OPOs can be used as a source of two-mode squeezed states, entangled photon pairs, or cluster states.

In Chapter 3 I efficiently modeled the use of single avalanche photodiodes for use in a segmented photon number resolving detector unlocking new insights. I also detail my work- together with my group- on improving the transition edge sensor's photon number resolving capability from around 8 photons per channel to 37, allowing us to resolve up to 100 photons setting a new record up from the previous record of 16.

Finally, in Chapter 4 I outline two applications of PNRD. I began by showing how I used the TES to create a quantum random number generator, formulating its theoretical framework and validating its performance experimentally. Next, I modeled a lossy Fock state interferometry setup, analyzing its effectiveness for phase discrimi-

nation under realistic conditions. The results affirm its viability as a robust tool for quantum metrology, offering low error rates despite losses, and further highlight the versatility of PNR detectors in advancing quantum information science.

Collectively, these contributions—high-gain OPOs for squeezing and resource generation, enhanced PNR detectors for high photon number resolution, and their practical applications—represent firm steps toward realizing the cubic phase gate and, by extension, universal CV quantum computing. This work brings together both the quantum states and measurement precision required for MBQC and non-Gaussian operations. Future efforts could build on these foundations by integrating these OPOs and detectors into a cohesive cubic phase gate demonstration, potentially unlocking new computational paradigms and applications.

Bibliography

[1] Richard P. Feynman. "Simulating Physics With Computers." In: *Int. J. Theor. Phys.* 21 (1982), pp. 467–488.

[2] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge, U.K.: Cambridge University Press, 2000.

[3] J. S. Bell. "On the Einstein-Podolsky-Rosen paradox." In: *Physics* 1 (1964), pp. 195–200.

[4] Scott Aaronson. *Quantum Computing since Democritus*. Cambridge University Press, 2013.

[5] P. W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring." In: *Proceedings,* 35^{th} *Annual Symposium on Foundations of Computer Science*. Ed. by S. Goldwasser. Santa Fe, NM: IEEE Press, Los Alamitos, CA, 1994, pp. 124–134.

[6] S. Lloyd. "Universal quantum simulators." In: *Science* 273 (1996), p. 1073.

[7] Simon M. Sze. *Physics of Semiconductor Devices*. 2nd. Wiley-Interscience, 1981.

[8] Michel H Devoret and Robert J Schoelkopf. "Superconducting circuits for quantum information: an outlook." In: *Science* 339.6124 (2013), pp. 1169–1174.

[9] J. Ignacio Cirac and Peter Zoller. "Quantum Computations with Cold Trapped Ions." In: *Physical Review Letters* 74.20 (1995), pp. 4091–4094.

[10] M Saffman. “Quantum computing with atomic qubits and Rydberg interactions: progress and challenges.” In: *Journal of Physics B: Atomic, Molecular and Optical Physics* 49.20 (Oct. 2016), p. 202001.

[11] Jeremy L. O’Brien. “Optical Quantum Computing.” In: *Science* 318.5856 (2007), pp. 1567–1570.

[12] Samuel L. Braunstein. “Squeezing as an irreducible resource.” In: *Phys. Rev. A* 71 (2005), p. 055801.

[13] R. Raussendorf and H. J. Briegel. “A one-way quantum computer.” In: *Phys. Rev. Lett.* 86 (2001), p. 5188.

[14] D. Gottesman. “Fault Tolerant Quantum Computation with Higher Dimensional Systems.” In: (1998).

[15] Stephen D. Bartlett et al. “Efficient classical simulation of continuous variable quantum information processes.” In: *Phys. Rev. Lett.* 88 (2002), p. 097904.

[16] Henning Vahlbruch et al. “Detection of 15 dB Squeezed States of Light and their Application for the Absolute Calibration of Photoelectric Quantum Efficiency.” In: *Phys. Rev. Lett.* 117 (11 Sept. 2016), p. 110801.

[17] Jun-ichi Yoshikawa et al. “Demonstration of a quantum nondemolition sum gate.” In: *Phys. Rev. Lett.* 101 (2008), p. 250501.

[18] A. Furusawa et al. “Unconditional quantum teleportation.” In: *Science* 282 (1998), p. 706.

[19] Kazunori Miyata et al. “Implementation of a quantum cubic gate by an adaptive non-Gaussian measurement.” In: *Phys. Rev. A* 93 (2 Feb. 2016), p. 022301.

[20] Kevin Marshall et al. “Repeat-until-success cubic phase gate for universal continuous-variable quantum computation.” In: *Phys. Rev. A* 91 (3 Mar. 2015), p. 032321.

[21] Daniel Gottesman, Alexei Kitaev, and John Preskill. “Encoding a Qubit in an Oscillator.” In: *Phys. Rev. A* 64 (2001), p. 012310.

[22] Shohini Ghose and Barry C. Sanders. “Non-Gaussian ancilla states for continuous variable quantum computation via Gaussian maps.” In: *J. Mod. Opt.* 54 (2007), pp. 855–869.

[23] Henning Vahlbruch et al. “Detection of 15 dB Squeezed States of Light and their Application for the Absolute Calibration of Photoelectric Quantum Efficiency.” In: *Phys. Rev. Lett.* 117 (11 Sept. 2016), p. 110801.

[24] R. E. Slusher et al. “Observation of squeezed states generated by four-wave mixing in an optical cavity.” In: *Phys. Rev. Lett.* 55 (1985), p. 2409.

[25] Z. Y. Ou, S. F. Pereira, and H. J. Kimble. “Realization of the Einstein-Podolsky-Rosen paradox for continuous variables in nondegenerate parametric amplification.” In: *Appl. Phys. B* 55 (1992), p. 265.

[26] Moran Chen, Nicolas C. Menicucci, and Olivier Pfister. “Experimental realization of multipartite entanglement of 60 modes of a quantum optical frequency comb.” In: *Phys. Rev. Lett.* 112 (12 Mar. 2014), p. 120505.

[27] Rajveer Nehra et al. “Photon-number-resolving, avalanche-photodiode, segmented detectors.” In: *arXiv:1708.09015 (revised version in preparation)* (2019).

[28] Miller Eaton et al. “Resolution of 100 photons and quantum generation of unbiased random numbers.” In: *Nature Photonics* 17.1 (2023), pp. 106–111.

[29] Leonardo Assis Morais et al. “Precisely determining photon-number in real-time.” In: *arXiv:2012.10158 [physics.ins-det]* (2020).

[30] Reihaneh Shahrokhshahi, Saikat Guha, and Olivier Pfister. *Fock state interferometry for quantum enhanced phase discrimination*. 2021.

[31] Semyon Yakovlev et al. “Remote Sensing of Atmospheric Methane with IR OPO Lidar System.” In: *Atmosphere* 11.1 (2020). ISSN: 2073-4433.

[32] J. Herz et al. “Expanding two-photon intravital microscopy to the infrared by means of optical parametric oscillator.” In: *Biophysical Journal* 98.4 (2010), pp. 715–723.

[33] Miller Eaton. *Measurement-Based non-Gaussian Quantum State Engineering*. 2022.

[34] B. E. A. Saleh and M. C. Teich. *Fundamentals of Photonics*. New York, NY: Wiley and Sons, 1991.

[35] Anthony Siegman. *Lasers*. Sausalito, CA: University Science Books, 1986.

[36] Robert W. Boyd. *Nonlinear Optics*. 3rd Edition. Academic Press, 2008.

[37] J. A. Armstrong et al. “Interactions between Light Waves in a Nonlinear Dielectric.” In: *Phys. Rev.* 127 (1962), p. 1918.

[38] M. M. Fejer et al. “Quasi-phase-matched second harmonic generation: tuning and tolerances.” In: *IEEE J. Quantum Electron.* 28 (1992), p. 2631.

[39] L. E. Myers et al. “Quasi-phase-matched optical parametric oscillators in bulk periodically poled $LiNbO_3$.” In: *J. Opt. Soc. Am. B* 12 (1995), p. 2102.

[40] T. Y. Fan et al. “Second harmonic generation and accurate index of refraction measurements in flux-grown $KTiOPO_4$.” In: *Applied Optics* 26.12 (1987), pp. 2390–2394.

[41] K. Fradkin et al. “Tunable midinfrared source by difference frequency generation in bulk periodically poled KTiOPO4.” In: *Applied Physics Letters* 74.7 (Feb. 1999), pp. 914–916. ISSN: 0003-6951.

[42] Christophe Couteau and. “Spontaneous parametric down-conversion.” In: *Contemporary Physics* 59.3 (2018), pp. 291–304.

[43] Christopher Gerry and Peter Knight. *Introductory Quantum Optics*. Cambridge University Press, 2004.

[44] D. F. Walls and G. J. Milburn. *Quantum Optics*. Springer, Berlin, 1994.

[45] A. D. Boardman et al. *Advanced Photonics With Second-Order Optically Nonlinear Processes*. Springer Netherlands, 1998.

[46] M. Pysher et al. "Quasi-phase-matched concurrent nonlinearities in periodically poled $KTiPO_4$ for quantum computing over the optical frequency comb." In: *Opt. Lett.* 35 (2010), p. 565.

[47] M. V. Pack, D. J. Armstrong, and A. V. Smith. "Measurement of the $\chi^{(2)}$ tensors of $KTiOPO_4$, $KTiOAsO_4$, $RbTiOPO_4$, and $RbTiOAsO_4$ crystals." In: *Appl. Opt.* 43 (2004), p. 3319.

[48] Robert L. Byer. "Quantum Electronics: A Treatise." In: ed. by H. Rabin and C.L. Tang. Vol. IB. Academic Press, New York, 1975. Chap. 9, p. 587.

[49] Albert Einstein. "On a heuristic point of view about the creation and conversion of light." In: *Annalen der Physik* 17.6 (1905), pp. 132–148.

[50] Daniel Salart et al. "Testing the speed of 'spooky action at a distance'." In: *Nature* 454.7206 (2008), pp. 861–864.

[51] Nicolas Gisin and Rob Thew. "Quantum communication." In: *Nature Photonics* 1 (Mar. 2007), p. 165.

[52] FE Becerra et al. "Experimental demonstration of a receiver beating the standard quantum limit for multiple nonorthogonal state discrimination." In: *Nature Photonics* 7.2 (2013), pp. 147–152.

[53] Sergei Slussarenko et al. "Unconditional violation of the shot-noise limit in photonic quantum metrology." In: *Nature Photonics* 11.11 (2017), pp. 700–703.

[54] Rajveer Nehra et al. “State-independent quantum state tomography by photon-number-resolving measurements.” In: *Optica* 6.10 (Oct. 2019), pp. 1356–1360.

[55] Han-Sen Zhong et al. “Quantum computational advantage using photons.” In: *Science* 370.6523 (2020), pp. 1460–1463.

[56] JM Arrazola et al. “Quantum circuits with many photons on a programmable nanophotonic chip.” In: *Nature* 591.7848 (2021), pp. 54–60.

[57] Joe C Campbell. “Recent advances in avalanche photodiodes.” In: *Journal of Lightwave Technology* 34.2 (2016), pp. 278–285.

[58] FE Becerra, Jingyun Fan, and Alan Migdall. “Photon number resolution enables quantum receiver for realistic coherent optical communications.” In: *Nature Photonics* 9.1 (2015), pp. 48–53.

[59] Juan Miguel Arrazola et al. “Machine learning method for state preparation and gate synthesis on photonic quantum computers.” In: *Quantum Science and Technology* 4.2 (2019), p. 024004.

[60] GS Thekkadath et al. “Quantum-enhanced interferometry with large heralded photon-number states.” In: *NPJ quantum information* 6.1 (2020), pp. 1–6.

[61] Miller Eaton, Rajveer Nehra, and Olivier Pfister. “Non-Gaussian and Gottesman–Kitaev–Preskill state preparation by photon catalysis.” In: *New Journal of Physics* 21.11 (2019), p. 113034.

[62] Young-Sik Ra et al. “Non-Gaussian quantum states of a multimode light field.” In: *Nature Physics* 16.2 (2020), pp. 144–147.

[63] Mattia Walschaers. “Non-Gaussian quantum states and where to find them.” In: *PRX Quantum* 2.3 (2021), p. 030204.

[64] Andrea Mari and Jens Eisert. "Positive Wigner functions render classical simulation of quantum computation efficient." In: *Physical review letters* 109.23 (2012), p. 230503.

[65] C. W. Helstrom. *Quantum Detection and Estimation Theory*. Mathematics in Science and Engineering, 123, Academic Press, New York, 1976.

[66] B.E. Kardynał, Z.L. Yuan, and A.J. Shields. "An avalanche-photodiode-based photon-number-resolving detector." In: *Nat. Photon.* 2 (2008), p. 425.

[67] J. Sperling, W. Vogel, and G. S. Agarwal. "True photocounting statistics of multiple on-off detectors." In: *Phys. Rev. A* 85 (2 Feb. 2012), p. 023820.

[68] Adriana E. Lita, Aaron J. Miller, and Sae Woo Nam. "Counting near-infrared single-photons with 95% efficiency." In: *Opt. Expr.* 16 (2008), pp. 3032–3040.

[69] Daiji Fukuda et al. "Titanium-based transition-edge photon number resolving detector with 98% detection efficiency with index-matched small-gap fiber coupling." In: *Optics express* 19.2 (2011), pp. 870–875.

[70] Thomas Gerrits et al. "Superconducting transition edge sensors for quantum optics." In: *Superconducting devices in quantum optics*. Springer, 2016, pp. 31–60.

[71] Thomas Gerrits et al. "Extending single-photon optimized superconducting transition edge sensors beyond the single-photon counting regime." In: *Optics Express* 20.21 (2012), pp. 23798–23810.

[72] Georg Harder et al. "Single-mode parametric-down-conversion states with 50 photons as a source for mesoscopic quantum optics." In: *Physical review letters* 116.14 (2016), p. 143601.

[73] Zachary H. Levine et al. “Algorithm for finding clusters with a known distribution and its application to photon-number resolution using a superconducting transition-edge sensor.” In: *J. Opt. Soc. Am. B* 29.8 (Aug. 2012), pp. 2066–2073.

[74] G Fujii et al. “Thin gold covered titanium transition edge sensor for optical measurement.” In: *Journal of Low Temperature Physics* 167.5 (2012), pp. 815–821.

[75] Niranjan Sridhar et al. “Direct measurement of the Wigner function by photon-number-resolving detection.” In: *J. Opt. Soc. Am. B* 31.10 (2014), B34–B40.

[76] Rajveer Nehra et al. “Generalized overlap quantum state tomography 1.” In: *Physical Review Research* 2.4 (2020), p. 042002.

[77] Miller Eaton et al. “Resolution of 100 photons and quantum generation of unbiased random numbers.” en. In: *Nature Photonics* 17.1 (Jan. 2023), pp. 106–111. ISSN: 1749-4893. (Visited on 02/12/2025).

[78] Alan M Ferrenberg, DP Landau, and Y Joanna Wong. “Monte carlo simulations: Hidden errors from ‘‘good’’random number generators.” In: *Physical Review Letters* 69.23 (1992), p. 3382.

[79] Xiongfeng Ma et al. “Quantum random number generation.” In: *npj Quantum Information* 2.1 (2016), pp. 1–9.

[80] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. “Quantum random number generators.” In: *Reviews of Modern Physics* 89.1 (2017), p. 015004.

[81] André Stefanov et al. “Optical quantum random number generator.” In: *Journal of Modern Optics* 47.4 (2000), pp. 595–598.

[82] Thomas Jennewein et al. “A fast and compact quantum random number generator.” In: *Review of Scientific Instruments* 71.4 (2000), pp. 1675–1680.

[83] Christian Gabriel et al. “A generator for unique quantum random numbers based on vacuum states.” In: *Nature Photonics* 4.10 (2010), pp. 711–715.

[84] Bruno Sanguinetti et al. “Quantum random number generation on a mobile phone.” In: *Physical Review X* 4.3 (2014), p. 031056.

[85] John Von Neumann. “13. various techniques used in connection with random digits.” In: *Appl. Math Ser* 12.36-38 (1951), p. 3.

[86] Yuval Peres. “Iterating von Neumann’s procedure for extracting random bits.” In: *The Annals of Statistics* (1992), pp. 590–597.

[87] Yi Zhao et al. “Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems.” In: *Physical Review A* 78.4 (2008), p. 042333.

[88] Min Ren et al. “Quantum random-number generator based on a photon-number-resolving detector.” In: *Physical Review A* 83.2 (2011), p. 023820.

[89] Christopher C. Gerry et al. “Proposal for a quantum random number generator using coherent light and a non-classical observable.” In: *J. Opt. Soc. Am. B* 39.4 (Apr. 2022), pp. 1068–1074.

[90] Clinton Cahall et al. “Multi-photon detection using a conventional superconducting nanowire single-photon detector.” In: *Optica* 4.12 (2017), pp. 1534–1535.

[91] Andrew Rukhin et al. “Nist special publication 800-22: A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications.” In: *NIST Special Publication* 800 (2010), p. 22.

[92] E. B. Wilson. “Probable Inference, the Law of Succession, and Statistical Inference.” In: *Journal of the American Statistical Association* 22.158 (1927), pp. 209–212.

[93] Antonio Acín and Lluis Masanes. “Certified randomness in quantum physics.” In: *Nature* 540.7632 (2016), pp. 213–219.

[94] Juan Soto and Lawrence Bassham. *Randomness testing of the advanced encryption standard finalist candidates*. Tech. rep. NISTIR 6483. *NIST Publications*, Department of Commerce, Gaithersberg, MD, 20899, 2000.

[95] A. Doğanaksoy et al. “New statistical randomness tests based on length of runs.” In: *Math. Prob. Engin.* 2015 (2015), p. 626408.

[96] Geert-Jan Schrijen and Roel Maes. “Creating an Efficient Random Number Generator Using Standard SRAM.” In: (2022).

[97] G. P. Agrawal. *Fiber-Optic Communication Systems*. 4th. Wiley Series in Microwave and Optical Engineering. Hoboken, NJ: Wiley-Interscience, 2010.

[98] S. Pirandola. “Quantum reading of a classical digital memory.” In: *Physical Review Letters* 106.9 (2011), p. 090504.

[99] R. Nair. “Discriminating quantum-optical beam-splitter channels with number-diagonal signal states: Applications to quantum reading and target detection.” In: *Physical Review A* 84.3 (2011), p. 032312.

[100] C. M. Caves. “Quantum-Mechanical Radiation-Pressure Fluctuations in an Interferometer.” In: *Phys. Rev. Lett.* 45 (1980), p. 75.

[101] J.-M. Levy-Leblond and F. Balibar. *Quantics: Rudiments of Quantum Physics*. North-Holland, 1990.

[102] B. Yurke, S. L. McCall, and J. R. Klauder. “SU(2) and SU(1,1) interferometers.” In: *Phys. Rev. A* 33 (1986), p. 4033.

[103] M. J. Holland and K. Burnett. “Interferometric detection of optical phase shifts at the Heisenberg limit.” In: *Phys. Rev. Lett.* 71 (1993), p. 1355.

[104] Isaac L. Chuang, Debbie W. Leung, and Yoshihisa Yamamoto. "Bosonic quantum codes for amplitude damping." In: *Phys. Rev. A* 56 (2 Aug. 1997), pp. 1114–1125.

[105] R. Demkowicz-Dobrzanski et al. "Quantum phase estimation with lossy interferometers." In: *Phys. Rev. A* 80 (1 July 2009), p. 013825.

[106] Linshu Li et al. "Cat Codes with Optimal Decoherence Suppression for a Lossy Bosonic Channel." In: *Phys. Rev. Lett.* 119 (3 July 2017), p. 030502.