PSEUDOTHERMAL LIGHT BASED QUANTUM RANDOM NUMBER GENERATOR

A Thesis

by

Abdulrahman Dandaşi

Submitted to the
Graduate School of Sciences and Engineering
In Partial Fulfillment of the Requirements for
the Degree of

Master of Science

in the
Department of Electrical and Electronics Engineering

Özyeğin University
January 2021

PSEUDOTHERMAL LIGHT BASED QUANTUM RANDOM NUMBER GENERATOR

Approved by:

Assistant Professor Kadir Durak
Department of Electrical and Electronics Engineering
Özyeğin University

Professor Fatih Uğurdağ
Department of Electrical and Electronics Engineering
Özyeğin University

Assistant Professor Muhammed Fatih Toy
Department of Biomedical Engineering
Istanbul Medipol University

Date Approved: 18/01/2021

To my parents.

ABSTRACT

Random number generators (RNGs) have recently gained lots of attention from the scientific and commercial communities recently. That is due to computers' fast development, making cracking cryptographic systems faster than before. Several RNGs emerged such as pseudorandom number generators and true random number generators. However, knowing the pros and cons of both, they started to show some weakness facing quantum computers. In specific computational tasks, quantum computers use quantum phenomena which makes them drastically faster than conventional computers. Thus, the need for a countermeasure arose for the applications where high-security is needed. This is when the idea of a RNG that exploits phenomena from the quantum realm saw the light and quantum random number generators (QRNGs) started to appear. One critical aspect of any QRNG is its speed, especially in practical applications. In this thesis, I show that the photon statistics affect the randomness characteristics of QRNGs. This works as an optical bit extraction which allows a faster sampling rate than the coherent source based balanced homodyne detection without compromising the randomness quality. Specifically, I propose adding thermal or chaotic characteristics for one of the optical paths in the vacuum fluctuations based QRNG in the homodyne configuration, allows a higher sampling rate of the raw signal without compromising the randomness quality. The idea is to increase the chaotic behavior of coherent sources using scattering, which reveals itself as the broadening of the distribution for the photon statistics and making it a super-Poissonian distribution.

ÖZETÇE

Gelişen teknoloji ile kriptografik sistemlerin daha hızlı kırılabilirliği, hem bilimsel hem de ticari toplulukların gözlerini Rastgele Sayı Üreteçlerine (RSÜ'lere) çevirmesine neden oldu. Geleneksel RSÜ'ler sözde veya gerçek rassal sayı üreteçleri diye ikiye ayrılır. Bu yöntemlerin güçlü ve zayıf yönlerini göz önünde tuttuğumuzda, geleneksel yöntemler kuantum bilgisayarlara karşı bazı zayıflıklar göstermeye başlıyor. Bazı işlemler için kuantum bilgisayarlar geleneksel bilgisayarlardan daha hızlı çalışmasını sağlayan kuantum temeline dayanan prensipler kullanır. Böylece yüksek güvenlik gerektiren uygulamalarda kuantum temeline dayanan presipler bir ışık olmuştur ve kuantum temelli rastgele sayı üreteçleri (KRSÜ'ler) gün yüzüne çıkmaya başlamıştır. KRSÜ'lerin en önemli özelliği, özellikle pratik uygulamalarda, hızlı olmasıdır. Bu tez, foton istatistiğinin KRSÜ'lerin rassallık özellikleri üzerindeki etkilerini gösterir. Bu çalışma rassallık kalitesinden ödün vermeden, eşevreli lazer kaynak temelli dengeli homodin ölçümünden daha hızlı örnekleme oranıyla bit çıkarımı sağlayan bir optik yöntemidir. KRSÜ temelli homodin uygulamalarına, vakum dalgalanmalarındaki ışın yollarından biri için termal veya kaotik özellikler ekledik ve rassallık kalitesinden ödün vermeden işlenmemiş sinyalin örneklem oranını arttırmayı sağladık. Saçılma kullanımının amacı eşevreli kaynakların kaotik özelliğini arttırmaktır, bu saçılma foton istatistiğindeki Poisson dağılımını genişleterek süper Poisson dağılımına çevirmektir.

ACKNOWLEDGEMENTS

I want to show my gratitude and appreciation to the nice people who surrounded me during my years in ÖzÜ:

First of all, my advisor Professor Kadir Durak for his constant support throughout my days in the lab. Alongside his theoretical and experimental help to us, his motivational speaks fired me up every week to achieve more and more in my life. Also to Helin, for her big contribution to our work. Her patience and hard work have led to the results seen in this thesis.

To the friends inside and outside the lab, for being my second family in Turkey. Of course, the biggest gratitude goes to my first family for their unconditional support in this journey.

In the end, I cannot express how thankful I am for Ozyegin University with everyone and everything in it. After spending 6 years here (BSc / MSc) I will always be proud to be part of this big family.

Special thanks to professors Fatih Uğurdağ and Muhammed Fatih Toy for accepting to be the jury of my thesis defense.

This research is carried out by the support of Scientific and Technological Research Council of Turkey (TUBITAK) Career Grant no: 118E156.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

For a very long time, randomness has been a deep field to be studied in philosophy and science. Since the time that it was a representation of free will and determinism in ancient history. In the 20^{th} century, computers - with the definition that comes to our minds nowadays - started to see the light. In which transformed randomness from some philosophical discussions into more machine-based practical applications. For example, it was using randomized trials to find solutions for some complicated problems. This was used in natural sciences (chemistry, biology, physics), mathematics, and finance. It was also used in cryptography to protect and encrypt valuable information. Although the concept of cryptography has been discovered for centuries, its affiliation with random numbers was introduced recently. This is also due to the invention of computers, which made it easier for cracking human-made cryptography.

Many physical phenomena around us can be used to generate randomness; some examples of it are discussed later on in the thesis. Such phenomena do not decrease, as they exist alongside human beings' existence. The question is, why mine this randomness and generate random numbers? A lot can be gained from mining and extracting this much randomness. Since the last few centuries, information gained lots of importance and increased day by day up to date. This is due to the technological revolution, which changed our lives remarkably. We reached the level of using random numbers daily. For example, an internet browser offers to generate a password for the user. Another one is when the bank sends a confirmation code to the mobile phone when purchasing something through the internet. Many other examples prove that random numbers became a necessity for human beings. We discuss how exactly and

why we mine and exploit random numbers in the following sections.

1.1 Random Number Generators Types

It is crucial to separate random numbers based on mathematical algorithms and random numbers extracted from randomly occurring physical phenomena. One main type of random number generators (RNGs) is called a pseudorandom number generator (PRNG), a deterministic algorithm that generates random numbers using a computer. Knowing the generation method, we also know that it is not "truly" random and that an intruder can guess these numbers. Such generators work based on a little set of numbers (seed) that enters the algorithm, generating a bigger sequence of random numbers. Most RNGs can generate numbers in the form of any random distribution. However, most RNGs work on producing uniformly distributed statistics [1]. Many PRNGs make use of the number theory. One example is using linear congruential generators [2]. These generators generate random numbers by the recursive formula: $X_{n+1} = (aX_n + c)\, mod\ m$ where $n \geq 0$, X_n represents the n^{th} digit of the bitstream, m is the modulus, a is the multiplier, and c is the increment. The latter parameters need to be chosen correctly to get the correct result. Otherwise, the random bitstream would have a short period, which is a critical property for a PRNG. Any PRNG will repeat itself and produce similar numbers to the ones already produced, which happens every *period*. This is why we choose PRNGs with broad periods in order not to have distinguishable repetitions. PRNGs have several advantages that make them popular in science. They stand to be the fastest among other RNGs for many years. They are also easier to generate and less costly than other RNGs. However, many other applications need the RNG to be truly random. Consequently, the importance of true random number generators (TRNGs) emerged in science.

TRNGs tend to be more random and unpredictable than PRNGs as they make

use of physically occurring incidents that very difficult for human beings to detect. TRNGs work on collecting the data in the process of *entropy gathering*, which can be taken from many sources, such as data collected from some processes inside a computer. Examples can be interrupted timings, disk access times, the letters written on the keyboard, or the mouse's movement. Some methods applied on Linux OS for entropy gathering and turning them into random bitstream can be seen in [3]. These generators can be called non-deterministic RNGs, according to their working principles [4]. Some other types of TRNGs use non-deterministic physical events such as the interactions of some physical experiment or inside an electronic circuit. Companies such as *Intel* and *VIA Technologies* make use of their processes to make TRNGs [5]. The first one uses the latch that happens because of the thermal noise. The other one uses the alternation from the oscillators, making thermal noise change the jitter. Such TRNGs come with internal electronic circuits that remove the random numbers' bias. As mentioned before, TRNGs are unpredictable and completely random. However, they were not integrated enough into the market for several reasons.

1. The rate of random number generation in TRNGs is slower than PRNGs. These methods are either too slow for some essential constraint or sampled too fast that the system cannot change enough, which means the bitstreams will have periods faster.

2. Detecting deficiencies in the systems is usually challenging. For example, if the computer's thermal noise device has failed and stopped working correctly, it might be too late to detect, compromising the random bits' quality.

Considering these reasons, and knowing that PRNGs can be predictable and traceable, QRNGs come in handy. They are systems that use quantum phenomena to implement fast and secure RNGs and will be discussed explicitly in the following sections.

1.2 Applications of Random Numbers

The need for random numbers in many fields increases with technology's daily development. In this section, I will describe some of these needs.

1.2.1 Simulations and Experimental Science

Random numbers have a vital role in different scientific areas. They are an essential part of the root of the randomized algorithms applied widely in computer science. It can be in number theory, computing, or simulations [6]. For some complex systems, running a numerical analysis can be very difficult to anticipate such systems' behavior correctly. Thus, there is a need for some simplified models to do the job of utilizing random numbers. The idea is that we can get precise results if enough cases are studied while choosing them randomly. The Monte Carlo method is an essential application of RNGs [7]. It is a scheme that uses numbers to solve a complicated problem with randomized trials. Such methods are broadly used to solve complex numerical integration and physics problems. Most often, randomly sampling the state space gives a valid result when using a PRNG. This is sufficient for almost all simulations. However, if some of these generators have a weak algorithm behind them, some of their generated bitstreams correlate with each other. This can be shown when a bitstream from these generators is put under some conventional randomness tests [8]. After many critical failures, suggestions started to appear for testing these PRNGs in real-life problems alongside the randomness tests. Also, in the Monte Carlo method, it is suggested to simulate the results using different PRNGs to avoid having faulty results.

1.2.2 Cryptography

One of the first implementations of cryptography is known as symbol replacement, which can be explained as follows; the whole alphabet is shifted by a specific number

known only to the two sides communicating. Secure communication using cryptography needs two main parts; the sender having an algorithm that encrypts the transmitted message so that an eavesdropper cannot interpret it. The receiver is having an algorithm that decrypts the message to entirely understand its meaning. Such algorithms are announced publicly so that the communicated parties can have secure and meaningful communication. This means that this, by itself, is not enough for having the needed communication. Some random numbers are added to the message to achieve secure communication, similar to the ancient used method. However, these are much more complicated as will be talked about in the following sections. Most modern cryptography systems follow the principle of Kerckhoff [9] where it is assumed that a cryptographic system might be accessible to an eavesdropper which means that the whole system is known perfectly to them. Thus, such methods are open to everyone as their security comes from choosing the secret key. This means that assuming a channel is compromised, and the communicators can simply change the key to communicate safely again. This practice is advantageous and can be used in many circumstances. For communication safety, it is indispensably important for the key to be random. This is done by choosing a uniform m-bit string randomly from the whole domain of the key. When we combine the data to be sent with the algorithm and the random bits, then the two parties can safely communicate together. This is assuming that the eavesdropper does not know the secret bitstream. Alternatively, some other practices of cryptography can make use of numbers that are not "much random" [10]. In different applications, random numbers are needed to be as nonces, which means that they are only used once. This can be used in sequence numbers to bypass attacks on passwords and digital signatures, or in sequence numbers [11]. Another significant application of cryptography is quantum cryptography. As a quantum key distribution can be attacked when the states and bases are not randomly chosen [12, 13]. Most cryptographic applications require random numbers

to be uniformly distributed, truly random, and unpredictable. They also need the generated numbers to lower the danger of a possible leaked key. There exist two important rules in cryptography applications. The first one is that even if an eavesdropper has access to the full sequence, their guessing probability of the next bit must not exceed 0.5. The second one requires that if the eavesdropper knows some part of the communicated sequence, they must not be able to guess the prior bits from the same generator. For practicality, these two conditions are reduced to one that summarizes both. It states that, in polynomial time, there must be no machine that can get a sequence of the stream bit and guess some other part of it [14]. To complete this system, we need a way to distribute this random bitstream to the receiver so that they can decrypt a *gibberish* message into a meaningful one. For this purpose, the one-time-pad method was developed, which is considered one of the safest encryption methods known up to date. It can be described as an upgrade of the ancient method discussed at the beginning of this section. But instead of shifting each letter of the message, we rather shift the index of each letter by a randomly chosen number as seen in Figure 1. This method can work efficiently under two terms. The first is that, for each letter of the encrypted message, the key must contain at least one random bit for it. The second is, all of these generated numbers must be unconditionally random and unpredictable. However, this method is not used nowadays due to the complication in producing long bitstreams. Also, it is even harder to distribute such long keys securely. Later on, in order to have practical encryption systems, there was a need for algorithms that require short ciphering keys for either employing them as algorithms or for distribution.

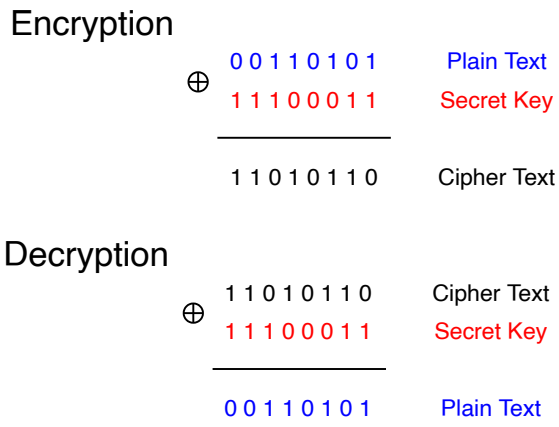

Figure 1: An explanation of an example of the one-time-pad.

The two most important algorithms nowadays are Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES). RSA and the methods similar to it are used to transfer the encrypting key. Where AES and the methods similar to it are used as encryption methods by themselves. During the encryption, like the case of the one-time-pad, the communicating parts use the same encrypting key which is called symmetric encryption. Where it is mostly required to have keys made of 256 bits for both sides. For distributing the keys, an algorithm called public-key cryptography is used. An example of that is RSA, as they use keys of 1024 or 2048 bits of length. Unlike the cryptographic algorithms, this does not require the keys to be of the same length and are called asymmetric encryption. Except for the one-time-pad, all other algorithms use one-way functions which are some mathematical problems that are very difficult to calculate from both directions but very simple to calculate from one direction to the other. An example for RSA can be the following, one can simply find the multiplication result of two prime numbers, but can have a hard time finding the two prime numbers when only given the resultant number. This idea means that such keys are safe to use since normal computers find it difficult to attack back while aiming to break the key. Nevertheless, in 1997, Peter Shor showed that we could break into the RSA algorithm using a quantum computer [15]. Ever

since, scientists have been trying to develop algorithms that are immune to quantum attacks. For that, quantum key distribution protocols started to see the light. They are used instead of asymmetric encryption for transferring the encryption key. The idea behind that is to employ the quantum nature and its laws to securely distribute the key between the communicators. This solves the key distribution problem to achieve a secure communication system. Several quantum key distribution protocols have been utilized in the 21^{st} century and the research about them is still ongoing [16].

1.3 Quantum Random Number Generators

QRNGs can be classified under TRNGs as the source of randomness is coming off some quantum phenomenon. The main idea behind the quantum realm in generating random numbers can be derived from presupposition in quantum physics. Measuring a quantum state will yield one eigenstate and give one of its corresponding results. Such outcomes can be approved by the experiments that will show the unpredictability of measurements which makes it an optimal choice for generating random numbers. In this section, we will discuss several QRNG implementations using different setups.

Path Branching QRNGs

This method is based on measuring the superposition of different photon paths. Let us introduce a state $|\alpha\rangle_1 |\beta\rangle_2$ that describes a photon that might take two different paths, and another state $|\beta\rangle_1 |\alpha\rangle_2$ that represents the same photon which pursues another path. Their superposition can be expressed as follows

$$\frac{|\alpha\rangle_1 |\beta\rangle_2 + |\beta\rangle_1 |\alpha\rangle_2}{\sqrt{2}} \tag{1.3.1}$$

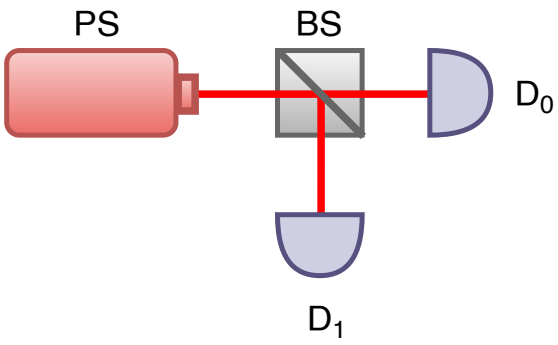

Figure 2: Photons are emitted one by one from the photon source to the balanced beam splitter then to the detectors. PS: photon source; BS: beam splitter; $D_{0,1}$: detectors.

When we put a detector at the end of both paths, we will measure one click in a detector with 1/2 as the probability for both paths. Several experiments in quantum optics can produce the same state, such as in Mach-Zehnder interferometer and other optical schemes. This can be done also propagating a weak light source into a balanced beam splitter, which is followed by two detectors connected to the two outputs of the beam splitter. When detector 0 clicks, then the bit is 0, when the other detector clicks then it is said to be 1 (Figure 2). A balanced beam splitter means that half the times the photon will be reflected and half the times the photon will be transmitted. This configuration was first applied in [17]. The fully implemented version of this setup was done in [18, 19]. Where they used photomultiplier tubes (PMT) which were first used to experimentally implement Bell Tests. These two methods were implemented with some slight differences. The main one is how the random bits are produced. As in the second implementation, when a click occurs in the first (second) detector, the signal is taken to a high (low) level. A constant bit generation can be done as follows, by sampling the signal with a clock that has a frequency that is lower enough than the detection rate, and by giving a 0 (1) if the state is low (high). This experiment has also been done using polarized photons and with a polarized beam splitter (PBS)

where all of them gave similar results. This experiment has also been done using a different technique in [20]. Where they used an attenuator to reduce the laser power into weak pulses that roughly produce a photon per pulse. Then it goes into a Fresnel multiple prism which is made of left and right-handed quartz. This prism isolates positive and negative components and leads them into two single-photon counting modules. Such a scheme that generates polarization can be changed to adjust the probabilities for all bits. This is done by adding a controlled polarizer such as in [21] where they use a decision-making system.

Phase Fluctuations

Any laser has fundamental phase fluctuations that are associated with the spontaneous emission that is classified to be a quantum phenomenon [22]. This comes from within the cavity of a semiconductor laser. Where the power of the laser is inversely proportional to the phase fluctuations. This means that when we emit a weak laser beam then the phase fluctuations will take over the signal instead of the classical noise. Directly measuring the phase fluctuations is not possible. However, an unbalanced Mach-Zehnder interferometer (as seen in Figure 3) can turn the changes of the phase to be represented as amplitude. Inside the unbalanced interferometer, a delay is introduced into one arm compared to the other one. When we assume the amplitude to vary slowly, the mean of the result will stay still and will vary proportionally with the phase difference

$$\Delta\phi(t) = \phi(t) - \delta(t + \tau) \tag{1.3.2}$$

As the resultant amplitude can be measured from the interferometer's outputs using conventional photodetectors. When the phase delay is much bigger than the coherence time of the laser, such that $\tau \gg 1/\pi\Delta v_L$. Here Δv_L is the linewidth of the laser. The phase difference tends to be a Gaussian random variable with an average of 0 [23]. While sampling the amplitude that we get from the photodetector, if we let the time difference between each sample be much larger than the addition of the delay to the

coherence time, $t_c \gg \tau + \tau_c$, then the resultant amplitudes do not depend on each other [24].

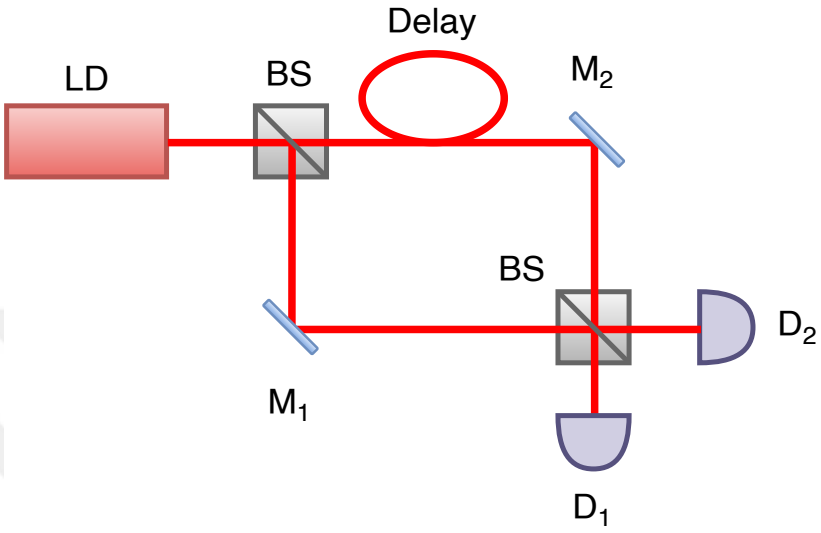

Figure 3: A bunch of photons are sent to the beam splitter, both detectors have the same probability of receiving any number of photons. PS: photon source; BS: beam splitter; $M_{1,2}$: mirrors; $D_{1,2}$: detectors.

Such amplitudes can be used as random variables of different optical QRNGs. The basic configuration of phase fluctuations based QRNG works as follows, a laser is divided by a beam splitter, one arm of its divided beam will be delayed, then it will enter another beam splitter alongside the beam of the other arm. Then the divided beam will be collected by two photodetectors. This scheme then will sample the voltage at a precise point. After that, measured voltages at the delayed time will be random variables that follow the Gaussian statistics and are independent of each other in the processing stage. The process of generating random numbers differs from one implementation to another. For example, the configuration of [25] adjusts the Mach-Zehnder interferometer by adding a phase compensator which prevents the effects of the classically drifting phase that could dominate the quantum signal. After that, the data is digitized using an analog-digital-converter (ADC). Generating random

numbers in this setup exploits the fact that the mean of the Gaussian statistics is around 0 by setting it as a threshold. If the output voltage of the ADC is > 0 then the random bit would be 1, if the voltage is < 0 then the recorded random bit would be 0. Another scheme can be seen in [24], as they take the least-significant bit of the sampled voltage and subtract the difference between each two consecutive output voltages to remove the bias of the used ADC that classifies the bits to be even (odd) which will be translated into 0 (1). In order to distill the distribution and produce uncorrelated random numbers, some schemes introduced randomness extraction [26] as they use the same delay methodology explained before. In [27], they adjust the interferometer by correcting the phase drift which increased the generation rate substantially to reach 68 Gbps. This however needs a high-speed photodetector and a very stable interferometer which has a high cost as well as many experimental challenges.

In this chapter, we reviewed the general meaning of randomness and introduced a different type of RNGs including QRNGs. In chapter 2, we discuss the theory and statistics behind generating different light sources and explain their way of behaving. After that, we proceed with the description of different methods to detect these light sources in chapter 3. Finally, I propose a pseudothermal light based QRNG. The idea behind this implementation is to make use of the photon statistics to provide better and faster QRNGs as shown in chapter 4.

CHAPTER II

QUANTIZATION OF THE ELECTROMAGNETIC FIELD

Many of the problems in light interactions can be solved in the classical realm as the results match the theory perfectly. However, some problems need to be quantized in order to be solved because their classical description will give the wrong answer [28, 29]. Non-classical states of light or spontaneous emission can be examples of such problems. Thus, the quantization of the electromagnetic field leads to many important results in physics. Some of which to be discussed in this chapter where it will lead to the photon statistics of the thermal and coherent light sources.

2.1 Quantization of Single-Mode Field

In order to quantize the electromagnetic field, a closed infinite cavity with volume V in perfectly reflecting mirrors is used as seen in Figure 4. We can describe a classical monochromatic single-mode electromagnetic field that is polarized in the $\hat{x}$-direction as

$$\mathcal{E}(z,t) = \hat{x}q(t)\sqrt{2\omega^2/\epsilon_0 V}sinKz \tag{2.1.1}$$

where $\mathcal{E}(z,t)$ is the electric field in a linearly-polarized plane wave propagation in z-direction with time t. $\hat{x}$ is the direction of the polarization, $q(t)$ is a measure of the field amplitude, ω is the single-mode field oscillation frequency, ϵ_0 is the permittivity of free space. V is the volume of the cavity, K is the wavenumber of the frequency ω divided by the speed of light c.

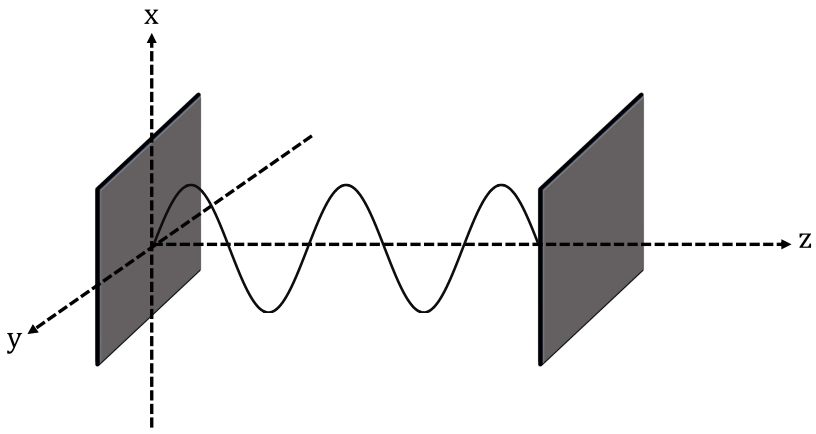

Figure 4: Quantizing the electromagnetic field using a one-dimensional cavity.

Knowing that Maxwell's equations in vacuum are satisfied by Equation 2.1.1, we add equation Equation 2.1.1 to the Maxwell–Faraday equation to find the magnetic field

$$\mathcal{B}(z,t) = \frac{\hat{y}}{c^2 K}\dot{q}(t)\sqrt{2\omega^2/\epsilon_0 V}cosKz \tag{2.1.2}$$

In this equation, the polarization is made into direction $\hat{y}$, and $\dot{q}(t)$ means that the value of the field amplitude measure is small and can be negligible. The energy density of the classical electromagnetic is found by

$$\eta = \frac{1}{2}[\epsilon_0 E^2 + B^2/\mu_0] \tag{2.1.3}$$

and its Hamiltonian is given by

$$\mathcal{H} = \frac{1}{2}\int_V dV[\epsilon_0 E^2 + B^2/\mu_0] \tag{2.1.4}$$

as dV is the volume element, E is the magnitude of $\mathcal{E}$, B is the magnitude of $\mathcal{B}$, and μ_0 represents the permeability of the free space. Combining Equation 2.1.1 and Equation 2.1.2 with Equation 2.1.4, we get

$$\mathcal{H} = 1/2(\omega^2 q^2 + p^2) \tag{2.1.5}$$

where p and q are the momentum and position operator. This is identical with the Hamiltonian of a simple harmonic oscillator that has a unit mass. Thus, the

quantization of a single-mode electromagnetic field can be done by rules of quantum mechanics on the quantization of the mentioned harmonic oscillator. We define the single-mode electromagnetic field Hamiltonian with the annihilation a and creation $a^\dagger$ operators by

$$\mathcal{H} = \hbar\omega(a^\dagger a + \frac{1}{2}) \tag{2.1.6}$$

$\hbar$ is Planck constant. The eigenstates $|n\rangle$ of the field which corresponds to the Hamiltonian are satisfied by

$$\mathcal{H}\,|n\rangle = \hbar\omega(n + \frac{1}{2}\,|n\rangle) \tag{2.1.7}$$

where $n = 0, 1, 2, 3, ...$ and represents the number of photons in $|n\rangle$. The state vector which corresponds to Equation 2.1.7 can be represented by a linear superposition of the energy eigenstates

$$|\psi\rangle = \sum\nolimits_n c_n\,|n\rangle \tag{2.1.8}$$

In order to find the electric field operator, we add the position operator in equation 3.138 of [9] and Equation 2.1.1 together

$$E(z,t) = \boldsymbol{E}_\omega(a + a^\dagger)sinKz \tag{2.1.9}$$

$\mathcal{E}_\omega$ represents the electric field of a photon and can be found by

$$\boldsymbol{E}_\omega = \sqrt{\frac{\hbar\omega}{\epsilon_0 V}} \tag{2.1.10}$$

Let us explore the physical meaning when we say *photon*. A photon is said to be created by the following equation

$$a\,|n\rangle = \sqrt{n}\,|n-1\rangle \tag{2.1.11}$$

or annihilated by

$$a^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle \tag{2.1.12}$$

This interprets the photon to be a single quantum mode of the electromagnetic field, which means that it fills the volume of the quantization. A photon in general describes

a multimode radiation packet whose average energy is $\hbar\omega$. It can be interpreted from the Fourier analysis that the localization of a wavepacket needs the modes to be in superposition, which means that photons are considered to be multimode objects.

2.2 Single-Mode Thermal Field

In order to show how comprehensive the quantum realm is compared to the classical one, let us consider the following. A single-mode electromagnetic field that has a Hamiltonian defined in Equation 2.1.6 with a state vector equals to Equation 2.1.8. It is seen that this quantum field is defined by infinitely many complex numbers without any classical fluctuation. Where a similar classical field can be completely defined by a complex number. The energy of a single-mode thermal field is given as

$$\langle \mathcal{H} \rangle = Tr\{\rho \mathcal{H}\} \tag{2.2.1}$$

We need to find the density matrix ρ in order to describe the latter field. This can be found classically if we maximize the entropy of the mode or by using the Lagrange multipliers. This is described classically to be

$$S = -k_B \sum_{\ell} P_\ell ln P_\ell \tag{2.2.2}$$

k_B is Boltzmann's constant, P_ℓ represents the probability to find our system in state ℓ, and both $\sum_\ell P_\ell$ are called the normalization condition [30]. To represent this in quantum physics, we replace the sum to be the trace, and P_ℓ by ρ as follows

$$S = -k_B Tr\{\rho ln \rho\} \tag{2.2.3}$$

Equivalently, the quantum version of the normalization condition is given by

$$Tr\{\rho\} = 1 \tag{2.2.4}$$

Maximizing the entropy is the goal under the constraints in Equation 2.2.1 and Equation 2.2.4. Let us first find the variation in S which corresponds to a little change in

ρ. Taking the partial derivative of Equation 2.2.3 we get

$$\delta S = -k_B Tr\{(1 + ln\rho)\delta\rho\} \tag{2.2.5}$$

Knowing that $Tr\{\delta\rho\} = 0$ and $Tr\{\mathcal{H}\delta\rho\} = 0$, we add them to Equation 2.2.5 so we get

$$\delta S = -k_B Tr\{(1 + ln\rho + \lambda + \beta\mathcal{H})\delta\rho\} \tag{2.2.6}$$

where λ and β are the Lagrangian multipliers of Equation 2.2.1 and Equation 2.2.4. Thus, to find the maximum entropy, the change in entropy δS must equal 0 for all $\delta\rho$ which gives

$$\rho = e^{-(1+\lambda)} exp(-\beta\mathcal{H}) \tag{2.2.7}$$

We add Equation 2.2.7 to Equation 2.2.4 to get

$$e^{1+\lambda} = Tr\{exp(-\beta\mathcal{H})\} \equiv Z \tag{2.2.8}$$

as Z is the system's partition function. Adding this to Equation 2.2.7 to find

$$\rho = \frac{exp(-\beta\mathcal{H})}{Tr\{exp(-\beta\mathcal{H})\}} = \frac{exp(-\beta\mathcal{H})}{Z} \tag{2.2.9}$$

Classically; we can find the Boltzmann coefficient as $\beta = \frac{1}{k_B T}$, where T is the temperature. What we have discussed previously has been on any Hamiltonian with thermal equilibrium, now we focus on the case in Equation 2.1.6. We remove $\hbar\omega/2$ which is called the zero-point energy. Then for simplicity, we will write $x = e^{-\beta\hbar\omega}$. Thus, we find Equation 2.2.9 to be

$$\rho = \frac{x^{a^\dagger a}}{Tr\{x^{a^\dagger a}\}} \tag{2.2.10}$$

Generally, ρ is expandable in any complete set of states similar to

$$\rho = \sum_n \rho_{nm} \sum_m |n\rangle \langle m| \tag{2.2.11}$$

We know that $\langle n| a^\dagger a |m\rangle = n\delta_{nm}$ which means that we can get the photon number expansion to be

$$\rho_{nm} = x^n[1 - x]\delta_{nm} \tag{2.2.12}$$

This shows that a thermal distribution is expandable on the diagonal by the photon number states, which makes the expectation of the electric field disappear in thermal equilibrium. Then, we can find the probability of finding n photons in a field $P(n)$ $(= \rho nn)$, which describes the photon statistics of thermal light. Using Equation 2.2.12 we get

$$|\Psi\rangle_{in} = |\psi\rangle_1 |\alpha_{LO}\rangle_2 \tag{2.2.13}$$

which is the Maxwell-Boltzmann distribution [30]. We can see that its maximum value occurs when $n = 0$. Thus we get that $max(P_{MB}(n)) = 1 - x$.

We find the mean photon number by

$$\bar{n} = \sum_{n=0}^{\infty} nP(n) \tag{2.2.14}$$

After some simplification, we get

$$\bar{n} = \frac{x}{1-x} \tag{2.2.15}$$

Then, writing x in its original form we get

$$\bar{n} = \frac{1}{e^{\hbar\omega/k_B T} - 1} \tag{2.2.16}$$

If we rewrite Equation 2.2.15 we find

$$x = \frac{\bar{n}}{\bar{n}+1} \tag{2.2.17}$$

Then, we can combine Equation 2.2.13 and Equation 2.2.17 for getting the following

$$P_{BE}(n) = \frac{1}{\bar{n}+1} \left(\frac{\bar{n}}{\bar{n}+1} \right)^n \tag{2.2.18}$$

which is the Bose-Einstein distribution [31]. Both Bose-Einstein and Maxwell-Boltzmann distributions can be used in describing any field with similar characteristics as a thermal field. Thus, an inherently thermal light source such as an LED or scattered coherent light source can be described by the these distributions under different circumstances [32]. An example of this distribution with different mean values is seen in Figure 5.

The average photon number fluctuations of a thermal light source [29] can be found by

$$\langle(\Delta n)^2\rangle = \langle\hat{n}^2\rangle - \langle\hat{n}\rangle^2 \tag{2.2.19}$$

We can also see that

$$\begin{aligned} \langle\hat{n}^2\rangle &= Tr(\bar{n}^2\hat{\rho}_{Th}) \\ &= \bar{n} + 2\bar{n}^2 \end{aligned} \tag{2.2.20}$$

This means that

$$\langle(\Delta n)^2\rangle = \bar{n} + \bar{n}^2 \tag{2.2.21}$$

Which is the variance of thermal light sources. Then, we can find its standard deviation (also known as root-mean-square) to be

$$\Delta n = \sqrt{\bar{n} + \bar{n}^2} \tag{2.2.22}$$

Both values are important to quantify the fluctuations in a statistical distribution. Also, they are compared with the variance and the standard deviation of Poisson distribution Table 1. While both Maxwell-Boltzmann and Poissonian distributions are used to represent thermal and coherent light sources, we can simulate both of them using the Gaussian distribution with different variance values (Figure 5). This is done for simplicity during the calculation of the min-entropy as done previously in the literature [26, 33, 34].

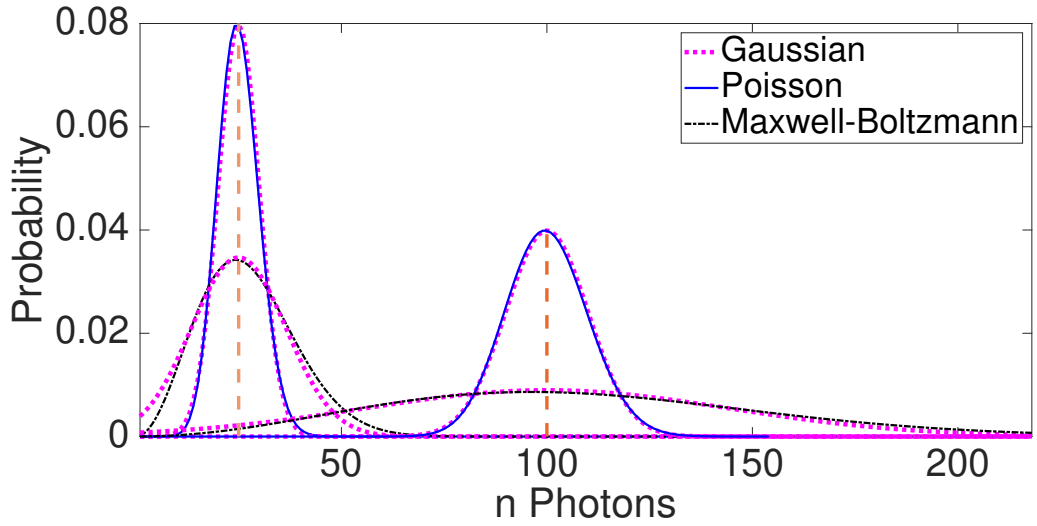

Figure 5: A simulation of the Gaussian distribution to fit both the Poissonian and the Maxwell-Boltzmann distributions at mean values of 25 and 100. The Gaussian and Poissonian look identical while the Maxwell-Boltzmann distribution is slightly skewed to the left of its average unlike the Gaussian distribution.

2.3 Coherent Fields

This section discusses different types of states from the simple harmonic oscillator which plays an important role in explaining the theory behind quantum random number generation. These states work on minimizing the Heisenberg uncertainty relation. One part of them is called coherent states, which lowers the spread of the momentum p and position q operators.

The method that will be used to explain coherent states indicates how close it is to classical explanation. This is done by finding the pure states of its harmonic oscillator that has average energy equal to the energy expressed classically. After that Ehrenfest's theorem is applied which can be explained as follows: the motion of center for a quantum wavepacket follows exactly the classical mechanics' laws. This is valid for free particles and particles in harmonic oscillators and uniform fields:

$$\begin{aligned} \langle\psi|p(t)|\psi\rangle &= p_c(t) \\ \langle\psi|q(t)|\psi\rangle &= q_c(t) \end{aligned} \tag{2.3.1}$$

where ψ is the wave function, and c represents the classical version of the variable. Adding Equation 2.3.1 to equation (3.131) in [30] we get the classical energy

$$\begin{aligned} \mathcal{H}_c &= \frac{p_c^2}{2} + \frac{\omega^2 q_c^2}{2} \\ &= \frac{1}{2}[\,\langle\psi|p(t)|\psi\rangle^2 + \omega^2\,\langle\psi|q(t)|\psi\rangle^2] \end{aligned} \tag{2.3.2}$$

Inserting this to equations (3.138, 3.139) in [30] then we can find

$$\mathcal{H}_c = \hbar\omega\,\langle\psi|a^\dagger|\psi\rangle\;\langle\psi|a|\psi\rangle \tag{2.3.3}$$

Then, the energy of the quantum oscillator becomes

$$\begin{aligned} \langle\mathcal{H}\rangle &= \langle\psi|\mathcal{H}|\psi\rangle \\ &= \hbar\omega\,\langle\psi|a^\dagger a|\psi\rangle \end{aligned} \tag{2.3.4}$$

this shows that the 0 of energy has been shifted by $\hbar\omega/2$. For ψ, the classical energy needs to be equal to the quantum energy. This can be expressed by the factorization condition

$$\langle\psi|a^\dagger|\psi\rangle\ \langle\psi|a|\psi\rangle = \langle\psi|a^\dagger a|\psi\rangle \tag{2.3.5}$$

We know that the mean of the operator a in state ψ equals to $\langle\psi|a|\psi\rangle$ and represents a complex number $\mathcal{E}(t)$ as long as a is non-Hermitian.

The definition in Equation 2.3.5 indicates that a coherent state is an eigenstate of the annihilation operator

$$a\,|\alpha\rangle = \alpha\,|\alpha\rangle \tag{2.3.6}$$

We can see that Equation 2.3.5 satisfies Equation 2.3.6. This can be implied by rewriting Equation 2.3.6 to be

$$\langle\psi|a^\dagger|\psi\rangle^2 = \langle\psi|a^\dagger a|\psi\rangle \tag{2.3.7}$$

According to the Gram–Schmidt process, by starting with $|\psi\rangle$ we can make a set that has an orthonormal basis and consists of $|\psi\rangle$ and a complementary infinite set of vectors $\{|J\rangle\}$. This can be expressed using the identity operator I as

$$I = |\psi\rangle\langle\psi| + \sum_J |J\rangle\langle J| \tag{2.3.8}$$

We insert this between the annihilation a and creation $a^\dagger$ operators to have

$$\begin{aligned}\langle\psi|a^\dagger a|\psi\rangle &= \langle\psi|a^\dagger|\psi\rangle\ \langle\psi|a|\psi\rangle + \sum_J \langle\psi|\,a^\dagger\,|J\rangle\,\langle R|\,a\,|\psi\rangle \\ &= |\,\langle\psi|a^\dagger|\psi\rangle\,|^2 + \sum_J |\,\langle J|\,a\,|\psi\rangle\,|^2\end{aligned} \tag{2.3.9}$$

When we equate this result with the left-hand-side of Equation 2.3.7 we get

$$\textstyle\sum_J |\,\langle J|\,a\,|\psi\rangle\,|^2 = 0 \tag{2.3.10}$$

Since that $\sum_J > 0$, then $\langle J|\,a\,|\psi\rangle$ must be equal to 0 for all terms of $|J\rangle$. This means that $a\,|\psi\rangle$ is orthogonal to all $|J\rangle$ such that

$$a\,|\psi\rangle = \lambda_\psi\,|\psi\rangle \tag{2.3.11}$$

This proves that the states which satisfy Equation 2.3.5 have to be eigenstates of a. This is written as $|\alpha\rangle$ that has an eigenvalue of α as can be seen in Equation 2.3.6.

We express the expansion of α using the number states $|n\rangle$ by the following

$$\begin{aligned} |\alpha\rangle &= \sum_n |n\rangle \langle n|a\rangle \\ &= \sum_n |n\rangle \langle 0| a^n/\sqrt{n!} |\alpha\rangle \\ &= \langle 0|\alpha\rangle \sum_n \frac{\alpha_n}{\sqrt{n!}} |n\rangle \end{aligned} \tag{2.3.12}$$

Knowing that $\langle\alpha|\alpha\rangle = 1$ we can get that $\langle 0|\alpha\rangle^2 = e^{-|\alpha|^2}$. When we choose a unit phase factor, we obtain the following

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_n \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{2.3.13}$$

This will give us the probability to find n photons in a coherent state to be

$$\begin{aligned} P_p(n) &= |\langle n|\alpha\rangle|^2 \\ &= e^{-|\alpha|^2} \frac{|\alpha^{2n}|}{n!} = e^{-\bar{n}} \frac{\bar{n}^n}{n!} \end{aligned} \tag{2.3.14}$$

Which is the Poisson distribution as can be seen in Figure 5. The Poisson statistics describe the result of the homodyne detector, which will be described explicitly in the next chapter. Let us show the coherent states using the vacuum state $|0\rangle$. This can be done by substituting equation (3.155) in [30] instead of $|n\rangle$ in Equation 2.3.13 to get

$$\begin{aligned} P_p(n) &= |\langle n|\alpha\rangle|^2 \\ &= e^{-|\alpha|^2} \frac{|\alpha^{2n}|}{n!} \end{aligned} \tag{2.3.15}$$

As it can be seen that we used $a|0\rangle = 0$ to reach the last step.

Finally, it is known for a Poisson distribution, that variance equals the average photon numbers and is written as

$$(\Delta n)^2 = \bar{n} \tag{2.3.16}$$

which means that the standard deviation is found by

$$\Delta n = \sqrt{\bar{n}} \tag{2.3.17}$$

as this result will be quite useful to find the min-entropy of any QRNG.

Light Types	Distribution	Average-Variance Relationship
Coherent (Laser)	Poissonian	$\bar{n} = \sigma^2$
Chaotic & Thermal	Super-Poissonian	$\bar{n} < \sigma^2$

Table 1: The difference of some photon distributions through different light sources.

CHAPTER III

MEASURING QUANTUM NOISE

In the previous chapter, we discussed the generation and the statistical behavior of photons produced from different light sources. This chapter will discuss the approach of detecting and measuring the resultant outputs, that is, the quantum noise. This analysis will be based on the noise continuous-wave laser beams alongside their amplitude, phase, and intensity. Throughout the chapter, we will discuss how to distinguish classical noise and quantum noise.

3.1 Direct Detection of Quantum Noise

The simplest method to detect quantum noise is to directly point a light source to a photodetector and examine the resultant output as seen in Figure 6. Assuming that the noise we have is Gaussian, then we will know everything about the type of variance for the noise. We can also use a spectrum analyzer, oscilloscope, or we can apply spectral decomposition of our data using fast Fourier transform (FFT). Such implementation is also used to find the intensity modulation from the beam of a laser, as both of them will be shown in the resultant spectrum. Mostly, when applying this method, the focus is to find the quantum noise which is the dominant effect of the signal-to-noise ratio (SNR).

Direct detection will result in an electrical noise power $p_i(\omega)$, where ω is the detection frequency. Such noise can be completely linked with quantum noise if the light source was a perfect laser. However, in reality, technical difficulties will appear and need to be solved. This needs a solid process that shows that the measured signal is truly quantum. $p_i(\omega)$, which can be shown on a spectrum analyzer, measures the photocurrent fluctuations, the amplification, and the contribution of the electronic

devices in the noise. For devices that are limited to quantum noise only, we get $p_{i,QNL}(\omega)$ so that all results are normalized to this value which will give the normalized variance

$$V_i(\Omega) = \frac{p_i(\omega)}{p_{i,QNL}(\omega)} \tag{3.1.1}$$

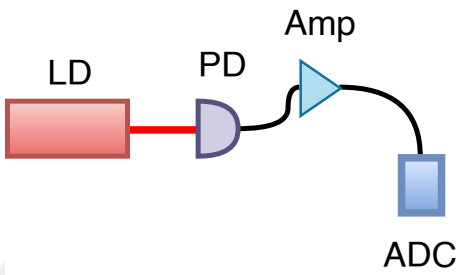

Figure 6: Schematic diagram of the direct detection method. The ADC is usually embedded in an oscilloscope or a spectrum analyzer. LD: laser diode; PD: photodetector; Amp: amplified; ADC: analog-digital-converter.

Decibel Scale

When we calibrate the measured noise, then we need to define a unit that describes this calibration. The output of the spectrum analyzer is mostly logarithmic, and the units shown are called "dBm" and they are logarithmic units to describe the power. In order to convert the Watt to dBm, we use the following formula [35]

$$p_i[dBm] = 10log_{10}\left(\frac{P[W]}{1[mW]}\right)$$

This unit is a unit of power, which means that if we have 1 mW of power then it equals 0 dBm. Note that these small numbers indicate the AC components of the power and not the total or DC power generated by the light source.

When the signal or noise change relatively, another unit of power is needed, which is called "dB" or "decibel". It interprets the ratio between both power levels. Similar to the dBm, we describe dBm logarithmically which means subtract the two powers

on the logarithmic scale as follows

$$\Delta p_{a,b}(\omega)[dBm] = 10log\left(\frac{P_a(\omega)}{P_b(\omega)}\right)$$

For example, if we amplify a signal by 6 dB, this means that we increased the power by $10^{6/10} = 3.98$. This shows that the increment is only by about a factor of $\sqrt{2}$. Such notation is used to describe any amplification or reduction of the signal is done by dB, which demonstrates changing the quadrature variance in the light.

The values of the noise power represent the time-varying averages. There exist some technical limitations in the noise spectrum such as *electronic noise*. Each photodetector comes with some electronic noise $P_{el}(\omega)$, which is also included in the noise spectrum. For this to be avoided, low-noise photodetectors can be specifically designed. Alternatively, we can measure the dark noise of the photodetector which happens when we block the photodetector. If we find the dark noise to be substantial, then the signal is corrected by taking it away from the measured signal after the measurement. We assume that both optical and electronic noise are included in the quadrature and are independent of each other. We also know that in some special types of detectors, the amount of dark noise is directly proportional to the photocurrent. In such cases, it is not enough and the usual measurement. Rather, more measurements in different values of the parameters (intensity and photocurrent level) are needed to examine the amount of electronic noise. One vital way to analyze the performance of a photodetector is by inspecting the noise equivalent power (NEP) of the photodetector. NEP is the level of power in which the amount of quantum noise is equivalent to the electronic noise, which is desirable to have in a photodetector. Most photodetectors have $p_{i,QNL}(\omega) = p_{el}(\omega)$. Typically, photodetectors have $NEP = 1\ mW$ while some advanced photodetectors have NEP of approximately 10 μW.

Another limitation is the *AC response*. The electronic circuits in photodetectors

have some gain that is dependent on the detecting frequency $g(\omega)$. Most photodetectors have a high roll-off frequency, which means their rate of reduction is considerably fast. This depends on the amplifier or diode used in the photodetector. There exists a sinusoidal curve that represents the frequency response. This is caused by an electronic mismatch in the photodetector's components. This is dealt with by normalizing the traces in Equation 3.1.1 as it does not affect the variance specifically.

We also need to consider the *efficiency* of the detector we use. Any photodetector cannot have perfect efficiency. Having low efficiency is similar to having a beamsplitter that swerves just a part of the light from its way. This is not critical for measurements that are only aiming for quantum noise. As the QNL can be measured by a portion of the light then compensate by electronic gain. Yet, knowing the efficiency is critical to find the SNR of the signal. Such an effect will be dissolved by having a photodetector with high efficiency. This shows that the efficiency and the electronic gain have different functions in photodetection.

Another problem that we might encounter can be the *power saturation*. Each detector can have a specific threshold when it comes to the maximum power to be received. This threshold differs from small avalanche photodiodes (APDs) which can handle only as little as a few milliwatts, up to large photodetectors that can handle power in the magnitude of Watts. If a photodetector receives more power than its threshold, then it most probably will be damaged due to the increase in heat inside. As the excessive light will heat the material of the diode and reverse-biased current will boost the ohmic heating. Also, if the amount of power sent to the photodetector was just below the threshold, the performance might not be optimal. As there are limited carriers in the material of detection which will increase the local intensity leading to less response. It is also important to have the illumination on the diode is uniform even while using the optimal power.

One last thing to be considered is the *amplifier saturation*. Some photodetectors

manifest an abnormal response due to having a high modulation signal which saturated the amplifier. Such saturation might hit one radio frequency but would affect different frequencies too. This can be avoided by recording high bandwidth spectra until reaching the roll-off frequency which guarantees not having a strong signal. Using some amplifiers back to back might be risky because the bandwidth would be broad in the first few amplifiers unlike the last few which is like using a low-pass filter by the output. This means that we would not see the high-frequency signals by the output, however, it causes the saturation in the early stages of the amplifiers. Saturation needs to be avoided because it might alter the noise spectrum in a broad bandwidth, and it might make the noise level lower.

After making sure all the mentioned complications have been avoided, now the QNL needs to be calibrated. This can be done by calculating the expected noise power $p_{i,QNL(\omega)}$ from Equation 3.1.1. Alternatively, we can calibrate the source by using a light source that is limited to quantum noise, such as a thermal white light source [35]. The way to do that is by emitting this thermal white light source on the detector while generating a non-varying DC photocurrent, and by recording the noise spectrum of the RF. Note that this measurement needs to be filtered in a close wavelength to the one used in the original experiment because the response in the photodiodes and the absorption depth depend on the wavelength. Also, the generation pattern needs to be approximately identical since the carrier depletion can be charged if the generation is localized. The last thing to take into consideration is, the diodes might be geometrically overfilled which makes it easy to heat and distort the measurement. Thus, it is very difficult for this measurement to distinguish the different noises from the quantum noise which is why another method is needed. The homodyne detection method, which eliminates classical noise and highlights Shot noise which is a sequence of quantum vacuum fluctuation.

Signal to Noise Ratio Definition

The SNR is defined as follows

$$SNR = \frac{\sigma^2_{total} - \sigma^2_{noise}}{\sigma^2_{noise}} \tag{3.1.2}$$

as σ^2_{total} is the variance of the whole signal, and σ^2_{noise} is the variance of the classical noise, and $\sigma^2_{quantum} = \sigma^2_{total} - \sigma^2_{noise}$ is the quantum variance. In the FFT spectrum of the signal, we can find the SNR by measuring the difference between the noise floor and the peak of the signal in dB directly. For low modulations, we need to consider the fact that both the noise and the signal are part of the peak which means that SNR = (signal peak - noise)/noise. Note that the electronic gain does not change the SNR. One last thing to be taken into account, when calculating the optical SNR by Equation 3.1.2, we need to consider the quantum efficiency and this includes the attenuation of the light source.

The theoretical signal level is defined by the shot noise for a light source that has Poissonian statistics which can be expressed as

$$P_Q = (2e\langle I\rangle \Delta f) R_L \tag{3.1.3}$$

where e corresponds to the charge of the electron, $\langle I\rangle$ to the average photocurrent, Δf to the bandwidth of the detector, and R_L to the load resistor [32]. The shot noise limit can be seen in Figure 12. Later on,

3.2 Homodyne Detection

As discussed in section 3.1, we use the direct detection technique to find the intensity noise of a light source. In a single-mode field, we combine a beamsplitter with two photodetectors to find the proportion of the quantum noise and the classical modulation. Yet this method is not sufficient to distinguish the difference between different quadratures as it mostly measures the amplitude or in phase quadrature. For that reason, we introduce a new parameter called the local oscillator which is used as a

reference beam for measuring various quadrature angles [36, 37]. For this beam to be a phase reference, it needs to be phase-locked with the input. There is a critical difference between a homodyne detector and a heterodyne detector. It is a homodyne detector if the input and the local oscillator are on the same frequency. On the other hand, for a heterodyne detector, the local oscillator is frequency shifted. One version of the homodyne detection method can be seen in Figure 7.

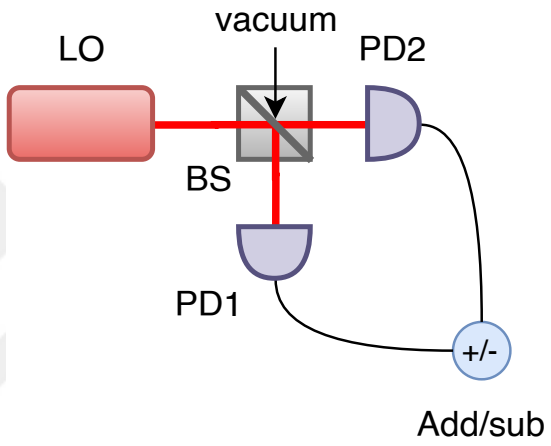

Figure 7: Homodyne detector. We mix the input signal, which is in our case the vacuum state, with a coherent signal called the local oscillator in a beam splitter. Then the split signals are collected by two identical photodetectors. The resultant signal is added or subtracted then processed after that. LO: local oscillator; BS: beam splitter; $PD_{1,2}$: photodetectors; Add/sub: adder or subtractor.

In the homodyne detection technique, we assume that both the input beam and the local oscillator come from the same source. However, in reality, this description can be much more complicated. This scheme is relatively similar to an interferometer. Both the local oscillator α_{lo} and input α_{in} beams are detected by two photodetectors $PD_{1,2}$. We can analyze the system's performance by utilizing classical mechanics.

The amplitudes of the beams are found by

$$\begin{aligned} \alpha_{in}(t) &= \alpha_{in} + \delta X_{1,in}(t) + j\delta X_{2,in}(t) \\ \alpha_{lo}(t) &= [\alpha_{lo} + \delta X_{1,lo}(t) + j\delta X_{2,lo}(t)]\, e^{j\phi_{lo}} \end{aligned} \tag{3.2.1}$$

where X_1 and X_2 are the quadrature amplitudes, and $e^{i\phi_{lo}}$ is the relative phase difference between the amplitudes of the local oscillator and the input beam. The latter can be changed by altering the length of the local oscillator arm. This is done by the fine-tuning of the propagation of the light into the beamsplitter. The output must be dominated by the local oscillator. Let us examine the case where the local oscillator beam has much more power than the input beam $\alpha_{lo}^2 \gg \alpha_{in}^2$. In this situation, we will have the output intensity dominated by the local oscillator which means that the intensity found on both photodetectors is equal

$$|\alpha_{D1}|^2 = |\alpha_{D2}|^2 = \frac{1}{2}|\alpha_{lo}|^2 \tag{3.2.2}$$

where α_{D1} and α_{D2} are the resultant beams of the D1 and D2. When comparing the proportional terms to α_{in}, we can leave out the proportional terms to α_{lo}. We can describe the signal coming out of the detectors using the conventional phase shift for a beam splitter, but we also shift the phase of on reflected beam by 180° as seen in Figure 8.

$$\begin{aligned} \alpha_{D1} &= \sqrt{1/2}[\alpha_{in}(t) + \alpha_{lo}(t)] \\ \alpha_{D2} &= \sqrt{1/2}[\alpha_{in}(t) - \alpha_{lo}(t)] \end{aligned} \tag{3.2.3}$$

The intensities (photocurrents) of both detectors are proportional to $|\alpha_{D1}|^2$ ($|\alpha_{D2}|^2$) and can be expressed as

$$|\alpha_{D1}|^2 = 1/2\left[|\alpha_{lo}(t)|^2 + \alpha_{lo}(t)\alpha_{in}^*(t) + \alpha_{in}(t)\alpha_{lo}^*(t) + |\alpha_{in}(t)|^2\right] \tag{3.2.4}$$

which is also equal to

$$\begin{aligned} |\alpha_{D1}|^2 &= 1/2[|\alpha_{lo}(t)|^2 + 2\alpha_{lo}\delta X_{1,lo}(t) \\ &+ 2\alpha_{lo}(\delta X_{1,in}(t)cos(\phi_{lo}) + j\delta X_{2,in}(t)sin(\phi_{lo}))] \end{aligned} \tag{3.2.5}$$

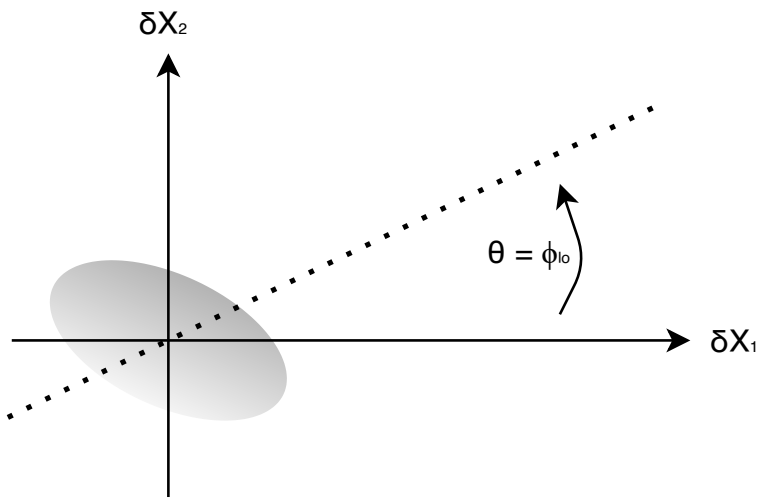

Figure 8: The projection of ϕ to the quadratures.

For having this approximation we neglect small terms since that we have much bigger values than them. Both α_{lo} and α_{in}^{*} were removed because we have $|\alpha_{lo}|^2$. We also removed $\alpha_{lo}\delta X^{*}$ since that we have $\alpha_{in}\delta X^{*}$. We also ignored the higher-order terms from δX. A similar result can be found in the other detector. Thus, the difference current can be defined as follows

$$i_{dif}(t) = 2\alpha_{lo}\left[\delta X_{1,in}(t)cos(\phi_{lo}) + j\delta X_{2,in}(t)sin(\phi_{lo})\right] \tag{3.2.6}$$

This shows that the difference photocurrent is depending on the amplitude of the local oscillator only while ignoring the effects of its noise or fluctuations. For example, the noise level of the local oscillator can be much higher than the QNL while the photocurrent can be still not influenced. Also considering the input beam, we realize that it is not affecting the photocurrent as long as its power is much less than the local oscillator's. We also see that the DC components cancel each other and we are only left with the AC components in $i_{dif}(t)$. After that, an AC amplifier or a splitter can be used to fluctuate the current. After that, we evaluate the variance in the current. An important remark here is that during the averaging process, the cross-terms such

as δX_1 and δX_2 cancel out each other. We get

$$\Delta i^2_{dif} = 4\alpha^2_{lo}[\delta X^2_{1,in} cos^2(\phi_{lo}) + \delta X^2_{2,in} sin^2(\phi_{lo})] \tag{3.2.7}$$

This result combines the fluctuations in two quadratures. Such that, we measure the variance of the amplitude in the quadrature when the phase $\phi_{lo} = 0$. We also measure the variance of the phase in the quadrature when $\phi_{lo} = \pi/2$. Alternatively, we can say that the fluctuating state which is under the angle $\theta = \phi_{lo}$ is measured by the homodyne detector with its variance. We can choose this angle when we scan the phase of the local oscillator.

We can also interpret this experiment by its sideband, as the relative phase θ changes in various modulation types. This change occurs between the lower and upper sidebands and the carrier frequency where the setup chooses only one phase. As the other phase modulation $\theta+90$ is not detected. Some specific quadrature in the modulation sideband is filtered out by the homodyne detector. As we fix the phase shift ϕ_{lo} in the local oscillator, we will get very sensitive detecting in some type of modulation. Such that, if $\phi_{lo} = 0$, then we only measure the amplitude modulation. And if $\phi_{lo} = 90$, then we only detect the phase modulation. The detection accuracy in this quadrature changes alongside $cos^2(\phi_{lo})$.

So far, We have calculated the outputs of the homodyne detector classically, let us investigate their correctness by going into the quantum realm. The homodyne detection technique represents a special case of the Mach-Zehnder interferometer which has been discussed in chapter 1 but using a 50/50 output mirror. We describe the two fields that are illuminated into the second beamsplitter by

$$\begin{aligned} \hat{a}_{in}(t) &= \alpha_{in} + \boldsymbol{\delta}\hat{\boldsymbol{X}}_{1,in}(t) + j\boldsymbol{\delta}\hat{\boldsymbol{X}}_{2,in}(t) \\ \hat{a}_{lo}(t) &= \left[\alpha_{lo} + \boldsymbol{\delta}\hat{\boldsymbol{X}}_{1,lo}(t) + j\boldsymbol{\delta}\hat{\boldsymbol{X}}_{2,lo}(t)\right] e^{j\phi_{lo}} \end{aligned} \tag{3.2.8}$$

Let us now analyze the quantum version of Equation 3.2.7 which finds the variance

of the photocurrent fluctuations

$$\begin{aligned}\Delta i_{dif}^2 &= 4\alpha_{lo}^2\left[\langle\boldsymbol{\delta}\hat{\boldsymbol{X}}_{1,in}^2\rangle cos^2(\phi_{lo}) + \langle\boldsymbol{\delta}\hat{\boldsymbol{X}}_{2,in}^2\rangle sin^2(\phi_{lo})\right] \\ &= 4\alpha_{lo}^2\left[V_{1,in}cos^2(\phi_{lo}) + V_{2,in}sin^2(\phi_{lo})\right] \end{aligned} \tag{3.2.9}$$

This equation will hold only when the beam of the local oscillator is much larger than the input beam ($\alpha_{lo} \gg \alpha_{in}$) [38].

As we saw that such little variation on the Mach-Zehnder interferometer we can measure the variance of one specific quadrature with all its quantum properties. Selecting a single quadrature is done by changing the phase angle for the local oscillator. When all quadratures are the same as it is while using only a coherent state, homodyne detection is not advantageous over direct detection. But once we introduce a new state - such as the vacuum state - then the variances in the quadratures start to change and the homodyne detector comes in handy.

Let us discuss some final points to note while using the homodyne detector. All the mentioned results are replicable even when the input intensity is too small, but it just needs to be smaller than the intensity of the local oscillator $|\alpha_{in}|^2 > |\alpha_{lo}|^2$. If the input beam has a close intensity to the local oscillator beam, then the intensity of the output changes drastically with a relative phase difference between the amplitudes of the local oscillator and the input beam ϕ_{lo}. Also, the resultant variance will be a combination of the variances of orthogonal quadratures. The toughest part of this experiment is to balance the setup. As we need to match the wavefront curvature and the amplitude at the outputs. This means that we need to use identical optical parts on both sides such as beamsplitters, and mirrors. We also need to consider the distance traveled for both beams (α_{lo}^2 and α_{in}^2) where they should be close to each other.

Photodetectors

As we see throughout this thesis, detectors are essential to understand and exploit the concepts of quantum physics. Let us briefly explain the mechanics of how photodetectors work. The schematic of the used photodetector (DET08CFC) in our experiment is seen in Figure 9. The photodetector receives light then converts it into a photocurrent called I_{PD}. The diode in the circuit operates on photoconductive mode which means that the diode is reversed biased. This increases the depletion junction width which decreases the junction capacitance but at the same time increases the responsivity of the photodetector. Such conditions might produce a high amount of dark current, unless a suitable material is chosen, which is the case for the detector we use. Thus, we find $I_O = I_{PD} + I_d$. Both shunt and series resistances have very little effects on the experiment we are proposing [39]. The load resistance is found in the coaxial cable connecting the photodetector to the oscilloscope. Alongside the output current, its job is to create a voltage to view on the oscilloscope.

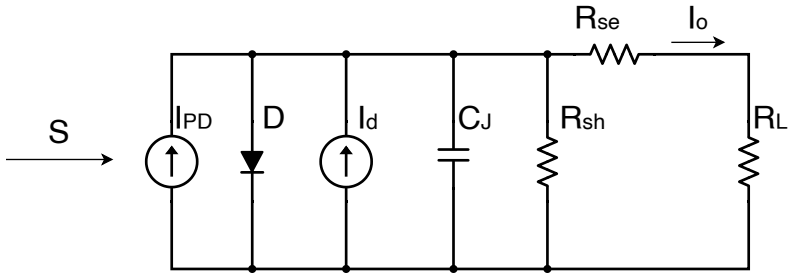

Figure 9: Schematic diagram to show the main components working inside our photodetectors. S: signal; I_{PD}: photodiode current; D: diode; I_d: dark current; C_J: junction capacitance; R_{sh}: shunt resistance; R_{se}: series resistance; I_o: output current; R_L: load resistance

CHAPTER IV

PSEUDOTHERMAL LIGHT BASED QUANTUM RANDOM NUMBER GENERATOR

The need for fast, reliable, and secure RNGs is growing alongside the daily growth of technology that can be seen in our modern life. QRNGs provide an ideal solution for that. Although they are not perfect yet, they are being improved regularly in order to solve all the loopholes that might be existing in them. One important aspect of any RNG (consequently QRNG) is its speed. In this thesis, I introduce a pseudothermal light based QRNG. The main idea behind our system is to exploit the photon statistics in order to improve the quality and speed of a QRNG application. We do that by implementing a slightly modified version of the homodyne detector. The modification is by adding a scattering surface (SS) to the homodyne detector which changes the photon statistics. This change drastically increases the speed of the QRNG as shown in the following sections. The goal behind using a SS in the setup is to produce a pseudothermal light source [40] and transform the photon statistics from Poissonian to super-Poissonian. This directly affects the variance of the distribution which plays a critical role in the quality and speed of QRNGs as will be seen in the following sections.

4.1 Experimental Setup

The experimental setup scheme is seen in Figure 10. When the homodyne setup is used for some experiments such as measuring squeezed light, there is usually a local oscillator alongside another light beam which is called the input beam. However, when implementing the homodyne detector in QRNGs, we block the other side of the

beam splitter in order to have the vacuum instead of the input beam. This is done to exploit the entropy of the vacuum state and mix it with the local oscillator. In our setup, our local oscillator is the beam of a continuous-wave single-frequency laser (NKT Koheras BASIK E15). This beam is illuminated into a beam splitter while blocking its other side which mixes the local oscillator with the vacuum state. Then two split beams emerge from the beam splitter. The first one is shined into a SS then detected by a photodetector (PD1), and the other beam is detected directly by an identical photodetector (PD2). The used photodetectors are fiber input InGaAs biased detectors (DET08CFC). After that, both photodetectors convert the coming beams into two photocurrents i_1 and i_2 which are subtracted using a subtractor. Then, we use an analog-digital-converter (ADC) to process the data. In our case, both the subtractor and the ADC are embedded in a fast oscilloscope (Lecroy WaveRunner 640Zi).

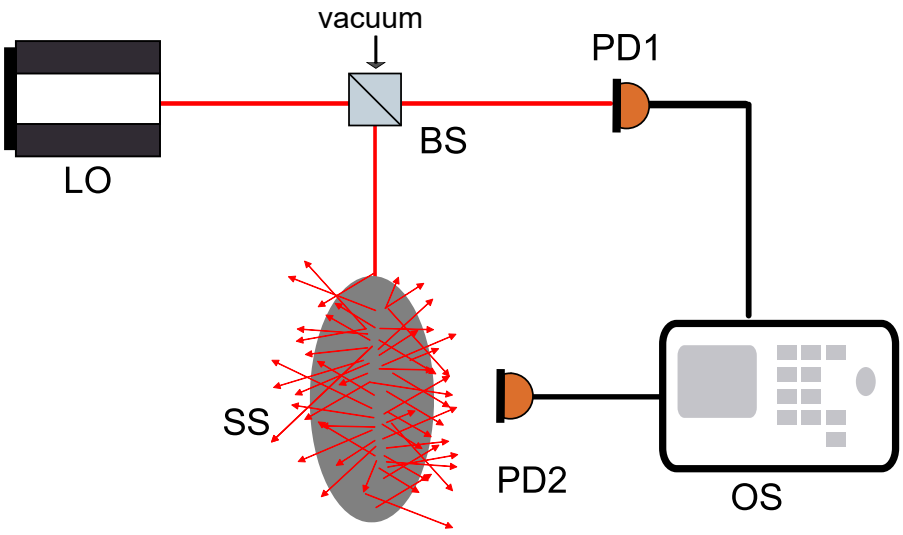

Figure 10: Schematic of the pseudothermal light based QRNG. Light from the local oscillator (LO) is split into two through a beam splitter (BS). The transmitted beam is connected directly to the photodetector PD1 and the reflected one is detected by PD2 after being scattered by a scattering surface (SS). The signals are subtracted from each other in the homodyne configuration to eliminate the classical noises (except electronic noise) using an oscilloscope (OS).

We focus on the applied scattering mechanisms in the experimental setup in order to choose the most suitable SSs. We know that both aluminum and silver have reflectivity for infrared and near-infrared/visible wavelengths [41]. Thus, mm radii unpolished aluminum and half-polished silver 5 coated objects are used in the experiment. Both aluminum and silver materials have one important common feature which is their rough surface that allows light beams to diffract in different directions and behave as pseudo-thermal light sources.

One major cause of increasing the amount of scattering of a surface for infrared light sources is the macroscopic deficiencies like deeper scratches [42]. The elliptical 900 silver object with relatively high purity has a rough surface with a root mean square roughness of 1.10 mm $\pm$ 0.05 mm. The aluminum object has a significantly low thickness of 0.02 mm and it is due to its highly uneven surface [43].

While different SSs have different scattering parameters, all result in a broadened distribution of the photon statistics. Figure 11 shows the distributions of the detected signal in homodyne configuration from a coherent light (blue), scattered light from half-polished silver (green), and scattered light from unpolished aluminum (red). The light from the laser exhibits Poissonian distribution. The random nature of scattering from a half-polished silver enhances the chaotic (thermal) characteristics of the light and broadens the distribution. Unpolished aluminum has a higher degree of scattering centers and the scattering is proportional to the surface roughness. Therefore, the distribution is further broadened compared to the silver case. This shows that chaotic behavior becomes more dominant when the scattering centers are more irregularly distributed.

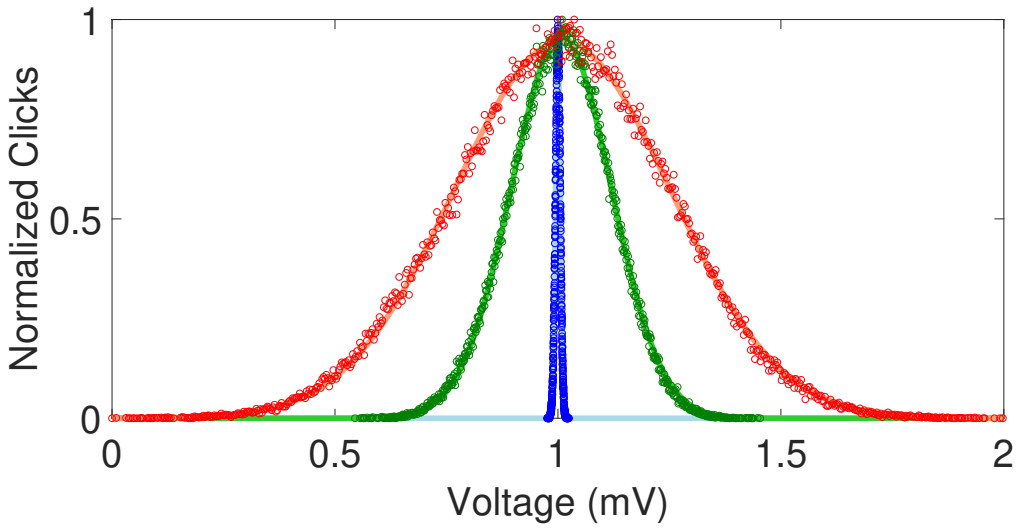

Figure 11: The normalized occurrences of the fluctuating signals are shown in three different cases. The signals are measured in homodyne configuration from a coherent light (blue), scattered light from half-polished silver (green), and scattered light from unpolished aluminum (red). While the blue curve follows the Poissonian distribution, the green and red curves follow the super-Poissonian statistics with a different full width at half maxima. The solid lines represent the Gaussian fit of the data points.

4.2 Entropy estimation

In order to ensure that the randomness we are extracting is predominantly quantum and not just electronic noise, we need to understand each noise source separately. This is necessary to ensure the validity of the extracted quantum noise and predict its entropy. To show the dominance of the quantum signal over the classical noise, the power spectra of two different signals are shown in Figure 12. The blue one shows the laser signal from the homodyne detection configuration. The red one is the classical noise which is measured by turning the laser off.

The most used way to measure randomness is by calculating any of the various types of entropy. Such calculations are about expressing the unexpectancy mathematically, or about quantifying the amount of surprise. The concept of entropy is coming from information theory and is expressed by bits. This is similar to the thermodynamic entropy but is taken into a natural formulation to process information and communicate. One main form of entropy is the Shannon entropy [44]. In a probability distribution P_X which has a random variable X, we find an outcome x of a discrete set $\mathcal{A}$ while having N possibilities for x, Shannon entropy of X can be found by

$$H(X) = -\sum_{x \in \mathcal{A}} P_X(x) log_2 P_X(x). \tag{4.2.1}$$

This finds how much information bits can be extracted in a single outcome on average. If we have an alphabet that has a uniform probability distribution and a cardinality $N = |\mathcal{A}|$, we can get all values with equal probability which can be described by $log_2 N$. As all the results are equally unexpected in this uniform random process and all the bits need to be used. However, in an uneven distribution, we can describe them with less number of bits. By using Shannon entropy, we roughly estimate the amount of randomness in a set of numbers. In the ideal case, we have a set of numbers that are uniformly distributed which has a Shannon entropy of almost $log_2 N$. Thus, having more Shannon entropy means extracting more randomness.

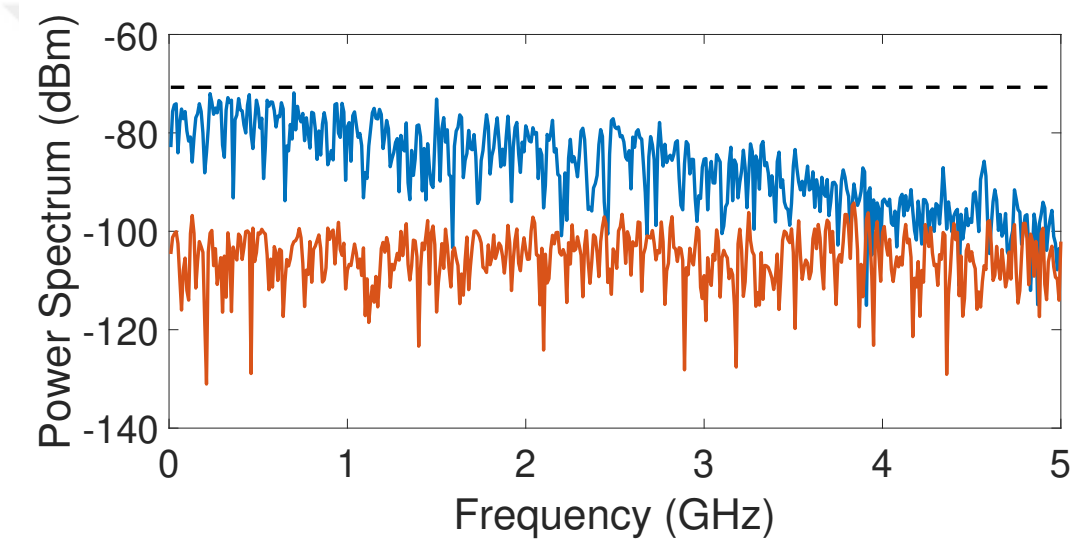

Figure 12: Power spectral density of the laser light from the homodyne detector (blue) alongside the electronic noise (orange). The black dotted line shows the theoretically calculated shot noise to be -70.73 dBm.

However, Shannon entropy still does not well quantify the randomness of a sequence [45]. This is why the need emerged to find a better method to precisely quantify randomness and to make it more compatible with randomness extractors. For that, a generalization of Shannon entropy called the Rényi entropy [46] was created and a specific case of it called min-entropy was employed for this manner. Min-entropy also a lower bound out of other Rényi entropies. For calculating min-entropy we need to give a few assumptions. The first is that our resultant signal from the homodyne setup is the sum of some electronic noise X_e and some quantum signal X_q. Hence, our signal is constructed as follows $X_t = X_e + X_q$. The second assumption is that we have the worst-case scenario, this means an eavesdropper can control the electronic noise X_e which makes it untrustable. The final one is that our signal follows the Gaussian distribution and is digitized using an ADC [47, 48]. We can define min-entropy as follows

$$H_{min}(X_q) = -log_2 \left[\underset{x \in \mathcal{A}}{max} P_q(x) \right] \tag{4.2.2}$$

It has the meaning of finding the probability to guess, in the first try, the result of the measurement for X in a known distribution. Thus, limiting the knowledge an adversary can obtain. Min-entropy depends on the variance depending on the photon distribution, they can be found in Equation 2.2.21 and Equation 2.3.16. The maximum value of a Gaussian distribution is $\frac{1}{\sqrt{2\pi}\sigma_q}$ where σ_q is the standard deviation which can be found from $\sigma_q = \sigma_t - \sigma_e$. Where σ_t is the standard deviation of the total signal, and σ_e is the standard deviation of the electronic noise which can be found by measuring the signal when the laser power is $0\,mW$. In our data, we find $\sigma_q = 4159.6$ which gives us a min-entropy of 13.4 per sample.

Randomness Extractors Randomness extraction is a method used to elicit a bunch of bits in the shape of a distribution that is almost uniform coming from biased and correlated bits [34]. The main purpose of randomness extraction methods is to improve the randomness of the raw data of a QRNG. This purpose is still attracting to

be used for the same reason, but recently this method has gained notable importance especially in the field of cryptography and computer science. It is also important because when we smooth the entropy source, Shannon Entropy function is maximized [48]. Different methods in the literature are used to extract randomness of QRNGs, some use Toeplitz-matrix hashing [48, 49] which needs a long seed to be used. Another extractor is the Trevisan extractor which needs a relatively shorter seed than the Toeplitz-matrix method. Although it is tested to have high security, the price to be paid for this high security is the limitation on its speed [48]. In this thesis, a randomness extractor is not deployed in order to compare the raw data of the coherent and thermal signals. Instead, the collected raw data of both signals is digitized by a fast comparator logic where below and above the mean values are labeled as 0 and 1, respectively.

4.3 Results

In this section, I will discuss the results which mainly compare the output of the conventional homodyne detector with the modified version of it.

4.3.1 Autocorrelation Function

The quality of randomness can be verified in a few ways. One of them is using the autocorrelation function in a bitstream. The meaning of the autocorrelation function is to manifest the correlation of any signal with its delayed version. This very much depends on the sampling rate of the raw data, as if the sampling rate is too high, the correlation between each bit and the next one gets higher [50]. The sampling rate of the oscilloscope is 40 GSps, which is much faster than the bandwidth of the detector we use (5 GHz) which means we need undersampling. The optimal undersampling value can be found through the autocorrelation function. This is since these samples give the shape of the primary approximation in the quality of the bitstream. The lag value shown corresponds to minimum autocorrelation which

indicates better randomness. When the minimum autocorrelation function occurs at small lag values, we can have the sampling rate be faster which means obtaining a higher final bit rate. We see in Figure 13, the autocorrelation functions for the scattered signals go around 0 faster than the autocorrelation function of the laser signal. We use this lag point for undersampling our signal. The lower value of the autocorrelation function of the scattered light shows better randomness characteristics compared to the laser light. The first autocorrelation value that intersects with zero happens at lag 10 for the unpolished aluminum. Dividing the oscilloscope's maximum sampling rate (40 GSps) by this 10 lag value gives 4 GSps. The Nyquist–Shannon sampling theorem states that we can sample our signal with twice the value found at the first lag which comes to zero [33]. This shows that 8 Gbps can be achieved maximally with the laser signal that is scattered from an unpolished aluminum SS. However, for the coherent source, we only get a rate of 3.2 Gbps. This is no surprise as the bandwidth of the detectors is 5 GHz and the subtraction of the signals is performed in the homodyne configuration.

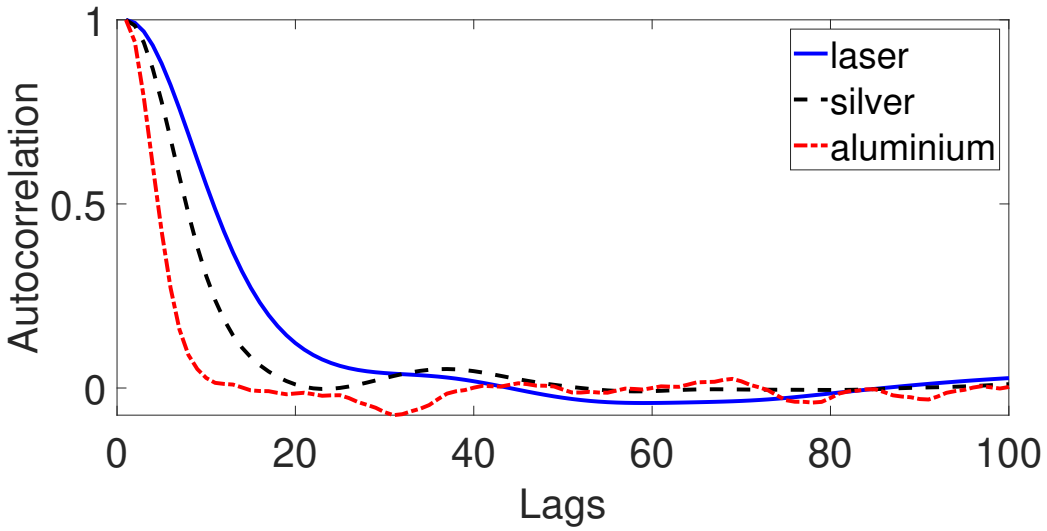

Figure 13: Autocorrelation functions measured by the oscilloscope show the analog signal from the laser directly (blue), after scattering half-polished silver surface (black), and after scattering of unpolished aluminum (red). The autocorrelation of the laser intersects with zero at a lag value of 44, half-polished silver at 22, unpolished aluminum at lag 10.

4.3.2 Randomness Tests Results

NIST test suite and TestU01 suite [8] is an example of the statistical randomness tests that are used to measure the ability of QRNGs to generate true randomness in the literature. Although such tests are designed to check RNGs that are based on algorithms, which means that they do not completely verify the quality of the RNG. Yet they are useful to test the RNG to some degree by showing that the produced numbers how low next-bit-predictability which proves not having a major pattern in them. As can be seen in Table 2, similar to [48], the data of coherent light in the homodyne scheme fails most NIST suite tests. On the other hand, when put under the same tests, undersampled scattered light data passes all the tests with the ideal sampling rate, which proves that scattered light improves the randomness of the stream bit without the need for post-processing.

Test Name	Coherent source	Pseudothermal source	p-Values for pseudothermal source
Frequency	Failure	Success	0.517
Block Frequency	Failure	Success	0.172
Runs	Failure	Success	0.328
Longest Run	Failure	Success	0.424
Rank	Failure	Success	0.688
DFT	Failure	Success	0.412
Non-Overlapping	Failure	Success	0.802
Overlapping	Failure	Success	0.206
Linear Complexity	Success	Success	0.593
Serial	Failure	Success	0.469
Approximate Entropy	Failure	Success	0.042
Cumulative Sums	Failure	Success	0.607
Random Excursions	Success	Success	0.738
R-E-V	Failure	Success	0.815

Table 2: The results of the NIST Suite Test applied on the signals of the homodyne detection for a coherent source and for pseudothermal source based on the scattering from a static aluminum scattering surface.

CHAPTER V

CONCLUSION

In this thesis, I propose a QRNG based on a pseudothermal light source. The first chapter gives an introduction to QRNGs in general. Why are they needed and what are they used for. Then described several types of various RNG implementations. In the second chapter, I explain the quantization of the electromagnetic field for thermal and vacuum fields. Then proceeded with the photon statistics behavior. After that, in the third chapter, I introduced different detection methods and showed how the homodyne detection can manifest better results in measuring the amplitude quadrature compared to other methods. In chapter four I present the experimental setup and results of our work.

I compare the photon statistics of the Poissonian and super-Poissonian sources and show that the ones that follow the super-Poissonian distribution manifest better randomness characteristics, this is done by optical scattering. We analyze the minimum lag value corresponding to the minimum autocorrelation function to demonstrate having a faster bit generation rate. We also test our random numbers in the randomness test suite.

In conclusion, adding a SS to one arm of the homodyne detector produces a faster random bit rate without compromising the randomness quality. The rate in our conventional homodyne detector is 3.2 Gbps where the improved version of it has a bit rate of 8 Gbps. We use this method as optical post-processing compared to the raw data of a coherent source. This idea can be used in commercial QRNGs which mostly use shot noise for the random bit generation. The proposed method has the potential to improve the speed and randomness quality of the optics based QRNGs.

Bibliography

[1] W. Hörmann, J. Leydold, and G. Derflinger, *Automatic Nonuniform Random Variate Generation*. Springer Berlin Heidelberg, 2004.

[2] P. L'Ecuyer, "Tables of linear congruential generators of different sizes and good lattice structure," *Mathematics of Computation*, vol. 68, pp. 249–261, Jan. 1999.

[3] Z. Gutterman, B. Pinkas, and T. Reinman, "Analysis of the linux random number generator," in *Symposium on Security and Privacy (S&P)*, IEEE, Mar. 2006.

[4] W. Killmann and W. Schindler, "A design for a physical RNG with robust entropy estimators," in *Cryptographic Hardware and Embedded Systems (CHES)*, pp. 146–163, Springer Berlin Heidelberg, Aug. 2008.

[5] G. Taylor and G. Cox, "Digital randomness," *IEEE Spectrum*, vol. 48, pp. 32–58, Sept. 2011.

[6] R. Motwani and P. Raghavan, "Randomized algorithms," *ACM Computing Surveys*, vol. 28, pp. 33–37, Mar. 1996.

[7] J. E. Gentle, *Computational Statistics*. Springer New York, 2009.

[8] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," tech. rep., NIST: National Institute of Standards and Technology, 2010.

[9] P. Meystre and M. Sargent, *Elements of quantum optics*. Springer Science & Business Media, 2007.

[10] R. Gennaro, "Randomness in cryptography," *IEEE Security & Privacy Magazine*, vol. 4, pp. 64–67, Mar. 2006.

[11] S. M. Bellovin, "Defending against sequence number attacks," *Internet Engineering Task Force (IETF)*, 1996.

[12] H.-W. Li, Z.-Q. Yin, S. Wang, Y.-J. Qian, W. Chen, G.-C. Guo, and Z.-F. Han, "Randomness determines practical security of BB84 quantum key distribution," *Scientific Reports*, vol. 5, Nov. 2015.

[13] J. Bouda, M. Pivoluska, M. Plesch, and C. Wilmott, "Weak randomness seriously limits the security of quantum key distribution," *Physical Review A*, vol. 86, Dec. 2012.

[14] A. C. Yao, "Theory and application of trapdoor functions," in *23rd Annual Symposium on Foundations of Computer Science (SFCS)*, IEEE, Nov. 1982.

[15] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, pp. 1484–1509, Oct. 1997.

[16] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, pp. 1301–1350, Sept. 2009.

[17] J. Rarity, P. Owens, and P. Tapster, "Quantum random-number generation and key sharing," *Journal of Modern Optics*, vol. 41, pp. 2435–2444, Dec. 1994.

[18] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, "Violation of Bell's inequality under strict Einstein locality conditions," *Physical Review Letters*, vol. 81, pp. 5039–5043, Dec. 1998.

[19] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Review of Scientific Instruments*, vol. 71, pp. 1675–1680, Apr. 2000.

[20] P. X. Wang, G. L. Long, and Y. S. Li, "Scheme for a quantum random number generator," *Journal of Applied Physics*, vol. 100, p. 056107, Sept. 2006.

[21] M. Naruse, M. Berthel, A. Drezet, S. Huant, M. Aono, H. Hori, and S.-J. Kim, "Single-photon decision maker," *Scientific Reports*, vol. 5, Aug. 2015.

[22] C. Henry, "Theory of the linewidth of semiconductor lasers," *IEEE Journal of Quantum Electronics*, vol. 18, pp. 259–264, Feb. 1982.

[23] M. Lax, "Classical noise. v. noise in self-sustained oscillators," *Physical Review*, vol. 160, pp. 290–307, Aug. 1967.

[24] H. Guo, W. Tang, Y. Liu, and W. Wei, "Truly random number generation based on measurement of phase noise of a laser," *Physical Review E*, vol. 81, May 2010.

[25] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," *Optics Letters*, vol. 35, p. 312, Jan. 2010.

[26] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," *Optics Express*, vol. 20, p. 12366, May 2012.

[27] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, "The generation of 68 gbps quantum random number by measuring laser phase fluctuations," *Review of Scientific Instruments*, vol. 86, p. 063105, June 2015.

[28] M. O. Scully and M. S. Zubairy, *Quantum Optics*. Cambridge University Press, 1997.

[29] C. Gerry and P. Knight, *Introductory Quantum Optics*. Cambridge University Press, 2004.

[30] P. Meystre and M. Sargent, *Elements of Quantum Optics*. Springer Berlin Heidelberg, 2007.

[31] E. Hanamura, Y. Kawabe, and A. Yamanaka, *Quantum Nonlinear Optics*. Springer Berlin Heidelberg, 2007.

[32] M. Fox, *Quantum optics: an introduction*, vol. 15. Oxford University Press, 2006.

[33] J. Haw, S. Assad, A. Lance, N. Ng, V. Sharma, P. Lam, and T. Symul, "Maximization of extractable randomness in a quantum random-number generator," *Physical Review Applied*, vol. 3, May 2015.

[34] Y. Shi, B. Chng, and C. Kurtsiefer, "Random numbers from vacuum fluctuations," *Applied Physics Letters*, vol. 109, p. 041101, July 2016.

[35] H.-A. Bachor and T. C. Ralph, *A Guide to Experiments in Quantum Optics*. Wiley, 2019.

[36] H. P. Yuen and J. H. Shapiro, "Quantum statistics of homodyne and heterodyne detection," in *Coherence and Quantum Optics IV*, pp. 719–727, Springer US, jun 1978.

[37] D. F. Walls and P. Zoller, "Reduced quantum fluctuations in resonance fluorescence," *Physical Review Letters*, vol. 47, pp. 709–711, Sept. 1981.

[38] U. Leonhardt, *Essential Quantum Optics*. Cambridge University Press, 2009.

[39] ThorLabs, *Fiber Input InGaAs Biased Detector User Guide*, 2019. Rev E.

[40] F. Devaux, K. P. Huy, S. Denis, E. Lantz, and P.-A. Moreau, "Temporal ghost imaging with pseudo-thermal speckle light," *Journal of Optics*, vol. 19, p. 024001, Dec. 2016.

[41] R. Steinkopf, A. Gebhardt, S. Scheiding, M. Rohde, O. Stenzel, S. Gliech, V. Giggel, H. Löscher, G. Ullrich, P. Rucks, A. Duparre, S. Risse, R. Eberhardt, and A. Tünnermann, "Metal mirrors with excellent figure and roughness," in *Optical Fabrication, Testing, and Metrology III* (A. Duparré and R. Geyl, eds.), SPIE, Sept. 2008.

[42] H. E. Bennett, "Scattering characteristics of optical materials," *Optical Engineering*, vol. 17, Oct. 1978.

[43] D. Vukobratovich and J. P. Schaefer, "Large stable aluminum optics for aerospace applications," in *Optomechanics 2011: Innovations and Solutions* (A. E. Hatheway, ed.), SPIE, Sept. 2011.

[44] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, July 1948.

[45] B. Chor and O. Goldreich, "Unbiased bits from sources of weak randomness and probabilistic communication complexity," in *26th Annual Symposium on Foundations of Computer Science (SFCS)*, IEEE, Oct. 1985.

[46] A. Rényi *et al.*, "On measures of entropy and information," in *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, The Regents of the University of California, June 1961.

[47] R. J. Glauber, "Coherent and incoherent states of the radiation field," *Physical Review*, vol. 131, pp. 2766–2788, Sept. 1963.

[48] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," *Physical Review A*, vol. 87, June 2013.

[49] Z. Cao, H. Zhou, X. Yuan, and X. Ma, "Source-independent quantum random number generation," *Physical Review X*, vol. 6, Feb. 2016.

[50] H. Zhou, X. Yuan, and X. Ma, "Randomness generation based on spontaneous emissions of lasers," *Physical Review A*, vol. 91, June 2015.

VITA

Abdulrahman Dandaşi has received his bachelor's degree from the Electrical and Electronics Engineering Department at Ozyegin University in 2018. He joined Dr. Durak's group as an intern at "Quantum Optics Laboratory" for one semester. After that, he started his master's degree in the same lab. His main research interest includes quantum optics and quantum communication. His thesis focuses on quantum random number generators.