Universidade de Aveiro
2021

Maurício de Jesus Ferreira

Geração de Números Verdadeiramente Aleatórios Baseados em Ruído Quântico

Quantum-Noise Based True Random Number Generation

Universidade de Aveiro
2021

Maurício de Jesus Ferreira

Geração de Números Verdadeiramente Aleatórios Baseados em Ruído Quântico

Quantum-Noise Based True Random Number Generation

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Física, realizada sob a orientação científica do Doutor Nelson de Jesus Cordeiro Muga, Investigador no Instituto de Telecomunicações de Aveiro, e do Doutor Nuno Alexandre Peixoto Silva, Investigador no Instituto de Telecomunicações de Aveiro.

o júri / the jury

presidente / president

Professor Doutor Manuel Almeida Valente
Professor Associado da Universidade de Aveiro

vogais / examiners committee

Professor Doutor Ariel Ricardo Negrão da Silva Guerreiro
Professor Associado da Faculdade de Ciências da Universidade do Porto

Doutor Nelson de Jesus Cordeiro Muga
Investigador Auxiliar do Instituto de Telecomunicações

acknowledgements

First of all, I would like to express my sincere gratitude to my supervisors, professor Dr. Nelson De Jesus Cordeiro Muga, and professor Dr. Nuno Alexandre Peixoto Silva, for guiding me throughout this journey. I thank you both for the incredible support, the contributions in the discussion of the results, and the suggestions to improve the structure and the writing of this work. To Daniel Pereira without whom the experimental component would be incomplete, and who endured my many questions.

To the University of Aveiro, and Instituto de Telecomunicações for providing all the conditions that made this work possible. In particular, to the projects DSPMetroNet (POCI-01-0145-FEDER-029405), QuantumPrime (PTDC/EEI-TEL/8017/2020), Q.DOT (POCI-01-0247-FEDER-039728), and UIDB/50008/2020-UIDP/50008/2020 (actions DigCORE and QuRunner), who provided all the necessary materials.

To the Programme New Talents in Quantum Technologies of the Gulbenkian Foundation (Portugal) who supported this work through their scholarship program.

To all those who helped me in the most difficult moments. To my colleagues for their friendship, many suggestions, and welcome work breaks. To a special group chat for always having my back and teaching me the importance of complementary colors.

To Ana for always being present and supporting me all the way. To my family for their unshakable trust during all these years. To my sister who always understood when I was not there.

Thank you.

palavras-chave

Gerador quântico de números aleatórios, Flutuações de amplitude em quadratura, Estado de vácuo, Extração de aleatoriedade, Deteção homódina.

resumo

Geradores quânticos de números aleatórios (QRNGs) prometem sistemas informação-teoricamente seguros explorando as propriedades intrinsecamente probabilísticas da mecânica quântica. No entanto, experimentalmente, um conjunto de pressupostos é tipicamente imposto sobre os dispositivos experimentais. Nesta dissertação, analisou-se uma abordagem para geração de números aleatórios que explora as flutuações de amplitude em quadratura de um estado vácuo. Para tal, recorre-se a um esquema de deteção homodina que permite um elevado desempenho e estabilidade, requerendo apenas dispositivos de baixo custo.

Um modelo matemático das diferentes etapas do gerador foi desenvolvido de forma a fornecer uma prova de segurança, e contabilizou-se o ruído de discretização introduzido pelo conversor analógico-digital. Adicionalmente, caracterizou-se o impacto de imperfeições experimentais como a resolução do conversor analógico-digital e a presença de ruído em excesso como consequência de uma deteção não balanceada. Uma abordagem para estimar esta contribuição no modelo de entropia de Shannon foi também proposta e experimentalmente verificada.

Adicionalmente, uma implementação em tempo-real foi caracterizada. A curva de caracterização do detetor homodino foi experimentalmente verificada, e uma preponderância de ruído quântico observado para potências óticas inferiores a $45.7\,\mathrm{mW}$. Através de uma estimativa da *min-entropy* condicionada ao ruído eletrónico, aproximadamente 8.39 bits por medição podem ser extraídos, o que corresponde a uma taxa de geração máxima de $8.23\,\mathrm{Gbps}$. Estes podem ser extraídos a uma taxa de $75\,\mathrm{Mbps}$ com um parâmetro de segurança de 2^{-105}, ilustrativo da qualidade desta implementação, através de um algoritmo eficiente de multiplicação de matrizes de Toeplitz. Posteriormente, o esquema foi validado, passando todos os testes estatísticos das baterias NIST, DieHarder, e SmallCrush, assim como a maioria das avaliações contidas na bateria Crush.

Por último, foi proposta uma abordagem para integrar esta fonte de entropia num canal de comunicação clássico, removendo desta forma a necessidade de uma implementação dedicada. Após avaliação das condições de preponderância do ruído quântico, foram observadas taxas de geração até $1.3\,\mathrm{Gbps}$. Os números obtidos foram também submetidos à bateria de testes do NIST, passando consistentemente todas as avaliações. Adicionalmente, a constelação de modulação de amplitude em quadratura obtida viabiliza a operação multifuncional do sistema.

keywords

Quantum random number generation, Quadrature amplitude fluctuations, Vacuum state, Randomness extraction, Homodyne detection.

abstract

Quantum Random Number Generators (QRNGs) promise information-theoretic security by exploring the intrinsic probabilistic properties of quantum mechanics. In practice, their security frequently relies on a number of assumptions over physical devices. In this thesis, a randomness generation framework that explores the amplitude quadrature fluctuations of a vacuum state was analyzed. It employs a homodyne measurement scheme, which can be implemented with low-cost components, and shows potential for high performance with remarkable stability.

A mathematical description of all necessary stages was provided as security proof, considering the quantization noise introduced by the analog-to-digital converter. The impact of experimental limitations, such as the digitizer resolution or the presence of excess noise due to an unbalanced detection, was characterized. Moreover, we propose a framework to estimate the excess entropy introduced by an unbalanced detection, and its high impact within the Shannon entropy model was experimentally verified.

Furthermore, a real-time dedicated QRNG scheme was implemented and validated. The variance characterization curve of the homodyne detector was measured, and the quantum fluctuations were determined to be preponderant for an impinging power $P_{\mathrm{LO}} < 45.7\,\mathrm{mW}$. By estimating the worst-case min-entropy conditioned on the electronic noise, approximately 8.39 true random bits can be extracted from each sample, yielding a maximum generation rate of $8.23\,\mathrm{Gbps}$. With a length-compatible Toeplitz-hashing algorithm, these can be extracted at $75\,\mathrm{Mbps}$ with an upper security bound of 2^{-105}, which illustrates the quality of this implementation. Moreover, the generation scheme was validated and verified to pass all the statistical tests of the NIST, DieHarder, and TestU01's SmallCrush batteries, as well as most of TestU01's Crush evaluations.

Finally, we propose a framework for time-interleaving the entropy source within a classical communication channel, which removes the need for a dedicated generation device. After assessing the conditions where quantum noise is dominant, support for generation rates up to $1.3\,\mathrm{Gbps}$ was observed. The random bitstream was subjected to the NIST randomness test suite and consistently passed all evaluations. Moreover, a clean quadrature phase shift keying constellation was recovered, which supports the multi-purpose function of the scheme.

Contents

List of Figures

Acronyms

ADC Analog-to-digital Converter.

BER Bit Error Rate.

BS Beamsplitter.

CMRR Common-mode Rejection Ratio.

CSPRNG Cryptographically-secure PRNG.

DAC Digital-to-analog Converter.

ES Entropy Source.

FPGA Field-programmable Gate Array.

KS Kolmogorov-Smirnov.

LO Local Oscillator.

OPM Optical Power Meter.

OTP One Time Pad.

PBS Polarization Beamsplitter.

PC Polarization Controller.

PD Photodetector.

PRNG Pseudorandom Number Generator.

QCNR Quantum-to-classical Noise Ratio.

QKD Quantum Key Distribution.

QOKD Quantum Oblivious Key Distribution.

QPSK Quantum Phase Shift Keying.

QRNG Quantum Random Number Generator.

RIN Relative Intensity Noise.

RN Random Number.

RNG Random Number Generator.

TIA Transimpedance Amplifier.

TRNG True Random Number Generator.

VOA Variable Optical Attenuator.

Chapter 1

Introduction

Randomness is a deep philosophical concept that has always paradoxically intrigued and unsettled humanity. It clashes with our inherent desire to understand the things around us and negates our predisposition to establish intent or causality in all circumstances. In fact, throughout history, randomness was intertwined with ideas of coincidence, luck, and fate that tried to confer meaning upon its nature. Science has not been impervious to such notions, as illustrated by Laplace's beliefs on causal determinism and the fundamentally predictable nature of the universe [1]. Somewhat ironically, the emergence of quantum mechanics has made randomness an unavoidable aspect of modern physics. Nonetheless, such thoughts have seldom been quieted, as sentiments such as those famously professed by Einstein reveal: "As I have said so many times, God doesn't play dice with the world."

Although not immediately apparent, defining the attribute of being random is itself a non-trivial question. It is unavoidable to look at the statistical notions of distributions and probabilities to derive its properties. Indeed, some of the earliest efforts to understand the laws surrounding randomness were inspired by chance games and population studies. Later contributions from the field of thermodynamics, where randomness assumed a fundamental role in the kinetic theory of gases, significantly developed probability theory and helped uncover the statistical properties that emerge from a set of random events [2]. While such notions are useful, the defining property of randomness is the unpredictability of individual outcomes, which can only be applied to a set of Random Numbers (RNs), rather than to any individual value [3]. This does not, however, necessarily imply an equiprobability of outcomes. One can thus describe randomness as the attribute of a source of uncorrelated values that follow a certain statistical distribution [4]. Nevertheless, in practical applications, and especially in cryptography, a uniform distribution is typically expected so that no meaningful information can be extracted. For this reason, efforts to certify randomness by evaluating the statistical properties of the supposedly random sets typically operate under the assumption of uniformity.

In the 1950s, the concept of Kolmogorov complexity was developed, describing the length of the shortest algorithm that can produce the evaluated sequence. Here, a random sequence is distinguishable by its incompressibility and consequent high Kolmogorov complexity [5]. Unfortunately, despite the development of numerous other statistical tests [6, 7, 8], it is impossible to confidently certify randomness. A sequence that passes a large number of evaluations certainly has properties that closely resemble those of a random one, but could still have been carefully designed using some deterministic process. In this case, its randomness is only apparent, as the set can be easily reconstructed by an agent with knowledge of the respective generation process. Furthermore, the question of to whom the sequence is random should also be considered. The unpredictability of a sequence to a given agent does not imply its randomness, and even a truly random sequence is predictable if publicly stored. Thus, more than a property of any sequence, randomness emerges from the generation method and is conditioned upon the maximum information that any agent can gather [3]. Any certification process should therefore consider both the randomness source itself and its privacy [9].

RNs play an essential role in numerous contemporary applications such as in numerical simulations, statistic analysis, decision-making, or even lotteries and other games of chance [3, 4, 10, 11]. In fact, its presence is ubiquitous in our daily days. They are, for example, used in statistical sampling to assure a representative and unbiased sample in scientific studies or other selection processes. In simulation, they are fundamental to model the behavior of systems whose numerical analysis proves too complex. Here, Monte Carlo methods are a particularly notable instance of the indispensability that RNs have assumed in scientific research and engineering applications. Moreover, any randomized or non-deterministic algorithms, such as neural networks or genetic simulations, will require a randomness source [11]. In fundamental sciences, RNs are also necessary to guarantee that no biases are introduced in the experimental results. This is particularly important in trials or simulations dealing with quantum mechanics, where randomness plays a central role. Notably, they are required to select the measurement basis on loophole-free Bell inequality tests [12].

It is, however, in cryptography that the importance of randomness is most significant. Indeed, RNs are used as random keys or initialization sequences (*seeds*) in the encryption, authentication, and digital signature protocols that support much of the modern communication infrastructure [13]. Contemporary cryptographic systems generally rely on the assumption that an adversary does not have enough computational power to break the protocol's security. The public-key protocol RSA, for example, relies on the hard problem of factorizing the product of two large prime numbers [14]. In accordance with Kerckhoffs's principle, these systems must be secure even if all details of the implementation (except for the key itself) are known [10]. Unintentionally, although often overlooked, this binds the security proof to the statistical properties of the random keys used. If the randomness source is structurally predictable or susceptible to be jeopardized by an attacker, the entire protocol is compromised even if the underlying algorithm is secure [2]. As a matter of fact, this is the case even for the unconditional secure One Time Pad (OTP) cipher, where the message is encrypted and decrypted by modular addition with a single-use previously shared secret key [3, 15]. In any case, a cryptographic system is only as secure as its weakest link. The recent emergence of post-quantum cryptographic protocols, as well as Quantum Key Distribution (QKD) and Quantum Oblivious Key Distribution (QOKD) algorithms, which require high-quality RNs to be secure [16, 17], is bound to guarantee an increase in the demand for fast and reliable randomness generation schemes in the forthcoming years.

1.1 State of the art

The first publicly available sources of randomness circulated in the form of pre-compiled tables drawn from a variety of methods [4]. In 1939, one of the first purposefully built mechanical Random Number Generators (RNGs) was used to compile a list of 100 000 numbers. These tables allowed easy access to relatively large amounts of RNs in a time when mechanical methods were too slow or inaccessible. Perhaps the most famous example, entitled "A million random digits with 100 000 normal deviates", was published in 1955 by the RAND corporation by extracting the output of an electronic roulette wheel [10]. Despite their popularity, such practices quickly proved to be inadequate for the growing demand due to memory limitations and the inconvenience of preparing such compilations. With the introduction of the first computers, the interest for on-demand algorithmic RNGs quickly arose [4].

Since 1946, when John von Neumann first suggested its middle-squared algorithm, Pseudorandom Number Generators (PRNGs) have traditionally been used as randomness sources [4]. These resort to deterministic algorithms to obtain an apparently unpredictable sequence from a shorter random key, the initial seed. As such, the yielded randomness follows the definition presented by Kolmogorov and is solely based on computational complexity [3]. An ideal PRNG should stand against the continuous scrutiny of every statistical test applied, such that, to an adversary, its output is indistinguishable from a truly random sequence. Even so, as Neumann himself pointed, such deterministic solutions cannot truly yield random results since their output is only dependent on the seed and the algorithm itself. Consequently, an inherent periodicity can be found,

and sufficient knowledge of these conditions allows the recreation of the entire pseudo-random sequence. Ironically, this reproducibility can be an advantage in applications such as simulations, where one may want to repeat a certain result [10]. In fact, several different implementations, such as linear congruential generators or linear shift feedback registers, have materialized and the best can pass numerous tests and present long-period cycles. The most widely used PRNG, the standard Mersenne Twister, belongs to the latter category and presents a period of $2^{19937} - 1$ [10].

Unfortunately, due to their high output rates and easiness of implementation, the limitations of these computational methods tend to be overlooked. A PRNG is obviously susceptible to cryptanalysis from an adversary looking to predict its outcome and is thus woefully inadequate for applications such as cryptography, where unpredictability is required [18]. The output of the standard Mersenne Twister, for example, can be deduced from a sufficiently long output sequence [10]. As such, the use of the so-called Cryptographically-secure PRNGs (CSPRNGs) is recommended in critical applications. Nonetheless, the prospect of increasing computational power and the maturity of quantum computation makes these implementations poor alternatives in the long run. In fact, carelessness in implementing PRNGs has already resulted in several disasters. Examples such as the Debian SSL generator, which was allowed to be vulnerable for two years, and the infamously bad RANDU generator, which was widely employed in the 1960s, show only a glimpse of the consequences of a vulnerable PRNG. RNG attacks are suspected to be the cause of several high-notoriety security breaches such as the Bitstamp exchange attack, which resulted in the theft of 18 866 bitcoins [2, 11]. Moreover, in 2012, a sanity check found that numerous RSA keys throughout the web offered no security at all due to insufficient randomness [19]. More severely, trust in the standardized solutions that should mitigate these problems has been eroded by the discovery that the NSA intentionally lowered the security of several RNGs through practices such as the deliberate insertion of a backdoor in the NIST certificated `Dual_EC_DRBG` CSPRNG [11]. This is especially worrying as the adoption of new communication technologies has increasingly exposed large amounts of data to the internet. There is, consequently, high demand for fast and reliable randomness generation methods for security-critical applications.

Nowadays, True Random Number Generators (TRNGs) are increasingly popular as a way to build resilience against future threats and mitigate the shortcomings presented by traditional PRNGs. These devices, like the first mechanical generators, use some apparently unpredictable physical phenomena as their randomness source. Some non-physical TRNGs rely on collecting parameters accessible to the operating system such as mouse movements, disk access times, or keystrokes [3, 10]. None of these phenomena are particularly good Entropy Sources (ESs) and can be prone to severe biases. More complex implementations use a dedicated device to measure an external physical process that has the desired statistical properties. Some examples include measuring atmospheric noise [20], electrical noise in electronic circuits [21], the evolution of chaotic systems [22], or the period of ring oscillators [23]. Initial implementations presented limited output rates and were mostly used to obtain random values to seed CSPRNGs, but modern devices can already reach several Gbps. In fact, successful commercial TRNGs can be found online as early as 1998, as is the case with the widely known *Random.org* service, and integrated solutions already exist, such as the generator provided by Intel [24]. Sadly, although believed to be a more secure approach to RN generation, it is hard to give a convincing argument for the randomness yielded by these classical TRNGs. This is particularly true for implementations based on fundamentally deterministic processes, such as chaos-based generators. Ultimately, such as in the case of a PRNG, the randomness extracted is still merely based on incomplete knowledge of the system or on the computation infeasibility to guess their output, given current technology. Moreover, ESs rarely produce an unbiased and uncorrelated distribution of outcomes. To obtain a bit-stream able to pass most statistical tests, TRNGs typically apply a randomness extraction algorithm that increases the available randomness by sacrificing the sequence's length. This postprocessing can mask failures of the ES that are hard to detect, which is particularly worrying given the lack of fundamental proof for their unpredictability. Physical sources are also frequently sensitive to environmental conditions, which makes them especially prone to manipulation by an adversary with even partial access to the ES [10]. As a matter of fact, successful attacks have already been conducted in systems sensitive to variations of temperature [25], input voltage [26], or susceptible

to strong electromagnetic fields [27].

Quantum random number generation is one of the many recent technologies to emerge from the second quantum revolution. In conjunction with the development of QKD protocols, it has driven innovation in the field of quantum cryptography, which explores the unique properties of quantum mechanics to achieve stronger security than its classical counterpart [28]. In contrast to classical TRNGs, Quantum Random Number Generators (QRNGs) derive their randomness from the intrinsic probabilistic nature of quantum phenomena. As illustrated in Fig. 1.1, these also belong to the class of physical TRNGs, but here the ES is clearly defined, fundamentally unpredictable to any adversary, and is thus able to yield information-theoretically provable randomness under reasonable assumptions such as a trusted-device scenario [29]. Instead of simply assessing if the output sequences of a deterministic process have all the statistical properties of a random sequence, a rigorous analysis of the physical process can be made to guarantee its privacy and justify its security. The first QRNGs were based on measurements of radioactive decays [30], but the need for a radioactive source and their limited output rate has hindered their popularity. Nowadays, most implementations explore the quantum properties of light due to the high availability and affordability of optical components, and the high generation rates that such devices can achieve [10]. Several different proofs of concept have been proposed, exploring phenomena such as amplified spontaneous emission [31], photon arrival times [32], photon number statistics [33], single-photon branching paths [34], stimulated Raman scattering [35] or the phase noise of a laser [36]. Recent developments have focused on achieving generation schemes with higher performance, with speeds up to 68 Gbps being reported [37]. Additionally, various self-testing, device-independent, or semi-device independent protocols have been proposed [38]. Although generally slower, these remove the necessity to have complete trust in the implementation details of the generator. Recently, some integrated solutions have also materialized [39, 40]. These remove the necessity of bulky implementations and are a fundamental step towards competing with the traditional algorithmic generators. Indeed, QRNGs are currently one of the few well-established quantum technologies able to make the jump from the research domain to a commercial market in rapid expansion [11]. However, their adoption is still restricted by a high cost in face of the traditional alternatives.

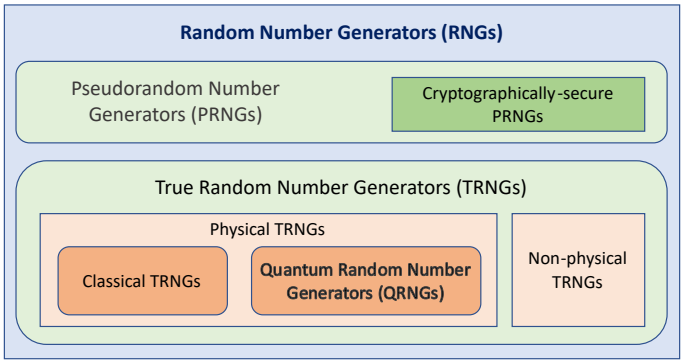


Fig. 1.1: Schematic diagram with the various types of RNGs. These can mainly be distinguished between PRNGs, which algorithmically expand an initial random seed, and TRNGs, which explore an entropy source, either through an external signal or a dedicated physical device. Physical TRNGs are further divided between those who explore classical and quantum phenomena. Only the latter can yield information-theoretically provable randomness.

A particularly promising solution explores the quadrature fluctuations of a vacuum state by resorting to a balanced homodyne detection scheme. These so-called vacuum-based QRNGs can achieve high generation rates with low-cost and widely available technologies. In fact, many implementations able to reach several Gbps have already been proposed [40, 41, 42, 43]. Furthermore, these QRNGs show high potential for chip integration due to the low number of components required and can potentially be incorporated within already existing optical fiber networks, as recently demonstrated [44]. The vacuum state is also easily obtainable and, assuming a trusted-

device scenario, its purity cannot be tampered with by an adversary, which guarantees the quality of the ES. Despite this, realistically, the quantum fluctuations will always be mixed with non-random contributions and, consequently, these schemes rely on randomness extraction algorithms. The first proposals have generally estimated these contributions by following the concept of Shannon entropy [45, 46]. As recommended by the NIST SP 800-90B standard, this is an inadequate estimator to quantify randomness [15, 47]. More recently, [29] developed a framework to assess the extractable entropy through a min-entropy estimator and proposed two information-theoretically provable random extraction algorithms. Posteriorly, authors in [48] proposed an estimation model considering the Analog-to-digital Converter (ADC) discretization, and analyzed the impact of the acquisition range and resolution of the ADC. Recently, [49] was able to increase the conditional min-entropy by discarding boundary-bin measurement and introducing multi-interval sampling. Besides improving performance, current research is focused on assessing and mitigating the impact of experimental non-idealities, such as an imperfect balancing condition, which can lead to the introduction of security loopholes. In [50], a novel approach that considers the fluctuations of a non-ideal Local Oscillator (LO) is developed. Other approaches concentrate on achieving a high-performance randomness platform [51], surpassing technical challenges posed by chip integration [52], or developing device-independent solutions [53, 54]. Meanwhile, research on new possible attacks is underway [55], which will surely improve the security of these protocols.

1.2 Motivation and objectives

Despite the recent developments reported, real-time implementations of vacuum-based QRNGs still generally rely on some unclarified assumptions such as a balanced detection scheme, or an ideal optical source without quantifying its impact on the security of the system. Moreover, detailed characterization of the entropy model behavior in a real-time operation is necessary, as the system is typically assumed to remain static and without fluctuations in the classical noise level. This is especially worrisome, as most implementations solely rely on the NIST statistical test suite for validation, which, while the most widely used randomness testing tool, is less rigorous than other extensive batteries such as Dieharder or TestU01 that could help reveal overlooked biases. Furthermore, while chip-integrated solutions are being developed, few efforts into removing the necessity of a physical dedicated implementation were taken.

This dissertation has focused on achieving a high-speed real-time QRNG implementation based on vacuum fluctuations using widely available optical devices and components, which is also able to address these omissions. Specifically, the following main objectives can be highlighted:

- Provide a comprehensive proof of randomness based on a mathematical description of a vacuum-based QRNG and the development of its variance model.
- Characterize the impact of non-ideal optoelectronic devices and other imperfections on the performance of the QRNG [56, 57].
- Comparatively analyze the main entropy estimation methods within the scope of a real-time QRNG based on homodyne measurements of vacuum fluctuations.
- Develop a framework to estimate the excess entropy contributions resultant from an unbalanced homodyne detection [57].
- Implement and validate a QRNG scheme time-interleaved with a Quantum Phase Shift Keying (QPSK) tributary signal within a classical coherent detector [58].

1.3 Dissertation structure

This document is organized into 6 chapters, with this introduction to RNGs being the first, and the others are summarized as follows:

- Chapter 2 introduces the conceptual formalism necessary to describe a QRNG implementation based on homodyne measurements of vacuum fluctuations. Namely, fundamental concepts in quantum optics and information theory are explored.
- Chapter 3 presents a block description of the proposed QRNG scheme, including a theoretical model of the physical layer and the postprocessing necessary to extract true random numbers.
- Chapter 4 describes and analyses the dedicated real-time experimental scheme implemented, comparing the performance under different postprocessing methods and describing the key technical challenges. Furthermore, extensive statistical validation is applied to guarantee the quality and security of the QRNG output.
- Chapter 5 includes a description of an alternative QRNG scheme, which removes the need for a dedicated physical implementation and proceeds with its experimental validation.
- Chapter 6 summarizes the main conclusions and outlines the future work.

1.4 List of Publications

The work developed in this dissertation has resulted on the following publications:

- Ferreira, Maurício J. and Silva, Nuno A. and Pinto, Armando N. and Muga, Nelson J. Characterization of a quantum random number generator based on vacuum fluctuations. *Applied Sciences*, 11(16), 2021
- Ferreira, Maurício J. and Silva, Nuno A. and Pinto, Armando N. and Muga, Nelson J. Homodyne noise characterization in quantum random number generators. In *2021 Telecoms Conference (ConfTELE)*, pages 1–6, Leiria, Portugal, 2021
- Maurício Ferreira and Daniel Pereira and Nelson Muga and Nuno Silva and Armando Pinto. Time-interleaved quantum random number generation within a coherent classical communication channel. In *Anais do I Workshop de Comunicação e Computação Quântica*, pages 37–42, Porto Alegre, RS, Brasil, 2021. SBC

Chapter 2

Theoretical Background

In this chapter, the theoretical formalism necessary to describe a QRNG based on homodyne measurements of vacuum fluctuations will be discussed. In section 2.1 a brief introduction to quantum optics is made, namely by analyzing the concept of number and coherent states. Posteriorly, the fundamental concepts of information theory are described in section 2.2. This supports the description of the homodyne detection model and the entropy estimation models presented in chapter 3.

2.1 Quantum optics

The quantization of the electromagnetic field is made by associating a quantum-mechanical harmonic oscillator of angular frequency $\omega_{\mathbf{k}}$ with each mode $\mathbf{k}$ in a quantization cavity. Assuming a single polarization, its Hamiltonian $\hat{\mathcal{H}}$ is thus simply obtained from the multi-modal generalization of the one-dimensional oscillator, which yields [59]:

$$\hat{\mathcal{H}} = \sum_{\mathbf{k}} \frac{\hat{p}_{\mathbf{k}}^2}{2m} + \frac{1}{2} m\omega_{\mathbf{k}}^2 \hat{q}_{\mathbf{k}}^2, \tag{2.1}$$

where $\hat{q}_{\mathbf{k}}$ and $\hat{p}_{\mathbf{k}}$ are, respectively, the position and momentum operators which follow the canonical commutation relation $[\hat{q}_{\mathbf{k}}, \hat{p}_{\mathbf{k}'}] = i\hbar\delta_{\mathbf{k},\mathbf{k}'}$. One can also rewrite (2.1) in relation to the dimensionless annihilation and creation operators, $\hat{a}_{\mathbf{k}}$ and $\hat{a}_{\mathbf{k}}^\dagger$, defined as:

$$\begin{aligned} \hat{a}_{\mathbf{k}} &= \frac{1}{\sqrt{2m\hbar\omega_{\mathbf{k}}}}\Big(m\omega_{\mathbf{k}}\hat{q}_{\mathbf{k}} + i\hat{p}_{\mathbf{k}}\Big), \\ \hat{a}_{\mathbf{k}}^\dagger &= \frac{1}{\sqrt{2m\hbar\omega_{\mathbf{k}}}}\Big(m\omega_{\mathbf{k}}\hat{q}_{\mathbf{k}} - i\hat{p}_{\mathbf{k}}\Big). \end{aligned} \tag{2.2}$$

Since different modes are independent, their commutation relation follows:

$$\Big[\hat{a}_{\mathbf{k}}, \hat{a}_{\mathbf{k}'}^\dagger\Big] = \hat{a}_{\mathbf{k}}\hat{a}_{\mathbf{k}'}^\dagger - \hat{a}_{\mathbf{k}'}^\dagger\hat{a}_{\mathbf{k}} = \delta_{\mathbf{k},\mathbf{k}'}, \tag{2.3}$$

and the Hamiltonian becomes:

$$\hat{\mathcal{H}} = \sum_{\mathbf{k}} \frac{1}{2}\hbar\omega_{\mathbf{k}}\Big(\hat{a}_{\mathbf{k}}\hat{a}_{\mathbf{k}}^\dagger + \hat{a}_{\mathbf{k}}^\dagger\hat{a}_{\mathbf{k}}\Big). \tag{2.4}$$

By analogy with the total radiative energy in the classical case, the classical vector potential can be associated with the quantum-mechanical annihilation and creation operators [59]. The quantized electric field operator is thus defined as:

$$\hat{E}_T = \sum_{\mathbf{k}} \sqrt{\Big(\frac{\hbar\omega_{\mathbf{k}}}{2\varepsilon_0 V}\Big)}\Big[\hat{a}_{\mathbf{k}}e^{-i\chi_{\mathbf{k}}} + \hat{a}_{\mathbf{k}}^\dagger e^{i\chi_{\mathbf{k}}}\Big], \tag{2.5}$$

where $\chi_{\mathbf{k}} = \omega_{\mathbf{k}} t - \vec{k} \cdot \vec{r} - \frac{\pi}{2}$. Here, ε_0 is the the vacuum permittivity, V the volume of the quantization cavity, $\vec{k}$ the wave vector, and $\vec{r}$ the position vector.

Other useful quantities when describing the quantum harmonic oscillator are the quadrature operators, which derive from the position and momentum operators:

$$\begin{aligned} \hat{X}_{\mathbf{k}} &= \sqrt{\frac{m\omega_{\mathbf{k}}}{2\hbar}}\hat{q}_{\mathbf{k}} = \frac{1}{2}(\hat{a}^{\dagger}_{\mathbf{k}} + \hat{a}_{\mathbf{k}}), \\ \hat{Y}_{\mathbf{k}} &= \frac{1}{\sqrt{2m\hbar\omega_{\mathbf{k}}}}\hat{p}_{\mathbf{k}} = \frac{i}{2}(\hat{a}^{\dagger}_{\mathbf{k}} - \hat{a}_{\mathbf{k}}), \end{aligned} \tag{2.6}$$

whose commutation relation yields:

$$\left[\hat{X}_{\mathbf{k}}, \hat{Y}_{\mathbf{k}'}\right] = \frac{i}{2}\delta_{\mathbf{k},\mathbf{k}'}. \tag{2.7}$$

In opposition to the creation and annihilation operators, these follow the hermitian condition and thus correspond to observables of the optical state. With these definitions, we can verify that:

$$\hat{\mathcal{H}} = \sum_{\mathbf{k}} \hbar\omega_{\mathbf{k}}\Big(\hat{X}^2_{\mathbf{k}} + \hat{Y}^2_{\mathbf{k}}\Big). \tag{2.8}$$

and from (2.5) the electric field operator becomes:

$$\hat{E}_T = \sum_{\mathbf{k}} \sqrt{\Big(\frac{2\hbar\omega_{\mathbf{k}}}{\varepsilon_0 V}\Big)}\Big[\hat{X}_{\mathbf{k}}\cos\chi_{\mathbf{k}} + \hat{Y}_{\mathbf{k}}\sin\chi_{\mathbf{k}}\Big], \tag{2.9}$$

Thus $\hat{X}_{\mathbf{k}}$ and $\hat{Y}_{\mathbf{k}}$ yield, respectively, the in-phase and in-quadrature components of the electric field amplitude. It can also be demonstrated through the Heisenberg uncertainty principle for non-commuting operators that the multiplication of their variances [60]:

$$\begin{aligned} \sigma^2_{\hat{X}_{\mathbf{k}}}\sigma^2_{\hat{Y}_{\mathbf{k}'}} &\geq \frac{1}{4}\Big|\big\langle\Big[\hat{X}_{\mathbf{k}}, \hat{Y}_{\mathbf{k}'}\Big]\big\rangle\Big|^2 \\ &\geq \frac{1}{16}\delta_{\mathbf{k},\mathbf{k}'}, \end{aligned} \tag{2.10}$$

which implies that the quadratures of the electric field in a given mode cannot be simultaneously measured with arbitrary precision.

2.1.1 Number states

Single-mode numbers states, or Fock states, noted $|n_{\mathbf{k}}\rangle$ form a complete set of orthonormal states that are characterized by the exact number of photons $n_{\mathbf{k}}$ excited in the cavity mode. They are the eigenstates of the Hamiltonian for each individual mode in the quantum harmonic oscillator defined in (2.4) and thus satisfy the energy eigenvalue relation [59]:

$$\hat{\mathcal{H}}_{\mathbf{k}}\,|n_{\mathbf{k}}\rangle = E_{n_{\mathbf{k}}}\,|n_{\mathbf{k}}\rangle\,, \tag{2.11}$$

where the eigenvalue $E_{n_{\mathbf{k}}}$ is the corresponding energy level:

$$E_{n_{\mathbf{k}}} = \Big(n_{\mathbf{k}} + \frac{1}{2}\Big)\hbar\omega_{\mathbf{k}}, \quad n_{\mathbf{k}} \in \mathbb{N}_0. \tag{2.12}$$

Thus consecutive eigenvalues are equally spaced by an energy quantum $\hbar\omega_{\mathbf{k}}$ and, for each mode, the vacuum state $|0_{\mathbf{k}}\rangle$ of the field in which no photons are excited has by definition the smallest allowable energy of $\frac{1}{2}\hbar\omega_{\mathbf{k}}$ [59]. Similarly, the energy eigenvalue of a multi-mode number state $|\{n_{\mathbf{k}\lambda}\}\rangle$, where $\{n_{\mathbf{k}\lambda}\}$ denotes the number of photons in each of the cavity modes that describe the total electromagnetic field, is given by the sum of the individual contributions shown in (2.12):

$$\hat{\mathcal{H}}\,|\{n_{\mathbf{k}\lambda}\}\rangle = \sum_{\mathbf{k}} \hbar\omega_{\mathbf{k}}\Big(n_{\mathbf{k}} + \frac{1}{2}\Big)\,|\{n_{\mathbf{k}\lambda}\}\rangle\,. \tag{2.13}$$

Strikingly, as no upper bound in the range of allowed frequencies $\omega_{\mathbf{k}}$ exists, it is implied that the zero-point energy of the electromagnetic field is infinite, although only the excitation energy above this value contributes to the observable optical intensity [59].

Simultaneously, a $n_{\mathbf{k}}$-number state is an eigenstate of the number operator:

$$\hat{N}_{\mathbf{k}} = \hat{a}_{\mathbf{k}}^{\dagger}\hat{a}_{\mathbf{k}}, \tag{2.14}$$

such that $\hat{N}_{\mathbf{k}}\left|n_{\mathbf{k}}\right\rangle = n_{\mathbf{k}}\left|n_{\mathbf{k}}\right\rangle$. Thus, the null uncertainty in the photon number remains implicit and $\sigma_{n_{\mathbf{k}}}^2 = 0$. Moreover, the action of the creation and annihilation operators on this state yields [59]:

$$\begin{aligned} \hat{a}_{\mathbf{k}}\left|n_{\mathbf{k}}\right\rangle &= \sqrt{n_{\mathbf{k}}}\left|n_{\mathbf{k}}-1\right\rangle, \\ \hat{a}_{\mathbf{k}}^{\dagger}\left|n_{\mathbf{k}}\right\rangle &= \sqrt{n_{\mathbf{k}}+1}\left|n_{\mathbf{k}}+1\right\rangle. \end{aligned} \tag{2.15}$$

From their application in the vacuum state results [59]:

$$\begin{aligned} \hat{a}_{\mathbf{k}}\left|0_{\mathbf{k}}\right\rangle &= 0, \\ \left\langle 0_{\mathbf{k}}\right|\hat{a}_{\mathbf{k}}^{\dagger} &= 0. \end{aligned} \tag{2.16}$$

Consequently, any generic photon state can be obtained by repeatedly applying the creation operator on $\left|0_{\mathbf{k}}\right\rangle$ [59]:

$$\left|n_{\mathbf{k}}\right\rangle = \frac{(\hat{a}_{\mathbf{k}}^{\dagger})^{n_{\mathbf{k}}}}{\sqrt{n_{\mathbf{k}}!}}\left|0_{\mathbf{k}}\right\rangle. \tag{2.17}$$

Given these formulations, the relations in (2.15) and the orthonormality shared by number states, the field quadrature properties yield:

$$\begin{aligned} \left\langle n_{\mathbf{k}}\right|\hat{X}_{\mathbf{k}}\left|n_{\mathbf{k}}\right\rangle = \left\langle n_{\mathbf{k}}\right|\hat{Y}_{\mathbf{k}}\left|n_{\mathbf{k}}\right\rangle &= 0, \\ \sigma_{\hat{X}_{\mathbf{k}}}^2 = \sigma_{\hat{Y}_{\mathbf{k}}}^2 &= \frac{1}{2}\left(\frac{1}{2}+n_{\mathbf{k}}\right). \end{aligned} \tag{2.18}$$

Thus, these fluctuations have identical properties for both phase quadratures and their variance depends explicitly on the number of photons excited in the cavity mode. Accordingly, the expected mean electric field is null and its variance follows (2.18), which means that a number state cannot carry information suitable for homodyne detection [59].

As shown in (2.6), the quadrature eigenstates $\left|x_{\mathbf{k}}\right\rangle$ and $\left|y_{\mathbf{k}}\right\rangle$ are a generalization of the usual position and momentum basis states on a quantum-mechanical harmonic oscillator. Consequently, the in-phase quadrature probability distribution $P_{n_{\mathbf{k}}}(x)$ of a given number state $\left|n_{\mathbf{k}}\right\rangle$ can be obtained from the eigenfunction solutions of the time-independent Schrödinger equation in the coordinate basis, $\Psi(q)$ [61]:

$$\Psi(q) = \frac{1}{\sqrt{2^{n_{\mathbf{k}}}n_{\mathbf{k}}!}}\left(\frac{m\omega_{\mathbf{k}}}{\hbar\pi}\right)^{1/4} e^{-\frac{m\omega_{\mathbf{k}}}{2\hbar}q^2} H_{n_{\mathbf{k}}}\left(\sqrt{\frac{m\omega_{\mathbf{k}}}{\hbar}}q\right), \tag{2.19}$$

where $H_{n_{\mathbf{k}}}$ denotes a Hermite polynomial of rank $n_{\mathbf{k}}$. Given the definition of the quadrature operator with a continuous eigenvalue x and the orthonormality condition of these functions, the wave function can be rewritten on the quadrature basis as:

$$\Psi(x) = \frac{1}{\sqrt{2^{n_{\mathbf{k}}}n_{\mathbf{k}}!}}\left(\frac{2}{\pi}\right)^{1/4} e^{-x^2} H_{n_{\mathbf{k}}}\left(x\sqrt{2}\right), \tag{2.20}$$

and thus, as given by the Born rule [60]:

$$P_{n_{\mathbf{k}}}(x) = \left|\langle x_{\mathbf{k}}|n_{\mathbf{k}}\rangle\right|^2 = \frac{1}{2^{n_{\mathbf{k}}}n_{\mathbf{k}}!}\left(\frac{2}{\pi}\right)^{1/2} e^{-2x^2}\left(H_{n_{\mathbf{k}}}\left(x\sqrt{2}\right)\right)^2, \tag{2.21}$$

where $|x_{\mathbf{k}}\rangle$ is the eigenstate of the quadrature operator $\hat{X}_{\mathbf{k}}$. Similarly, an identical expression can be derived for the in-quadrature probability distribution $P_{n_{\mathbf{k}}}(y)$ from the momentum representation of the wave function. Consequently, quadrature measurements of a number state are inherently probabilistic and will fluctuate with a probability distribution described by (2.21) around the null expected value. The phase space distribution of a single mode number state with $n_{\mathbf{k}} > 0$ along any direction is thus characterized by the null probability fringes corresponding to the zeros of the Hermite polynomials, as shown in Fig. 2.1 for $n_{\mathbf{k}} = 0$, $n_{\mathbf{k}} = 3$, and $n_{\mathbf{k}} = 4$.

(a) (b) (c)

Fig. 2.1: Representation of the phase space probability distribution of number states with (a) $n_{\mathbf{k}} = 0$, (b) $n_{\mathbf{k}} = 3$, and (c) $n_{\mathbf{k}} = 4$. Dark zones represent an higher probability density. The radial projection in any direction is described by the quadrature probability distribution.

2.1.1.1 Vacuum state

As previously mentioned, the vacuum state $|\{0\}\rangle$ of the electromagnetic field corresponds to the state in which no photons are excited in any cavity mode and is thus the ground state of the single-mode quantum harmonic oscillator. As will be further discussed in section 2.1.2, it has the special property of simultaneously being a number and a coherent state of the electromagnetic field. For any particular individual mode, the quadrature properties of the vacuum state can be derived from (2.18):

$$\begin{aligned} \langle 0_{\mathbf{k}}| \hat{X}_{\mathbf{k}} |0_{\mathbf{k}}\rangle = \langle 0_{\mathbf{k}}| \hat{Y}_{\mathbf{k}} |0_{\mathbf{k}}\rangle = 0, \\ \sigma^2_{\hat{X}_{\mathbf{k}}} = \sigma^2_{\hat{Y}_{\mathbf{k}}} = \frac{1}{4}, \end{aligned} \tag{2.22}$$

which is the minimal value compatible with the uncertainty relation (2.10). As also shown in Fig. 2.1a, $|0_{\mathbf{k}}\rangle$ is consequently a quadrature-minimum uncertainty state. Furthermore, considering that the Hermite polynomial $H_0(x) = 1$, its quadrature probability density function yields:

$$P_{0_{\mathbf{k}}}(x) = \left(\frac{2}{\pi}\right)^{1/2} e^{-2x^2}. \tag{2.23}$$

Here, its dual nature becomes clear. Akin to the coherent states, the quadrature measurements in each mode follow an isotropic Gaussian distribution with variance equal to $\frac{1}{4}$. Simultaneously, similarly to the other number states, the vacuum fluctuations oscillate around a null expected value and have a completely random phase [59].

Despite the theoretical simplicity of number states, it is usually difficult to experimentally obtain optical states with a well-defined number of photons. This contrasts with the vacuum state, which can be produced with good approximation at a frequency $\omega_{\mathbf{k}}$ by assuring a certain temperature of the optical system T, as given by the Plank thermal excitation function. It describes the mean number of photons excited in a thermal state [59]:

$$\langle n_{\mathbf{k}} \rangle = \frac{1}{e^{\frac{\hbar\omega_{\mathbf{k}}}{k_{\mathrm{B}}T}} - 1}, \tag{2.24}$$

where k_B is the Boltzmann constant. As such, as long as $T \ll \frac{\hbar\omega_\mathbf{k}}{k_B}$, $\langle n_\mathbf{k}\rangle \sim 0$ and the number of photons excited can be considered negligible [59]. At the conventional 1550 nm band this yields approximately 9282 K, an thus the condition is satisfied at room temperature.

2.1.2 Coherent states

A single-mode coherent state $|\alpha\rangle$ is defined as a linear superposition of number states that can be described in the form [59]:

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle , \quad \alpha = |\alpha| e^{i\theta} \in \mathbb{C}. \tag{2.25}$$

These are the states with properties more similar to those of a classical electromagnetic wave, as they have a constant field amplitude and, in contrast with the number states previously described, a fixed phase. It follows from their definition that coherent states are normalized such that $\langle\alpha|\alpha\rangle = 1$. They do not, however, share orthogonality, as:

$$\langle\alpha|\beta\rangle = e^{-\frac{1}{2}(|\alpha|^2+|\beta|^2)+\alpha^*\beta} \quad \text{and} \quad |\langle\alpha|\beta\rangle|^2 = e^{-|\alpha-\beta|^2}. \tag{2.26}$$

Although never orthogonal, they become approximately so when $|\alpha - \beta| \gg 1$, which describes their proximity in the complex plane.

Coherent states follow a right-eigenstate relation with the annihilation operator, where α is the eigenvalue. Similarly, the conjugate relation is obeyed by the creation operator [59]:

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle \quad \text{and} \quad \langle\alpha|\,\hat{a}^\dagger = \langle\alpha|\,\alpha^*. \tag{2.27}$$

These relations allow to obtain the mean photon number and photon number variance, as given by the number operator $\hat{N}$:

$$\begin{aligned} \langle n\rangle &= \langle\alpha|\,\hat{N}\,|\alpha\rangle = \alpha^*\alpha = |\alpha|^2, \\ \sigma_n^2 &= \langle\alpha|\,\hat{N}^2\,|\alpha\rangle - \big(\langle\alpha|\,\hat{N}\,|\alpha\rangle\big)^2 = |\alpha|^2. \end{aligned} \tag{2.28}$$

The photon number mean and variance are thus equal, solely depending on the amplitude of the coherent state. In fact, its distribution follows a Poisson statistic [59]:

$$P_\alpha(n) = e^{-\langle n\rangle}\frac{-\langle n\rangle^n}{n!}, \tag{2.29}$$

which approaches a Gaussian distribution for large values of $\langle n\rangle$. Consequently, the relative fluctuation of the photon number diminishes with increasing values of the mean photon number, becoming negligible for large fields. Nonetheless, this uncertainty is experimentally observed as shot noise in optical detection, and its variance is proportional to the impinging optical power, as implied by (2.28).

Alternatively, coherent states can also be defined as a displacement of the vacuum state in phase space [59]:

$$|\alpha\rangle = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}\,|0\rangle = \hat{D}(\alpha)\,|0\rangle\,, \tag{2.30}$$

where $\hat{D}(\alpha)$ is the so-called coherent-state displacement operator. It becomes clear, as previously discussed, that the vacuum state can simultaneously be described as the base number state or a non-displaced coherent state. As seen in Fig. 2.2, applying this translation transforms the vacuum state into a coherent state of well-defined phase without changing the distribution of its quadratures. In fact, using the relations described in (2.27) and considering the polar representation of the complex amplitude α:

$$\begin{aligned} \langle\alpha|\,\hat{X}\,|\alpha\rangle &= \mathrm{Re}(\alpha) = |\alpha|\cos\theta, \\ \langle\alpha|\,\hat{Y}\,|\alpha\rangle &= \mathrm{Im}(\alpha) = |\alpha|\sin\theta. \end{aligned} \tag{2.31}$$

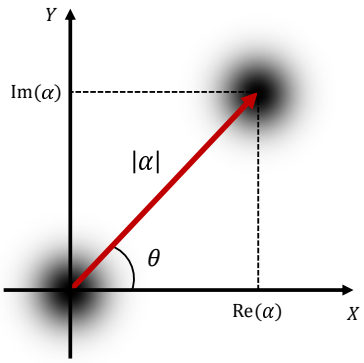


Fig. 2.2: Representation of a coherent state $|\alpha\rangle$ as a displacement of the vacuum state $|0\rangle$ in the phase space by the complex amplitude α. While the quadrature distributions remain isotropic and of minimum uncertainty, their expected values are now shifted by $|\alpha|\cos\theta$ along the X-quadrature and $|\alpha|\sin\theta$ along the Y-quadrature.

Thus, the mean values of the quadrature operators yield the real and imaginary parts of its complex amplitude. Furthermore, the quadrature variances are:

$$\sigma^2_{\hat{Y}} = \sigma^2_{\hat{X}} = \frac{1}{4}, \tag{2.32}$$

which shows that a coherent state has minimum quadrature uncertainty for any photon number $|\alpha|^2$, which is consistent with the definition (2.30). Lastly, analogously to the quadrature measurements of a vacuum state, the coherent state also follows a Gaussian quadrature probability distribution such that [60]:

$$P_\alpha(x) = \left(\frac{2}{\pi}\right)^{1/2} e^{-2(x-\mathrm{Re}(\alpha))^2}. \tag{2.33}$$

2.1.2.1 Continuous-mode coherent state

While the fundamental properties of coherent states are accurately reflected in the single-mode description made, a time-dependent representation necessarily requires considering the infinite range of excitations modes in a multi-mode optical state. As the multi-mode number state previously described, the multi-mode coherent state $|\{\alpha\}\rangle$ defines the set of complex amplitudes that represent the coherent states in each excited cavity mode [59]. However, most of the realistic optical experiments are better characterized by a free space quantization of the field, which is defined by a continuous wave vector. For a cavity of length L, the summations over $\mathbf{k}$ are converted to integrations as $\sum_{\mathbf{k}} \to \frac{1}{\Delta\omega}\int d\omega$, where $\Delta\omega = \frac{2\pi}{L} \to 0$ as $L \to \infty$. Consequently, the continuous-mode creation and annihilation operators [59]:

$$\hat{a}_{\mathbf{k}} \to (\Delta\omega)^{\frac{1}{2}}\hat{a}(\omega) \quad \text{and} \quad \hat{a}^\dagger_{\mathbf{k}} \to (\Delta\omega)^{\frac{1}{2}}\hat{a}^\dagger(\omega), \tag{2.34}$$

and the corresponding time-dependent operators, $\hat{a}(t)$ and $\hat{a}^\dagger(t)$, are obtained through their Fourier transform. Here, $\left[\hat{a}(t), \hat{a}^\dagger(t')\right] = \delta(t-t')$ and the number operator is now defined as:

$$\hat{N} = \int \hat{a}^\dagger(t)\hat{a}(t)\,dt = \int \hat{f}(t)\,dt, \tag{2.35}$$

where $\hat{f}(t)$ is the photon flux operator.

Continuous-mode coherent states are obtained through a generalization of the relation mentioned in (2.30). As their single-mode counterparts, they remain left-eigenstates of the continuous-

mode annihilation operator [59]:

$$\begin{aligned} \hat{a}(t)\,|\{\alpha\}\rangle &= \alpha(t)\,|\{\alpha\}\rangle\,, \\ \langle\{\alpha\}|\,\hat{a}^{\dagger}(t) &= \langle\{\alpha\}|\,\alpha^{*}(t), \end{aligned} \tag{2.36}$$

and the mean photon flux yields:

$$\langle \hat{f}(t)\rangle = |\alpha(t)|^2. \tag{2.37}$$

This formalism is useful to describe the emission of a single-mode laser operating above the threshold level [59], as will be required in chapter 3.

2.2 Information theory

Quantifying the unpredictability of a given random variable is a central problem in randomness generation as it is essential to characterize a randomness source and account for potential access to side information by an eavesdropper.

The uncertainty associated with the outcomes of a certain random variable X is given by its entropy, which can be defined in many different ways. Shannon entropy is often proposed as a good estimator and is defined in the unit of bits as [62]:

$$H(X) = -\sum_i P_X(x_i)\log_2 P_X(x_i), \tag{2.38}$$

where $P_X(x_i)$ is the probability of each outcome x_i. This quantity expresses the average information conveyed by each outcome x_i and thus constitutes a measure of the average unpredictability of X. If a second random variable Y is considered, their joint Shannon entropy is [60]:

$$H(X,Y) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} P_{X,Y}(x,y)\log_2 P_{X,Y}(x,y), \tag{2.39}$$

where $P_{X,Y}(x,y)$ is the joint probability function of these variables, and $\mathcal{X},\mathcal{Y}$ their respective images. The joint entropy can be rewritten through the chain rule for entropies as [60]:

$$H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y), \tag{2.40}$$

where $H(Y|X)$ is the conditional entropy between the two random variables [60]:

$$H(Y|X) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} P_{X,Y}(x,y)\log_2 P_{Y|X}(y|x). \tag{2.41}$$

The conditional entropy describes the entropy of Y given that the result of X is known to an observer. Their mutual information, which yields the amount of information gathered about one variable by measuring the other, is thus defined as [62]:

$$I(X:Y) = H(Y) - H(Y|X) = \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} P_{X,Y}(x,y)\log_2 \frac{P_{X,Y}(x,y)}{P_X(x)P_Y(y)}. \tag{2.42}$$

Finally, for a continuous variable X, the definition (2.38) is no longer valid. Instead, the analogous differential entropy for a distribution $p_X(x)$ is defined as [62]:

$$h(X) = -\int_{x\in\mathcal{X}} p_X(x)\log_2 p_X(x)\,dx. \tag{2.43}$$

The term entropy is generally interpreted as Shannon entropy by default. Unfortunately, Shannon entropy is inadequate to quantify randomness, particularly for highly skewed distributions. Consider, for example, a random variable B with $n+1$ outcomes, where an extreme outlier exists and the remaining are normally distributed:

- $B = 0$ with $P_B(0) = \frac{1}{2}$,
- $B \in \{1, 2, ..., n\}$ with $P_B(b_i) = \frac{1}{2n}$.

In this case $H(B) = -\frac{1}{2}\log_2\frac{1}{2} - \frac{1}{2}\log_2\frac{1}{2n} \to \infty$ when $n \to \infty$ [15]. Thus it is possible to define a random variable with large Shannon entropy whose guessing is trivial. Here, $H(B)$ acts, at best, as an upper entropy bound, and for a large n it is no longer an adequate estimator. In such cases, the unpredictability is better characterized by the min-entropy [63]:

$$H_{\min}(X) = -\log_2 \max_{x_i \in X} P_X(x_i), \tag{2.44}$$

which describes the entropy associated with the best strategy to guess the random variable. The probability of observing any outcome is thus no greater than $2^{-H_{\min}}$ and the min-entropy is maximized for a uniform distribution when it is equal to the Shannon entropy [63]. In the example described, $H_{\min}(B) = 1$ regardless of n and thus sets a lower bound for the unpredictability of B. For a random variable X, the classical worst-case conditional min-entropy $H_{\min}(X|E)$ conditioned on classical side-information E is determined by [48]:

$$H_{\min}(X|E) = -\log_2 \max_{e_j \in \mathrm{supp}(P_E)} \max_{x_i \in X} P_{X|E}(x_i|e_j), \tag{2.45}$$

where the support $\mathrm{supp}(P_E)$ is the set where $P_E(e_j) > 0$ and equals $\mathbb{R}$ for a normal distribution.

As will be described in chapter 3, the measured distribution M will simultaneously contain contributions from quantum noise Q and classical fluctuations E. This constitutes an additive white noise Gaussian channel, where all contributions are normally distributed independent random variables such that $M = Q + E$. In these circumstances, their respective variances can be written as $\sigma_M^2 = \sigma_Q^2 + \sigma_E^2$, and the mutual information between the measured distribution and the quantum noise yields [62]:

$$\begin{aligned} I(Q:M) &= H(M) - H(M|Q) \\ &= H(M) - H(Q+E|Q) \\ &= H(M) - H(Q|Q) - H(E|Q), \end{aligned} \tag{2.46}$$

and since, using (2.41), $H(Q|Q) = 0$ and $H(E|Q) = H(E)$ [62]:

$$\begin{aligned} I(Q:M) &= H(M) - H(E) \\ &= \frac{1}{2}\log_2(2\pi e\sigma_M^2) - \frac{1}{2}\log_2(2\pi e\sigma_E^2) \\ &= \frac{1}{2}\log_2\left(\frac{\sigma_M^2}{\sigma_E^2}\right) \\ &= \frac{1}{2}\log_2\left(1 + 10^{\frac{\mathrm{QCNR}}{10}}\right), \end{aligned} \tag{2.47}$$

where the Quantum-to-classical Noise Ratio (QCNR) is defined as:

$$\mathrm{QCNR} = 10\log_{10}\frac{\sigma_Q^2}{\sigma_E^2}. \tag{2.48}$$

The formalism here introduced allows to give a detailed randomness proof for the ES described in chapter 3. The key concepts to retain are the description of the vacuum state made in section 2.1.1.1, which characterizes its expected quadrature behavior, and the entropy definitions presented in (2.38) and (2.45), which provide a mathematically rigorous approach to quantify the randomness present in the generation scheme.

Chapter 3

A Vacuum-based Quantum Random Number Generator

In this chapter, a complete description of the implemented continuous-variable QRNG based on homodyne measurements of vacuum fluctuations is presented. Initially, an overview of a QRNG scheme and its subdivision into different stages is made. In section 3.1, the formalism previously introduced is applied to derive a theoretical description of a homodyne detection scheme. Finally, comparative analyses of the different entropy estimation methods and randomness extraction algorithms implemented in chapter 4 are presented in sections 3.2 and 3.3, respectively.

A typical QRNG can generally be subdivided into two very distinct stages with different functions: the physical layer and the postprocessing layer. The physical layer is perceived as the randomness source of the implementation and contains both the quantum phenomena being explored and the physical apparatus necessary to prepare, maintain or measure the ES. As seen in Fig. 3.1, in this stage, it is possible to distinguish between the physical ES, from where the quantum entropy is extracted and the trustworthiness of the system derives, and the analog-to-digital conversion, which introduces additional noise. The physical layer ultimately determines the maximum achievable performance, as no other stage can compensate for an eventual lack of entropy. Unfortunately, the quantum signal is inevitably mixed with classical noise contributions. These typically originate from the digitization stage, where electronic noise intrinsic to the physical devices is superimposed on the acquired signal, but other factors such as an improper state preparation can also contaminate the raw output [15]. Moreover, even if the measured quantity is truly random, seldom physical phenomena are uniformly distributed in nature. This results in a fundamentally biased output, which is not desirable for cryptographic applications. Even worse, these classical noise sources can potentially be manipulated or explored by an eavesdropper seeking to increase its probability of guessing the RNG outcomes. Consequently, a postprocessing layer is necessary to remove classical contributions and attain uniformly distributed RNs [10].

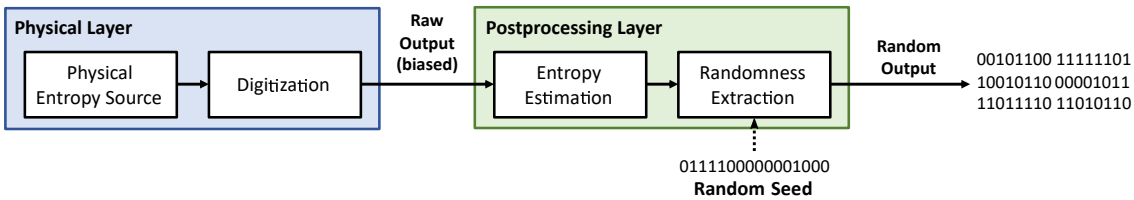


Fig. 3.1: Block diagram of a typical QRNG. The ES outputs raw measurements, which simultaneously contain quantum and classical contributions. Posteriorly, the postprocessing layer extracts a shorter set of uncorrelated and uniformly distributed RNs by applying a randomness extractor.

The postprocessing layer consists of an entropy estimation module to quantify the impact of side-information introduced by classical sources, followed by a randomness extraction stage. Ran-

domness extractors are deterministic functions able to extract almost-uniformly distributed data from a biased source by sacrificing a portion of the output sequence. Similarly to PRNGs, these may also require a short initial random seed, which can be obtained from a second randomness source or by forfeiting part of the RNG output. Here, however, the randomness obtained remains unpredictable as long as the input of the extractor is not deterministic and thus possesses some usable entropy. This differs from the PRNG construct, where the output is solely dependent on the initial seed. Nonetheless, the postprocessing layer imposes some computational costs, which limits the real performance of the implementation and reduces the output bit rate [3, 15].

As seen in chapter 1, numerous distinct QRNG schemes exist and the exact description of each stage will vary considerably. Implementations can generally be distinguished between device-dependent QRNGs, which rely on security assumptions about the various components of the physical layer, and device-independent generators. These rely on some fundamental quantum properties such as the violation of Bell inequalities to obtain certified RNs that do not depend on the implementation details, but are generally slow and difficult to implement. Semi-device independent solutions are also available and offer a compromise between the two approaches. Here, one considers the case in which an adversary has access either to the randomness source or to the detection scheme. Nonetheless, in practice, the security proof will rely on the characterization of at least some part of the implementation. Device-dependent schemes, in particular, assume that the implementation can be appropriately modeled to quantify all the noise sources present at the output. The choice of the postprocessing layer is thus interlinked with the physical implementation, and the entropy estimation must derive from a careful analysis of the physical layer. Furthermore, although some physical RNGs can drop its implementation if the raw sequences possess a negligible bias, the randomness extraction algorithms must be carefully chosen to balance the tradeoff between speed and the security level [10].

3.1 Physical layer

In this thesis, as previously mentioned, a device-dependent QRNG based on probing the quadrature amplitude fluctuations of the vacuum state will be implemented and validated. As the relation (2.23) shows, quadrature measurements of such a field follow an inherently probabilistic Gaussian distribution that can be repeatedly taken to obtain random outcomes. However, direct detection cannot measure the phase properties of incident light since it only measures the photon flux of the light beam [59]. Consequently, vacuum-based QRNGs rely on a homodyne detection scheme, which can measure the amplitude quadrature component of an input signal by comparing it with a laser of the same frequency, the so-called Local Oscillator (LO). In Fig. 3.2, such a schematic model of a self-homodyning detection scheme is illustrated. A strong laser beam, represented by the annihilation operator $\hat{a}_{\mathrm{LO}}(t)$, acts as the LO and interferes with the vacuum state, $\hat{v}_s(t)$, in a lossless Beamsplitter (BS). Here, as shown by (2.24), the purity of the optical state can be guaranteed with good approximation by blocking one of the input ports so that no input signal is present and only the vacuum fluctuations may arise.

In the quantum mechanical picture, a lossless BS, as the one depicted in Fig. 3.3, is described in terms of the annihilation operators by its 2x2 BS matrix [59]:

$$\begin{pmatrix} \hat{a}_3 \\ \hat{a}_4 \end{pmatrix} = \begin{pmatrix} \mathcal{R}_{31} & \mathcal{T}_{32} \\ \mathcal{T}_{41} & \mathcal{R}_{42} \end{pmatrix} \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix}, \tag{3.1}$$

where $\mathcal{R}_{31}$, $\mathcal{T}_{32}$, $\mathcal{R}_{42}$, and $\mathcal{T}_{41}$ represent, respectively, the complex reflection and transmission coefficients for each optical path [59]. Considering the energy conservation between input and output arms, these quantities follow:

$$|\mathcal{R}_{31}|^2 + |\mathcal{T}_{41}|^2 = |\mathcal{R}_{42}|^2 + |\mathcal{T}_{32}|^2 = 1 \quad \text{and} \quad \mathcal{R}_{31}\mathcal{T}_{32}^* + \mathcal{T}_{41}\mathcal{R}_{42}^* = 0. \tag{3.2}$$

By writing these coefficients in their polar form and considering the previous relations:

$$\phi_{31} + \phi_{42} - \phi_{32} - \phi_{41} = \pm\pi \quad \text{and} \quad \frac{|\mathcal{R}_{31}|}{|\mathcal{T}_{41}|} = \frac{|\mathcal{R}_{42}|}{|\mathcal{T}_{32}|}, \tag{3.3}$$

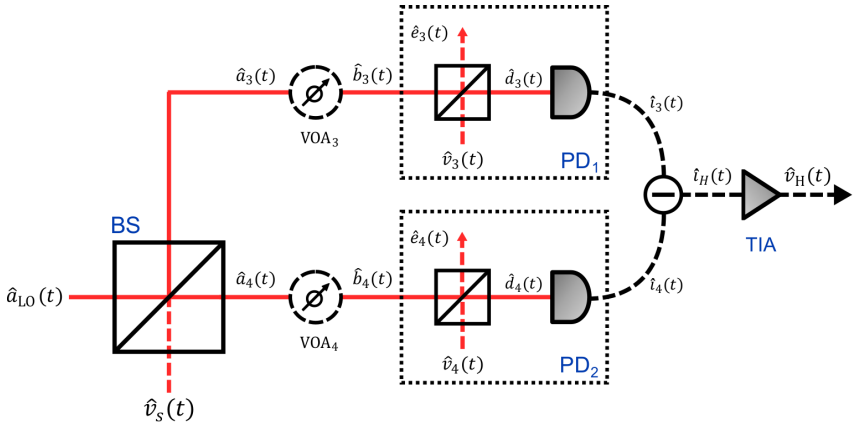


Fig. 3.2: Schematic representation of the homodyne detector model considered for quadrature measurements of the vacuum state. Here, each Variable Optical Attenuator (VOA) is obtained from a lossless BS. Similarly, each practical Photodetector (PD) can be modeled by introducing a lossless BS before a perfectly efficient PD. Electrical paths are presented as dashed lines.

---

which shows that the two sets of coefficients must have equal amplitudes:

$$|\mathcal{R}_{31}| = |\mathcal{R}_{42}| = |\mathcal{R}| \quad \text{and} \quad |\mathcal{T}_{32}| = |\mathcal{T}_{41}| = |\mathcal{T}|. \tag{3.4}$$

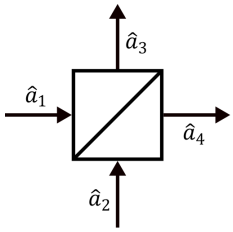


Fig. 3.3: Quantum mechanical representation of a lossless BS as a function of the annihilation operators associated to the input, $(\hat{a}_1, \hat{a}_2)$, and output, $(\hat{a}_3, \hat{a}_4)$, quantized electric field operators.

For simplicity, it is assumed that these coefficients are symmetrical, which yields $\phi_{31} = \phi_{42} = \phi_{\mathcal{R}}$ and $\phi_{32} = \phi_{41} = \phi_{\mathcal{T}}$. In this case, the phase shift between the reflected and transmitted beams yields $\phi_{\mathcal{R}} - \phi_{\mathcal{T}} = \pm\frac{\pi}{2}$. By fixing $\phi_{\mathcal{T}} = 0$ and admitting $\phi_{\mathcal{R}} = \frac{\pi}{2}$, the output signals, $\hat{a}_{3,4}(t)$, in the considered homodyne model are described as [59]:

$$\begin{cases} \hat{a}_3(t) & = i\sqrt{\frac{1}{2}+\Delta}\;\hat{a}_{\mathrm{LO}}(t) + \sqrt{\frac{1}{2}-\Delta}\;\hat{v}_s(t) \\ \hat{a}_4(t) & = \sqrt{\frac{1}{2}-\Delta}\;\hat{a}_{\mathrm{LO}}(t) + i\sqrt{\frac{1}{2}+\Delta}\;\hat{v}_s(t) \end{cases}, \tag{3.5}$$

considering the imbalance of the BS, Δ, such that $|\mathcal{R}|^2 = (\frac{1}{2} + \Delta)$.

The resulting fields are posteriorly measured by two detectors, PD_1 and PD_2, that yield a photocurrent, $\hat{i}_{3,4}(t)$, proportional to the photon flux in each output arm and thus, following the definition (2.35):

$$\hat{i}_{3,4}(t) = q\hat{d}^{\dagger}_{3,4}(t)\hat{d}_{3,4}(t), \tag{3.6}$$

where q is the charge of the electron [59]. Unfortunately, in a realistic application, neither the BS nor the PDs are ideal devices. In fact, the homodyne detection will always be slightly unbalanced due to different coefficient amplitudes in the BS. Thus, typically, a VOA is introduced in each channel to allow balancing of the detection scheme. In this framework, these devices can also

quantify the attenuation at each output arm, which in opposition to the BS imbalance, does not preserve the total impinging optical power. Additionally, a realistic PD can only register a fraction of the photon arrivals, which is reflected in its quantum efficiency. Such a device is modeled by imposing a virtual BS before a theoretical perfect PD [59]. As illustrated in Fig. 3.2, one of the output signals, $\hat{e}_{3,4}(t)$, will be lost while the other, $\hat{d}_{3,4}(t)$, is measured by the detector, such that, analogously to the relations in (3.5):

$$\begin{cases} \hat{e}_{3,4}(t) & = i\sqrt{1-\eta_{3,4}}\ \hat{b}_{3,4}(t) + \sqrt{\eta_{3,4}}\ \hat{v}_{3,4}(t) \\ \hat{d}_{3,4}(t) & = \sqrt{\eta_{3,4}}\ \hat{b}_{3,4}(t) + i\sqrt{1-\eta_{3,4}}\ \hat{v}_{3,4}(t) \end{cases}, \tag{3.7}$$

where $\eta_{3,4}$ denote the quantum efficiency of each PD, and $\hat{v}_{3,4}(t)$ their input vacuum states. Here, $\hat{b}_{3,4}(t)$ represent the output signals of each VOA, which, similarly to the PDs, are moduled as two additional lossless BSs with variable transmissivities $\eta_{\mathrm{VOA}_{3,4}}$. Consequently, the set of equations required to describe the impinging signals yields [64]:

$$\begin{aligned} \hat{d}_3(t) = {} & i\sqrt{\Big(\frac{1}{2}+\Delta\Big)\eta_3\eta_{\mathrm{VOA}_3}}\ \hat{a}_{\mathrm{LO}}(t) + \sqrt{\Big(\frac{1}{2}-\Delta\Big)\eta_3\eta_{\mathrm{VOA}_3}}\ \hat{v}_s(t) \\ & + i\sqrt{\eta_3(1-\eta_{\mathrm{VOA}_3})}\ \hat{v}_{\mathrm{VOA}_3}(t) + i\sqrt{1-\eta_3}\ \hat{v}_3(t) \\ \hat{d}_4(t) = {} & \sqrt{\Big(\frac{1}{2}-\Delta\Big)\eta_4\eta_{\mathrm{VOA}_4}}\ \hat{a}_{\mathrm{LO}}(t) + i\sqrt{\Big(\frac{1}{2}+\Delta\Big)\eta_4\eta_{\mathrm{VOA}_4}}\ \hat{v}_s(t) \\ & + i\sqrt{\eta_4(1-\eta_{\mathrm{VOA}_4})}\ \hat{v}_{\mathrm{VOA}_4}(t) + i\sqrt{1-\eta_4}\ \hat{v}_4(t), \end{aligned} \tag{3.8}$$

and $\hat{v}_{\mathrm{VOA}_{3,4}}(t)$ are the vacuum fields arising from each VOA [59].

Finally, the photocurrents yielded in each PD are subtracted so that, in a balanced detection, only the LO shot noise remains. The photocurrent difference operator, $\hat{i}_{\mathrm{H}}$, is thus given by:

$$\hat{i}_{\mathrm{H}} = \hat{i}_3 - \hat{i}_4 = q\big[\hat{d}_3^{\dagger}(t)\hat{d}_3(t) - \hat{d}_4^{\dagger}(t)\hat{d}_4(t)\big]. \tag{3.9}$$

As described in chapter 2, a strong coherent laser signal operating above the threshold level can be described by a continuous-mode coherent state with amplitude:

$$\alpha_{\mathrm{LO}}(t) = \alpha(t)e^{i(\omega_{\mathrm{LO}}t+\theta(t))} = \sqrt{F+\Delta f_{\mathrm{lo}}(t)}e^{i(\omega_{\mathrm{LO}}t+\theta(t))}, \tag{3.10}$$

where $\alpha(t)$ is the time-dependent photon flux, ω_{LO} the frequency and $\theta(t)$ the initial phase of the laser, F the time-independent mean photon flux and $\Delta f_{\mathrm{lo}}(t)$ denotes the laser intensity fluctuations such that $\langle \Delta f_{\mathrm{lo}}(t)\rangle = 0$ [59]. The time-dependence of the initial phase generally implies the existence of phase noise, but in this analysis, no additional noise contribution will be considered. This consideration remains valid as long as no additional phase shift, $\Delta\phi$, is introduced between the output beams of the BS. Here, identical optical path lengths are considered for both output arms, such that $\Delta\phi = 0$, and this contribution is thus safely disregarded [57].

We shall consider, as a preliminary approach, the theoretical scenario of a perfectly balanced homodyne detection where $\eta_3 = \eta_4 = \eta_{\mathrm{VOA}_3} = \eta_{\mathrm{VOA}_4} = 1$, and $\Delta = 0$. Here, no attenuation of the optical signal is imposed by the VOAs, and each PD acts as an ideal device. Following the previous definitions, and abiding by the formalism in chapter 2:

$$\langle \hat{d}_{3,4}^{\dagger}(t)\hat{d}_{3,4}(t)\rangle = \langle \frac{1}{2}\big[\hat{a}_{\mathrm{LO}}^{\dagger}(t)\hat{a}_{\mathrm{LO}}(t) \mp i\hat{a}_{\mathrm{LO}}^{\dagger}(t)\hat{v}_s(t) \pm i\hat{v}_s^{\dagger}(t)\hat{a}_{\mathrm{LO}}(t) + \hat{v}_s(t)^{\dagger}\hat{v}_s(t)\big]\rangle, \tag{3.11}$$

yielding $\langle \hat{d}_{3,4}^{\dagger}(t)\hat{d}_{3,4}(t)\rangle = \langle \frac{1}{2}|\alpha_{\mathrm{LO}}(t)|^2\rangle$. Given that the phase difference between the LO and the vacuum field is arbitrary [15]:

$$\begin{aligned} \langle \hat{i}_{\mathrm{H}}(t)\rangle &= q\langle \frac{i}{2}\Big[\hat{v}_s^{\dagger}(t)\hat{a}_{\mathrm{LO}}(t) - \hat{a}_{\mathrm{LO}}^{\dagger}(t)\hat{v}_s(t)\Big]\rangle, \\ &= q\sqrt{F}\langle \frac{i}{2}\Big[\hat{v}_s^{\dagger}(t) - \hat{v}_s(t)\Big]\rangle = q\sqrt{F}\langle \hat{Y}_{\mathrm{vac}}\rangle = 0, \end{aligned} \tag{3.12}$$

where $\hat{Y}_{\text{vac}}$ represents the mean quadrature field of the vacuum state at the BS input, $\hat{v}_s(t)$. This yields a null value in accordance with the properties established by (2.22). Thus it is verified that under ideal conditions the balanced homodyne detection scheme probes the quadrature amplitude of the vacuum field, as revealed by the LO shot noise level.

A complete analysis must, however, consider the presence of excess noise under non-ideal conditions. The output signal is finally amplified by the Transimpedance Amplifier (TIA) and will always contain at least electronic noise, which is independent of the impinging optical power. The resultant output voltage, $\hat{v}_{\text{H}}(t)$ is consequently given by the convolution between the detector's impulse response function, $h(t)$, and the sum of all amplified electric currents:

$$\hat{v}_{\text{H}}(t) = G_{\text{TIA}}\big[\hat{i}_e(t) + \hat{i}_{\text{H}}(t)\big] \circledast h(t), \tag{3.13}$$

where G_{TIA} is the TIA gain, and $\hat{i}_e$ is the amplifier electronic noise [64]. Here, $h(t)$, implies additional assumptions, since that, to obtain a complete description, the detector's impulse response function should simultaneously consider the time response of the TIA and the impulse response of each PD, $h_{1,2}(t)$, which are not necessarily equal. To simplify the analysis, it was considered that $h(t)$ can mainly be characterized by the former contribution, since the PDs typically present a much higher bandwidth than the amplifier. Consequently, an equal ideal response was assumed for both photodiodes, such that $h_1(t) = h_2(t) = \delta(t)$. Under these approximations, the description in (3.13) remains valid, and the impulse response of the PD can be approximated to a Butterworth filter, whose frequency response is:

$$|H(\omega)|^2 = \frac{1}{1 + \left(\frac{\omega}{2\pi\Delta f}\right)^{2n}}, \tag{3.14}$$

where n is the filter-order, and Δf is the detector's bandwidth. As $n \to \infty$ it behaves as an ideal low-pass filter, removing all frequencies above the noise bandwidth [57]. Moreover, it is assumed to be normalized in the time-domain such that $\int_{-\infty}^{+\infty} h(t)\, dt = 1$.

In this framework, it shall be considered that the electronic noise mainly arises from the random movements of charge carriers [65]. Consequently, similarly to the intensity fluctuations, the electrical noise is moduled as white noise with a constant power spectral density level over the detector bandwidth. Hence, through the Wiener-Khintchine theorem [65]:

$$\langle \hat{i}_e(t_1)\hat{i}_e(t_2)\rangle = 2\frac{k_{\text{B}}T}{R}\delta(t_1 - t_2), \tag{3.15}$$

where R is the load resistance of the TIA. The electronic noise is thus considered a process with a null mean, $\langle \hat{i}_e\rangle = 0$, whose variance level only depends on the temperature of the optical system and the design of the detector. Similarly, for a theoretical perfect PD with unitary quantum efficiency [65, 66]:

$$\langle \Delta f_{lo}(t_1)\Delta f_{lo}(t_2)\rangle = \text{RIN}F^2\delta(t_1 - t_2), \tag{3.16}$$

where RIN represents the average Relative Intensity Noise (RIN) over the bandwidth of the detector. Finally, considering a non-ideal detection scheme, (3.11) can be rewritten as:

$$\langle \hat{d}^{\dagger}_{3,4}(t)\hat{d}_{3,4}(t)\rangle = \Big(\frac{1}{2} \pm \Delta\Big)\eta_{3,4}\eta_{\text{VOA}_{3,4}}\langle \hat{a}^{\dagger}_{\text{LO}}(t)\hat{a}_{\text{LO}}(t)\rangle = \Big(\frac{1}{2} \pm \Delta\Big)\eta_{3,4}\eta_{\text{VOA}_{3,4}}\, F. \tag{3.17}$$

And since the impulse response is normalized, the expected output voltage yields:

$$\langle \hat{v}_{\text{H}}(t)\rangle = qG_{\text{TIA}}\gamma' F, \tag{3.18}$$

where:

$$\gamma' = \Big(\frac{1}{2} + \Delta\Big)\eta_3\eta_{\text{VOA}_3} - \Big(\frac{1}{2} - \Delta\Big)\eta_4\eta_{\text{VOA}_4}. \tag{3.19}$$

As expected, fluctuations common to both PDs are cancelled, and $\langle \hat{v}_{\text{H}}(t)\rangle = 0$ in a balanced homodyne scheme. The voltage variance, $\sigma^2_{\text{H}}(t)$, can be obtained from the autocovariance function, $K(\tau)$, evaluated at $\tau = 0$ [65]. For an ergodic stochastic process [65]:

$$K(\tau) = \langle \hat{v}_{\text{H}}(t)\hat{v}_{\text{H}}(t+\tau)\rangle - \langle \hat{v}_{\text{H}}(t)\rangle\langle \hat{v}_{\text{H}}(t+\tau)\rangle, \tag{3.20}$$

where:

$$\langle \hat{v}_{\mathrm{H}}(t)\hat{v}_{\mathrm{H}}(t+\tau)\rangle = G_{\mathrm{TIA}}^2 \int_{-\infty}^{+\infty} d\tau' \int_{-\infty}^{+\infty} d\tau'' \Big[\langle \hat{i}_e(\tau')\hat{i}_e(\tau'')\rangle + \langle \hat{i}_{\mathrm{H}}(\tau')\hat{i}_{\mathrm{H}}(\tau'')\rangle\Big] h(t-\tau')h(t+\tau-\tau''), \tag{3.21}$$

and:

$$\langle \hat{i}_{\mathrm{H}}(\tau')\hat{i}_{\mathrm{H}}(\tau'')\rangle = q^2\langle \big[\hat{d}_3^\dagger(\tau')\hat{d}_3(\tau') - \hat{d}_4^\dagger(\tau')\hat{d}_4(\tau')\big]\big[\hat{d}_3^\dagger(\tau'')\hat{d}_3(\tau'') - \hat{d}_4^\dagger(\tau'')\hat{d}_4(\tau'')\big]\rangle. \tag{3.22}$$

This expression is subsequently expanded using the formalism in chapter 2:

$$\begin{aligned}\langle \hat{d}_{3,4}^\dagger(\tau')\hat{d}_{3,4}(\tau')\hat{d}_{3,4}^\dagger(\tau'')\hat{d}_{3,4}(\tau'')\rangle &= \langle \hat{a}_{\mathrm{LO}}(\tau')^\dagger \hat{a}_{\mathrm{LO}}(\tau'')^\dagger \hat{a}_{\mathrm{LO}}(\tau')\hat{a}_{\mathrm{LO}}(\tau'')\rangle \Big[\eta_{3,4}\eta_{\mathrm{VOA}_{3,4}}\Big(\frac{1}{2}\pm\Delta\Big)\Big]^2 \\ &+ \delta(\tau'-\tau'')\langle \hat{a}_{\mathrm{LO}}(\tau')^\dagger \hat{a}_{\mathrm{LO}}(\tau'')\rangle \Big[\Big[\eta_{3,4}\eta_{\mathrm{VOA}_{3,4}}\Big(\frac{1}{2}\pm\Delta\Big)\Big]^2 + (\eta_{3,4}\eta_{\mathrm{VOA}_{3,4}})^2\Big(\frac{1}{2}+\Delta\Big)\Big(\frac{1}{2}-\Delta\Big) \\ &+ \eta_{3,4}^2\eta_{\mathrm{VOA}_{3,4}}(1-\eta_{\mathrm{VOA}_{3,4}})\Big(\frac{1}{2}\pm\Delta\Big) + \eta_{3,4}(1-\eta_{3,4})\eta_{\mathrm{VOA}_{3,4}}\Big(\frac{1}{2}\pm\Delta\Big)\Big].\end{aligned} \tag{3.23}$$

Moreover:

$$\langle \hat{d}_{3,4}^\dagger(\tau')\hat{d}_{3,4}(\tau')\hat{d}_{4,3}^\dagger(\tau'')\hat{d}_{4,3}(\tau'')\rangle = \langle \hat{a}_{\mathrm{LO}}(\tau')^\dagger \hat{a}_{\mathrm{LO}}(\tau'')^\dagger \hat{a}_{\mathrm{LO}}(\tau')\hat{a}_{\mathrm{LO}}(\tau'')\rangle \Big[\eta_3\eta_4\eta_{\mathrm{VOA}_3}\eta_{\mathrm{VOA}_4}\Big(\frac{1}{2}+\Delta\Big)\Big(\frac{1}{2}-\Delta\Big)\Big], \tag{3.24}$$

where:

$$\langle \hat{a}_{\mathrm{LO}}(\tau')\hat{a}_{\mathrm{LO}}(\tau'')\rangle \approx F e^{i(\omega(\tau''-\tau')+\phi(\tau'')-\phi(\tau'))}, \tag{3.25}$$

$$\langle \hat{a}_{\mathrm{LO}}(\tau')^\dagger \hat{a}_{\mathrm{LO}}(\tau'')^\dagger \hat{a}_{\mathrm{LO}}(\tau')\hat{a}_{\mathrm{LO}}(\tau'')\rangle = F^2 + \mathrm{RIN}F^2\delta(\tau'-\tau''). \tag{3.26}$$

With these considerations, it is finally possible to rewrite the autocovariance function as:

$$K(\tau) = \Big[2G_{\mathrm{TIA}}^2\frac{k_{\mathrm{B}}T}{R} + q^2G_{\mathrm{TIA}}^2\beta' F + q^2G_{\mathrm{TIA}}^2\mathrm{RIN}\gamma'^2F^2\Big]\int_{-\infty}^{+\infty} d\tau'\, h(t-\tau')h(t-\tau'+\tau), \tag{3.27}$$

where:

$$\beta' = \Big(\frac{1}{2}+\Delta\Big)\eta_3\eta_{\mathrm{VOA}_3} + \Big(\frac{1}{2}-\Delta\Big)\eta_4\eta_{\mathrm{VOA}_4}. \tag{3.28}$$

Although the solution of the cross-correlation present in (3.27) is non-trivial in the time-domain, it can be simplified by considering the convolution theorem [65]:

$$\begin{aligned}\mathcal{F}\{K(\tau)\} &= \Big[2G_{\mathrm{TIA}}^2\frac{k_{\mathrm{B}}T}{R} + q^2G_{\mathrm{TIA}}^2\beta' F + q^2G_{\mathrm{TIA}}^2\mathrm{RIN}\gamma'^2F^2\Big]\overline{\mathcal{F}\{h(\tau)\}}\mathcal{F}\{h(\tau)\}, \\ &= \Big[2G_{\mathrm{TIA}}^2\frac{k_{\mathrm{B}}T}{R} + q^2G_{\mathrm{TIA}}^2\beta' F + q^2G_{\mathrm{TIA}}^2\mathrm{RIN}\gamma'^2F^2\Big]|H(f)|^2,\end{aligned} \tag{3.29}$$

where $\mathcal{F}$ represents the Fourier transform, and $\overline{\mathcal{F}}$ is its complex conjugate. Finally, the voltage variance yields:

$$\sigma_{\mathrm{H}}^2(t=0) = \frac{2\pi}{3}G_{\mathrm{TIA}}^2\Delta f\Big[\underbrace{2\frac{k_{\mathrm{B}}T}{R}}_{\text{Electronic Noise}} + \overbrace{q^2\beta' F}^{\text{Shot Noise}} + \underbrace{q^2\mathrm{RIN}\gamma'^2F^2}_{\text{RIN Noise}}\Big], \tag{3.30}$$

for a Butterworth's filter of order $n = 3$. It is thus possible to distinguish the three main sources of noise in a homodyne detection scheme. Besides the electronic noise, the ideal operation of

the detector is deviated by the RIN from the LO, which follows a quadratic dependence with its photon flux. It appears due to imperfections in the measurement scheme such as an unbalanced BS, different PD efficiencies, or different signal attenuations in the optical path, which lead to an inability to cancel the fluctuations of the LO. This contrasts with the linear dependence of the shot noise contributions [66]. Obviously, all excess noise should be minimized by assuring a good balancing condition and guaranteeing a significant shot noise preponderance above the electronic noise level. However, the RIN contribution can quickly become dominant, and thus a careful characterization of the detector must be made [57]. During the QRNG operation, these contributions are typically assumed to remain constant, but the classical noise levels can be periodically assessed or continuously monitored through on-off keying the LO [56].

The equation (3.30) generally and adequately characterizes the output signal of the detector. However, although not considered, other factors such as a non-linear response, or an imperfect Common-mode Rejection Ratio (CMRR), can also cause deviations in the detector's response. An example of such an additional noise source comes from the ADC discretization of the continuous outcomes, $v_{\mathrm{H}}(t)$, into a discrete set. The description of the physical layer is thus incomplete without considering a model of the ADC. As represented in Fig. 3.4, a uniform mid-tread quantizer with resolution of n bits and bin width of $\delta_d = \frac{R}{2^{n-1}}$ was considered. Here, R defines the sampling range, which is performed over $[-R + \frac{\delta_d}{2}, R - \frac{3\delta_d}{2}]$ [48]. In this case, the discretized outcomes, $m_i(v_{\mathrm{H}}(t))$:

$$m_i[v_{\mathrm{H}}(t)] = \begin{cases} -R, & v_{\mathrm{H}}(t) < -R + \frac{\delta_d}{2} \\ \delta_d \lfloor \frac{v_{\mathrm{H}}}{\delta_d} + \frac{1}{2} \rfloor, & -R + \frac{\delta_d}{2} \leq v_{\mathrm{H}}(t) < R - \frac{3\delta_d}{2} \\ R - \delta_d, & v_{\mathrm{H}}(t) \geq R - \frac{3\delta_d}{2} \end{cases}, \tag{3.31}$$

which, as will be developed in section 3.2.2, highlights the relevance of choosing an acquisition range that does not misrepresent the output distribution. The quantization error is thus defined as $e(t) = m_i[v_{\mathrm{H}}(t)] - v_{\mathrm{H}}(t)$. Assuming that the measured signal amplitude is significantly larger than the bin width of the ADC, $e(t)$ can be considered uniformly distributed between $[-\frac{\delta_d}{2}, \frac{\delta_d}{2}]$. Under these assumptions, the quantization noise has null mean, and its probability density function is $P(e) = \frac{1}{\delta_d}$. Moreover, it is uncorrelated with the sampled continuous signal. Consequently, its variance, σ_e^2 is calculated as [67]:

$$\sigma_e^2 = \int_{-\frac{\delta_d}{2}}^{\frac{\delta_d}{2}} e^2 P(e)\, de = \int_{-\frac{\delta_d}{2}}^{\frac{\delta_d}{2}} e^2 \frac{1}{\delta_d}\, de = \frac{e^3}{3\delta_d}\Big|_{-\frac{\delta_d}{2}}^{\frac{\delta_d}{2}} = \frac{\delta_d^2}{12}. \tag{3.32}$$

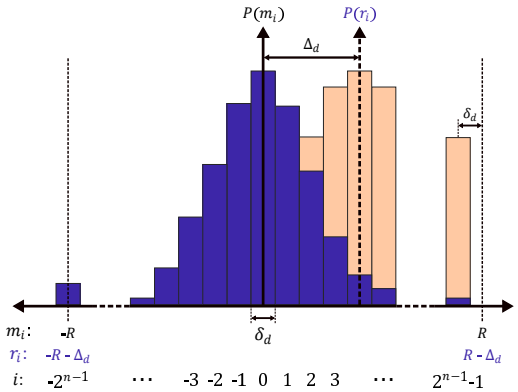


Fig. 3.4: Discretization model of a mid-tread n-bit ADC with bin width δ_d and acquisition range $[-R + \frac{\delta_d}{2}, R - \frac{3\delta_d}{2}]$. A non-null mean is modeled by a second reference frame r centered at the offset Δ_d such that the acquisition range is $[-R - \Delta_d + \frac{\delta_d}{2}, R - \Delta_d - \frac{3\delta_d}{2}]$. Adapted from [48].

Assuming the independence of all noise sources, the total variance is given by the sum of these contributions. Hence, it is finally possible to rewrite the equations (3.18) and (3.30), after

ADC discretization, in function of the wavelength-dependent responsivity, $\mathcal{R}(\lambda) = \frac{q\lambda}{hc}\eta(\lambda)$, and the optical power of the LO, P_{LO}. Assuming that $\eta_3 = \eta_4 = \eta$:

$$\begin{cases} \langle \hat{v}_{\mathrm{H}}(t) \rangle = G_{\mathrm{TIA}}\gamma \\ \sigma^2_{\mathrm{H}}(t=0) = \frac{2\pi}{3} G^2_{\mathrm{TIA}} \Delta f \left[2\frac{k_{\mathrm{B}}T}{R} + q\beta + q\mathrm{RIN}\gamma^2 \right] + \frac{\delta_d^2}{12} \end{cases} , \tag{3.33}$$

where γ and β are, respectively, the redefined γ' and β' quantities, such that:

$$\begin{cases} \beta = \mathcal{R}(\lambda) P_{\mathrm{LO}} \left[\left(\frac{1}{2} + \Delta\right) \eta_{\mathrm{VOA}_3} + \left(\frac{1}{2} - \Delta\right) \eta_{\mathrm{VOA}_4} \right] \\ \gamma = \mathcal{R}(\lambda) P_{\mathrm{LO}} \left[\left(\frac{1}{2} + \Delta\right) \eta_{\mathrm{VOA}_3} - \left(\frac{1}{2} - \Delta\right) \eta_{\mathrm{VOA}_4} \right] \end{cases} . \tag{3.34}$$

As described in chapter 1, the QRNG approach here illustrated presents numerous advantages. Besides allowing high-speed generation rates with widely available products, it relies on an easily obtainable quantum optical state. Moreover, a balanced homodyne detection scheme rejects most of the excess LO noise, which provides resilience against external perturbations.

3.2 Entropy estimation

A secure implementation will require the application of a postprocessing layer consisting of an entropy estimation module followed by a randomness extractor. As required by NIST recommendations [47], a credible justification for the expected entropy estimation should be provided, and the prediction model must be supported by thorough characterization of the randomness source. Here, once again, vacuum-based QRNGs present an advantage since, as shown in the previous section, the ES is clearly defined even when accounting for additional classical noise. In this scheme, two distinct real-time implementations of the models explored in [45] and [48] were considered and are respectively presented in the following sections. In both cases, a device-dependent solution is considered, which implies the trustworthiness of all experimental components. As such, only the presence of an eavesdropper is accounted for, but, as previously described, the classical noise level can still be periodically assessed to ensure that it does not increase.

3.2.1 Shannon entropy

Considering the additive white noise Gaussian channel discussed in chapter 2, the measured distribution can be written as $M = Q + E$, where Q is the quantum noise distribution, and E the electronic noise. After discretization by the ADC into 2^n bins, the amount of randomness originating from the ES gathered from measuring M can thus be quantified by the mutual information [15]:

$$I(M:Q) = H(M) - H(M|Q) = -\sum_{i}^{2^n} P_M(m_i)\log_2(P_M(m_i)) - \int dq\, P_Q(q) H(M|Q=q), \tag{3.35}$$

since Q is a continuous distribution. With increasing binning resolution, this value approaches the maximum channel capacity determined in (2.47):

$$I(M:Q)_{\max} = \frac{1}{2}\log_2\left(1 + \frac{\sigma_Q^2}{\sigma_E^2}\right), \tag{3.36}$$

which implies that the amount of randomness extractable from each sample is physically limited by the QCNR observed at the physical layer [15].

For the uniform ADC model considered, M yields a discretized normal distribution, and thus biased raw data is obtained from the sampling process. To maximize the Shannon entropy of the

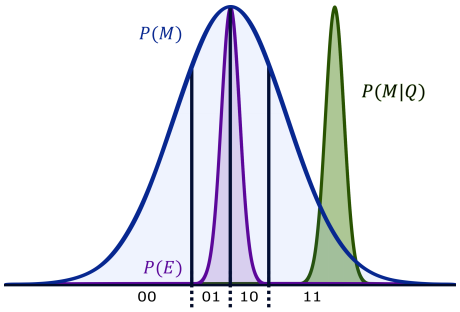


Fig. 3.5: Partitioning into equiprobable bins of the homodyne noise distribution M for a sequence length of 2 bits. This binning is posteriorly imposed upon the electronic noise distribution E in order to calculate the probability of an outcome e falling in each bin. Furthermore, the conditional probability distribution of $P(M|Q)$ for an arbitrary quantum noise outcome q is represented.

---

measured data, the measurements are projected into a uniform distribution by partitioning them into a set of 2^n equiprobable bins [45], whose edges are calculated as:

$$x_p = \mu_M + \sigma_M \sqrt{2}\Big[\operatorname{erf}^{-1}\left(2F_M(x_p) - 1\right)\Big], \quad 0 \leq p \leq 2^n, \tag{3.37}$$

where x_p is the p-th edge, erf^{-1} is the inverse error function, and $F_M(x)$ is the probability of a measurement not being greater than x. In these conditions, a reflected binary sequence of length n can posteriorly be assigned to all outcomes that fall in the same bin, yielding unbiased n-bit random sequences, as represented in Fig. 3.5 for a length of 2 bits. The total entropy of M is now only dependent on the amount of binning, such that $H(M) = n$. As can be seen in the same figure, the conditional probability distribution $P(M|Q)$ corresponds to the probability density function of the electronic noise shifted by the outcome q.[1] Since the equiprobable partitioning yields a higher concentration of bins near $m = 0$, $H(M|Q)$ as given by (2.41), is intuitively higher at $q = 0$, which yields the probability density function of the electronic noise. A lower bound for the mutual information can consequently be established by only considering this case [15]:

$$I(M : Q) \geq H(M) - H(M|q = 0) = H(M) - H(E). \tag{3.38}$$

Consequently, the minimum fraction of entropy that can be extracted from each sample without compromising the implementation is simply given by the subtraction between the entropy of the binned signal and the electronic noise entropy. An estimation of $H(E)$ can similarly be obtained by imposing the binning calculated on its measurements $H(E) = -\sum_{i=1}^{2^n} p_i^{\mathrm{e}} \log_2 p_i^{\mathrm{e}}$, where p_i^{e} is the probability of finding an electronic noise measurement in each bin [45]. Finally, although the electronic noise constitutes the major contribution to the fraction of entropy originating from classical effects, on a practical generation scheme, an additional component will be introduced by excess LO noise due to an unbalanced detection, H_{unbal}, such that $H_{\mathrm{class}} = H(E) + H_{\mathrm{unbal}}$, and:

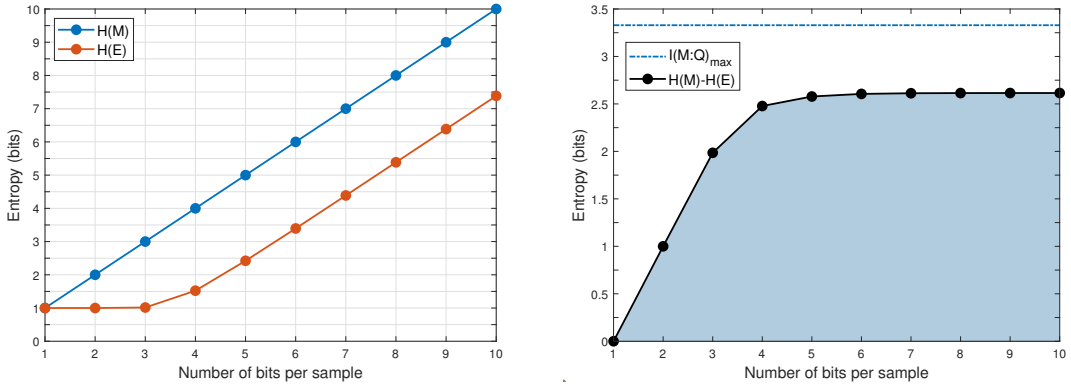
$$I(M : Q) \geq n - H_{\mathrm{class}}. \tag{3.39}$$

Unfortunately, it is not easy to quantify these contributions and, consequently, only the electronic noise is typically considered since it can simply be measured by removing the LO.

This entropy estimation method is exemplified in Fig. 3.6 for a QCNR of 20 dB. As can be seen, the effective entropy that can be extracted from each sample asymptotically approaches a maximum value, which is significantly lower than the theoretical maximum $I(M : Q)_{\max}$. As seen in Fig. 3.6a, this limit results from a similar increase rate on the entropy of the electronic noise and the measured distribution. After a certain amount of binning, the higher concentration of bins near $m = 0$ leads to the electronic noise being partitioned at the same rate of the measured

[1] This result will be demonstrated in section 3.2.2.

distribution, and thus no additional effective entropy can be extracted. Consequently, it is necessary to determine the binning that maximizes the effective bits extracted. In this algorithm, the distribution is partitioned for increasing sequence lengths until gain in the extractable entropy is no longer observed. This is defined by the stopping criteria of 0.1 bit. This hard limit on the extractable randomness ultimately restricts the generation rate of the QRNG regardless of how the distribution is binned. Moreover, as discussed, randomness is not adequately estimated by the Shannon entropy, which challenges the reliability of this protocol.



(a) (b)

Fig. 3.6: (a) Entropy of the measured distribution $H(M)$ and the classical noise $H(E)$ under multiple partitioning lengths. (b) Respective lower bound for the mutual information $I(M|Q)$. Dashed line represents the theoretical maximum for the mutual information. Adapted from [15].

3.2.2 Worst-case conditional min-entropy

A more acceptable entropy estimation can be obtained by considering the discretization imposed by the ADC instead of an arbitrary binning, and quantifying the maximum probability of an eavesdropper guessing an outcome of the generator, given knowledge of all classical contributions. With this objective, the ADC model described in section 3.1 is considered, and a non-null mean of the measured distribution M is modeled by a reference frame r centered at the offset Δ_d. Under this framework, the probability distribution of the discretized signal [48]:

$$P_M(m_i) = \begin{cases} \int_{-\infty}^{-R-\Delta_d+\frac{\delta_d}{2}} p_M(r)\,dr, & i = -2^{n-1} \\ \int_{r_i-\Delta_d-\frac{\delta_d}{2}}^{r_i-\Delta_d+\frac{\delta_d}{2}} p_M(r)\,dr, & -2^{n-1} < i < 2^{n-1}-1 \\ \int_{R-\Delta_d-\frac{3\delta_d}{2}}^{\infty} p_M(r)\,dr, & i = 2^{n-1}-1 \end{cases}, \tag{3.40}$$

where $p_M(m)$ follows a Gaussian distribution centered at the origin. Here, the ADC resolution and acquisition range present a relevant consideration. For a given resolution, the acquisition range must be properly chosen as to not risk endangering the security of the implementation. For instance, a wide acquisition range will lead to the concentration of all samples on a small number of quantization levels. Thus we misrepresent the Gaussian distribution and necessarily limit the randomness that can be extracted. The necessity to lower the entropy estimation in this situation is justified by the consideration that, with increasing acquisition ranges, the homodyne and electronic noise distributions will be progressively indistinguishable, since measurements are mapped to the same limited number of bins. In an extreme case, guessing the yielded outcome will become trivial to an adversary, as the limited number of unique values greatly increases the probability of finding a measurement in each particular bin. On the other hand, a narrow acquisition range increases the probability of a measurement falling outside the considered interval and, consequently, leads to saturation of the first and last bins. In this case, the probability of

these particular results increases, which could be used by an observant adversary to increase its chances of predicting the QRNG outcome [48, 57].

The conditional probability density function $p_{M|E}(m|e)$ can be calculated through:

$$p_{M|E}(m|e) = \frac{p_{M,E}(m,e)}{p_E(e)} = \left(\frac{\sigma_E\sqrt{2\pi}}{2\pi\sigma_M\sigma_E\sqrt{1-\rho^2}}\right) e^{-\frac{1}{2(1-\rho^2)}\left[\left(\frac{m}{\sigma_M}\right)^2 - 2\rho\left(\frac{me}{\sigma_M\sigma_E}\right) + \left(\frac{e}{\sigma_E}\right)^2\right] + \frac{1}{2}\left(\frac{e}{\sigma_E}\right)^2}, \tag{3.41}$$

where ρ is the correlation coefficient between M and E:

$$\rho = \frac{\mathrm{cov}(M,E)}{\sigma_M\sigma_E} = \frac{\mathrm{cov}(Q+E,E)}{\sigma_M\sigma_E} = \frac{\sigma_E}{\sigma_M}, \tag{3.42}$$

since Q and E are statistically independent. Consequently [48]:

$$p_{M|E}(m|e) = \frac{1}{\sqrt{2\pi(\sigma_M^2-\sigma_E^2)}} e^{-\frac{(m-e)^2}{2(\sigma_M^2-\sigma_E^2)}} = \frac{1}{\sqrt{2\pi(\sigma_Q^2)}} e^{-\frac{1}{2}\left(\frac{m-e}{\sigma_Q}\right)^2}, \tag{3.43}$$

and its discretized conditional probability distribution $P(M|E)$ follows (3.40). This expresses the probability of an eavesdropper with full access to the classical fluctuations guessing a particular outcome of M, and yields the probability density function of Q shifted by the electronic noise outcome e [15]. A similar result ensues for $P(M|Q)$, as shown in Fig. 3.5. An entropy estimation can now be made considering the maximum probability of the discretized conditional distribution. Following the definition of the worst-case min-entropy (2.45) and (3.40):

$$\max_{m_i\in M} P_{M|E}(m_i|e) = \max\begin{cases} \frac{1}{2}\left\{1-\mathrm{erf}\left(\frac{e+R+\Delta_d-\frac{\delta_d}{2}}{\sigma_Q\sqrt{2}}\right)\right\} \\ \mathrm{erf}\left(\frac{\delta_d}{2\sigma_Q\sqrt{2}}\right) \\ \frac{1}{2}\left\{1+\mathrm{erf}\left(\frac{e-R+\Delta_d+\frac{3\delta_d}{2}}{\sigma_Q\sqrt{2}}\right)\right\} \end{cases}, \tag{3.44}$$

where erf is the error function. The maximum probability of $P_{M|E}(m_i|e)$ lies in either one of the boundary bins or at the central value $r_i - e = 0$, since this corresponds to the best guessing strategy. In fact, if the classical noise outcome largely exceeds the ADC range, the outcome m_i has a high probability of being saturated at one of the edge bins. Thus guessing it becomes trivial to the eavesdropper and no randomness can be obtained. Since a trusted device scenario is here considered, a maximum excursion for the classical noise $e \in [e_{\min}, e_{\max}]$ can be assumed from the characterization of the implementation. If the interval is symmetric, the probability value of the lower boundary is always inferior, and can consequently be dropped [48]:

$$\begin{aligned} H_{\min}(M|E) &= -\log_2\left[\max\left\{\frac{1}{2}\left[1+\mathrm{erf}\left(\frac{e_{\max}-R+\Delta_d+\frac{3\delta_d}{2}}{\sigma_Q\sqrt{2}}\right)\right], \mathrm{erf}\left(\frac{\delta_d}{2\sigma_Q\sqrt{2}}\right)\right\}\right], \\ &= -\log_2\left[\max\left\{c_1, c_2\right\}\right]. \end{aligned} \tag{3.45}$$

In this implementation, a maximum excursion of $5\sigma_E$ was always assumed for the classical noise. This is expected to fail only once in every 1 744 278 measurements. As can be seen in Fig. 3.7, the min-entropy is now dependent not only on the QCNR but also on the sampling range and resolution of the ADC. As such, the performance of the implementation is no longer limited by the QCNR, and a higher extraction ratio can be obtained by simply increasing the ADC resolution. Conversely, a less powerful digitizer is necessary for high QCNRs. Surprisingly, randomness can be extracted even for negative QCNRs, when the classical fluctuations overcome the quantum noise. Nonetheless, for an unoptimized R, there is a threshold QCNR at which the distribution saturates the boundary bins, and thus the entropy estimation quickly diminishes. For higher resolutions, the larger amount of bins imposes a lower threshold as the probability of guessing the most likely value will be lower. This point, where $c_1 = c_2$, can be used to reach the optimal min-entropy value in ADCs with variable sampling ranges [48].

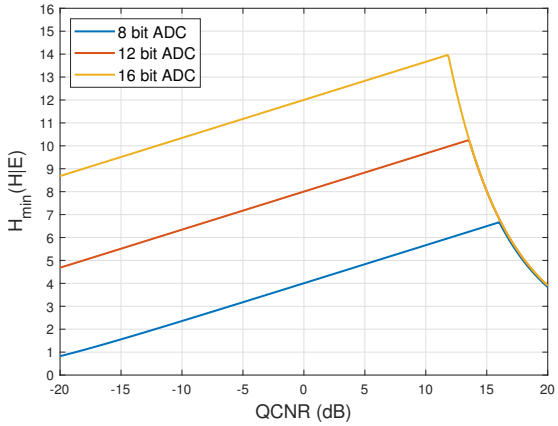


Fig. 3.7: Worst-case conditional min-entropy as a function of the QCNR for an 8-bit, 12-bit, and 16-bit ADC. An unoptimized R results on a threshold at which the entropy estimation quickly diminishes. Simulations taken for a maximum excursion of $5\sigma_E$, $\Delta_d = 0$, $R = 20$, and $\sigma_E = 1$.

3.3 Randomness extraction

Two probability distributions X and Y defined in the same domain $\mathcal{X}$ are said to be ϵ-close if their statistical difference is bound [68]:

$$d(X,Y) = \max_{x \in \mathcal{X}} |P_X(x) - P_Y(x)| \leq \epsilon, \tag{3.46}$$

where ϵ is the security parameter. A (n, m, k, ϵ) randomness extractor is a mathematical function that converts n bits from a (n, k)-source into m bits with a distribution ϵ-close to a uniform distribution U_m over $\{0,1\}^m$, which is the ideal output of a RNG [68, 29]. Here, a random distribution is considered a (n, k) source if its min-entropy $H_{\min} \geq k$. This value defines the maximum number of uniformly distributed bits that can be extracted from the original n-bit sequence. Nonetheless, randomness can only be extracted if the input sequence already possesses some extractable entropy. Consequently, $m \leq k$ must necessarily hold to obtain a uniform sequence. The specific extractor implementation chosen must always consider the algorithmic speed, as to not compromise the final throughput of the generator, and preserve as many bits as allowed by the entropy estimated in section 3.2. Here, two distinct algorithms based on different principles were explored, although only the Toeplitz extractor was chosen in the final implementation.

3.3.1 SHA-512 hashing

Deterministic randomness extractors are defined as a function Ext : $\{0,1\}^n \to \{0,1\}^m$, and are very attractive for forgoing additional randomness sources, as only the input sequence is required. Unfortunately, no universal deterministic extractor exists for unpredictable sources [10, 68]. Nonetheless, several methods have been proposed, such as XORing parallel randomness sources or different subsets of random sequences, taking the least significant bit, applying the von Neumann de-biasing algorithm, or feeding a linear feedback shift register [15, 29]. These methods are frequently uncritically accepted as they require few resources, forgoing execution on a computer or micro-controller, and can produce sequences that pass numerous statistical tests. Nevertheless, the distilled randomness is not information-theoretically secure, and their application may actually introduce unexpected correlations [69]. Alternatively, one-way cryptographic hash functions project their input sequence to a set of fixed length m such that the input values can not be determined solely from the output sequence. Consequently, their output is as close to uniformly distributed as possible, minimizing the probability of two different inputs resulting in the same hash value. Nevertheless, collisions still occur, and blindly applying a hash function does not suffice since the size of the input sequence n must be chosen so that it has enough entropy.

In this implementation, a randomness extraction algorithm was developed by hashing subsets of the QRNG output using the SHA-512 function, which outputs sequences of 512 bits [63]. In this case, n must clearly be higher than 512 bits to guarantee a uniformly distributed output. In fact, the input sequence length is chosen as [57]:

$$n = \lceil 512 \frac{H_{\mathrm{t}}}{H_{\mathrm{q}}} \rceil, \tag{3.47}$$

where H_{q} is the estimated entropy due to quantum fluctuations and H_{t} the total entropy of the raw output. This method has the advantage of relying on well-tested and fast hashing implementations, such as the one here chosen [70]. The implemented algorithm can process the raw output at approximately 8.69 Mbps on a Intel i7-9700K CPU. Unfortunately, nonuniversal hashing still relies on computational assumptions and, ultimately, does not provide information-theoretically provable RNs [29]. Even worse, biases of the hashing function are inherited by the output RNs even if the input is perfectly random [69].

3.3.2 Toeplitz-hashing

A (n, m, d, k, ϵ) seeded extractor is defined as $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$. It accepts a n-bit input sequence, and a perfectly random d-bit seed to output a m-bit sequence ϵ-close to U_m. In particular, an extractor is said to be strong if concatenating the output $\mathrm{Ext}(X, U_d)$ with the seed U_d yields a distribution ϵ-close to U_{m+d}, and thus maintains the randomness of the initial seed [68]. Consequently, the QRNG output can be subdivided into blocks that are subsequently hashed with the same seed without compromising the security of the implementation. These constructions are especially attractive for providing some information-theoretically provable randomness extractors secure against quantum adversaries such as the Trevisan extractor. Unfortunately, this specific implementation is particularly slow [29]. An alternative method for constructing seeded extractors employs two-universal hashing functions, which are randomly chosen from a universal hashing family $\mathcal{H} = \{h : \mathcal{S} \to \mathcal{T}\}$, where the probability $P_{h\in\mathcal{H}}\{h(x) = h(y)\} \leq \frac{1}{|\mathcal{T}|}, \forall x \neq y \in S$ [29].

One particularly promising implementation employs universal hashing by constructing a $n \times m$ Toeplitz matrix and obtaining m random bits by multiplication with the raw data vector. Since a Toeplitz matrix is solely defined by the first column and the first row, a seed of length $m + n - 1$ is required. Consequently, a seed longer than the output vector is necessary, and no net randomness can be extracted. Fortunately, a Toeplitz extractor constitutes a strong extractor [48], and hence the initial seed can be recycled in each subsequent application. If the good statistical properties of the initial seed are assured, the uniformity of the output is information-theoretically guaranteed by the leftover hash lemma. This theorem states that given a two-universal hashing family $\mathcal{H} = \{h : \{0,1\}^n \to \{0,1\}^m\}$, and a probability distribution $X \in \{0,1\}^n$ with $H_{\min}(X) \geq k$, if [68]:

$$m = k - 2\log_2\big(\frac{1}{\epsilon}\big), \tag{3.48}$$

then for $x \in X$, $h \in H$, and $\epsilon > 0$, $\mathrm{Ext}(x, h) := h(x)$ is a (k, ϵ) strong extractor. In other words, the statistical distance $d\Big(\big(\mathrm{Ext}(X, U_d), U_d\big), \big(U_d, U_m\big)\Big) \leq \epsilon$ [68].

In the real-time implementation of this algorithm, the raw bits were subdivided into sequences of 2^{12} bits ($n = 4096$) and the output m was chosen so that [57]:

$$m = \lfloor 2^{12} p \frac{H_{\mathrm{q}}}{H_{\mathrm{t}}} \rfloor, \tag{3.49}$$

where p was arbitrarily chosen at 90% to account for any potential entropy overestimation. Note that this method does not fix a specific security parameter and thus a careful analysis of the matrix dimensions should be made. Furthermore, estimations obtained through the Shannon entropy do not satisfy (3.48), which can decrease the security level of this particular random extractor. In general, the length of the output sequence is given by [29]:

$$m = n\frac{H_q}{H_t} - 2\log_2\big(\frac{1}{\epsilon}\big), \tag{3.50}$$

where $\frac{H_q}{H_t}$ expresses the fraction of entropy from quantum contributions on a 1-bit sequence. In the following analysis, numbers from a Mersenne Twister PRNG were used to seed the Toeplitz matrices.

3.3.2.1 Length-compatible Toeplitz-hashing

With the Toeplitz-extractor described, raw bits can be processed at approximately 3.68 Mbps for an input length of 32 Mbits, which severely limits the output rate of the QRNG. Furthermore, the algorithmic complexity of the Toeplitz-vector multiplication is $O(n^2)$, and thus the postprocessing rate quickly decreases when hashing sequences of greater length. To improve the speed of the implementation, a fast multiplication algorithm for Toeplitz matrices that reduces the complexity to $O(nlog(n))$ was implemented [71]. This method explores a well-known method for multiplication of $n \times n$ circulant matrices, C_n, which are a particular kind of Toeplitz matrices where each row is shifted by only one entry. These can be solely characterized by the first column $\vec{a}_n$, and have the useful property of being diagonalized by the discrete Fourier transform matrix F_n such that $C_n = F_n^{-1}\text{diag}(F_n\vec{a}_n)F_n$, where $\text{diag}(\cdots)$ represents the diagonal matrix. Consequently, its multiplication with a given vector $\vec{x}$ yields [72]:

$$C_n\vec{x} = \mathcal{F}^{-1}\{\mathcal{F}(\vec{a}_n) \odot \mathcal{F}(\vec{x}_n)\} = \mathcal{F}^{-1}\{\vec{v} \odot \vec{y}\}, \tag{3.51}$$

where $\odot$ represents the Hadamard product and $\mathcal{F}^{-1}$ the inverse Fourier transform. An arbitrary $n \times m$ Toeplitz matrix, $T_{n\times m}$, can be embedded into a circulant matrix of size $n + m$ simply by concatenating extra elements. In fact, if $\vec{a}_n = [a_0, \cdots, a_{n-1}]$ is its first column and $\vec{b}_m = [a_0, \cdots, a_{-(m-1)}]$ is the first row, then the Toeplitz matrix can be contained in a circulant described by [72]:

$$\vec{a}_{n+m} = [a_0, a_1, \cdots, a_{n-1}, a_0, a_{-(m-1)}, \cdots, a_{-1}]. \tag{3.52}$$

As such, it is possible to transform the Toeplitz hashing into a circulant matrix multiplication by a vector $\vec{r}$ with the raw binary output by following the steps:

1. Construct $\vec{a}_{n+m}$ from the elements of the Toeplitz matrix, as described by (3.52).
2. Append $\vec{0}$ of size m to $\vec{r}$ and compute $\vec{y} = \mathcal{F}\{[\vec{r}, \vec{0}]\}$.
3. Compute $\vec{u} = \mathcal{F}^{-1}\{\mathcal{F}(\vec{a}_{n+m}) \odot \vec{y}\}$.
4. Extract the first m entries of $\vec{u}$, which are the solution for $T_{n\times m}\vec{r}$.

The length-compatible algorithm described was thus implemented on a GeForce RTX 3070 GPU. To avoid exhausting the memory of the GPU, the multiplication problem is subdivided into smaller matrices with 4 Mbits input blocks, which are serially processed. Since the computational precision required to retrieve accurate results from the Fourier transform increases with the input length, the blocks are further subdivided into parallelized smaller batches to allow the use of single-precision calculations, which vastly increases the postprocessing speed [71]. In Table 3.1, these results are compared with a non-parallelized implementation on an Intel i9-10900k CPU for different batch sizes. Batches of 2 Mbits show better performance and are thus chosen in the final implementation, yielding a mean postprocessing rate of 143.29 Mbps.

Table 3.1: Speed (Mbps) of the hashing algorithm for different input lengths and batch sizes.

Input length (Mbits)	CPU Implementation		GPU Implementation		Gain (%)	
	1 Mbit Batch	2 Mbit Batch	1 Mbit Batch	2 Mbit Batch	1 Mbit Batch	2 Mbit Batch
4	68.67	74.28	125.12	143.29	82.13	92.91
8	72.33	89.19	126.48	143.18	74.87	60.53
16	58.73	83.42	111.52	137.35	89.89	64.65
32	38.28	62.59	83.01	116.21	116.85	85.67

Chapter 4

Implementation of a Real-time Vacuum-based QRNG

In this chapter, a dedicated real-time implementation of the vacuum-based generation scheme previously described in chapter 3 is explored, and its main experimental results are presented. In section 4.1, the physical layer is described and characterized. In 4.1.1, the variance characterization curve of the homodyne detector is taken to assess the conditions where randomness extraction is feasible. Moreover, a study of the output homodyne noise was posteriorly made in section 4.1.2 to verify the preponderance of quantum fluctuations. The analysis then moves to comparatively characterize the performance of the entropy estimation models employed. In section 4.2, the results under a Shannon entropy model are presented, and in 4.2.1 a framework to estimate the excess entropy contribution from an unbalanced detection under this method is proposed. Posteriorly, results pretending to the final implementation are shown in section 4.2.2. Finally, the quality of extracted randomness is assessed, and the implementation validated, by applying a set of statistical tests in section 4.3.

4.1 Experimental Setup

A diagram of the experimental setup used during the characterization of the QRNG scheme is presented in Fig. 4.1.

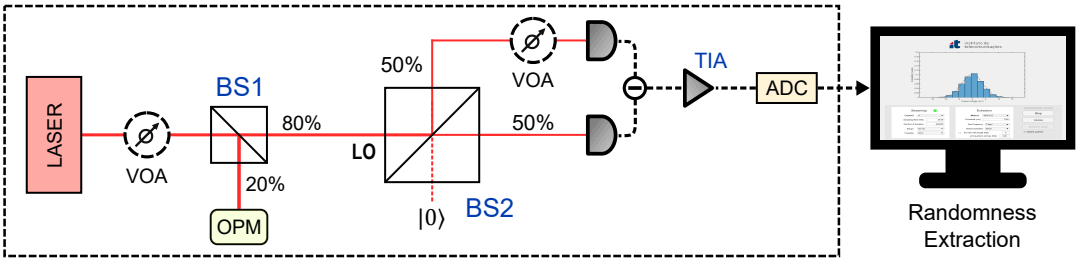


Fig. 4.1: Experimental setup employed for the characterization of the QRNG implementation. A laser is split by a BS with one of its input ports blocked (BS2) and the subsequent photocurrents are subtracted. An 80/20 BS (BS1) and an Optical Power Meter (OPM) allow monitoring of the input power which, such as the balancing condition, is controlled by a VOA. The resulting signal is processed in real-time by a Matlab application to obtain a string of unbiased random bits.

In this scheme, a continuous-wave laser (Yienista OSICS TLS/C) tuned at 1550.92 nm is employed as the LO, and a VOA is used to accurately vary its output power. Posteriorly, a 80/20 BS (BS1) and a OPM were introduced to monitor the input power at a 50/50 BS (BS2). Here,

another VOA was used to allow variation of the balancing condition of the detection scheme. The resultant output beams are detected by an AC-coupled balanced receiver (WL-BPD1GA) with a transimpedance gain of 3500 V/W and an output bandwidth from 300 kHz to 1 GHz. This suppresses the low-frequency noise contributions that arise from electric hum and flicker noise in the circuit, which would otherwise need to be removed by introducing a DC block or by digitally selecting a flat spectral band, as will be described in chapter 5. The subsequent response is sampled at 983.04 MSa/s by a 16-bit ADC module (Texas Instruments ADS54J60EVM) with a ± 0.95 V acquisition range, which yields a quantization noise variance, $\frac{\delta_d^2}{12}$, of 7×10^{-5} mV^2. As specified by the Nyquist sampling theorem, the signal cannot be accurately recovered when its bandwidth is larger than half the sampling frequency, f_s. Here, however, the aliasing effects are advantageous. Since only white noise is measured, they lead to a flatter spectral band and higher entropy. In fact, perfect reconstruction of the homodyne signal is not the objective of a RNG. Consequently, to avoid temporal correlations between measurements, the sampling rate must be less than twice the detector's bandwidth, or, in this case, 2 GSa/s. Finally, the raw measurements are continuously postprocessed in real-time by a Matlab graphical interface that implements the entropy estimation models and randomness extractors described in chapter 3.

Since a device-dependent implementation was considered, a careful analysis of all the optical components is required to assure the viability of the implementation. Consequently, the characterization curve of each BS was traced to assess their balancing condition and evaluate the power relations between their output arms. For the BS1, a linearisation with a coefficient $r^2 = 0.9999$ yields an asymmetry of (79.22 ± 0.04) %, and the power at the 80% output, $P_{80\%}$, can be estimated from the value measured at the OPM through a multiplication by (3.812 ± 0.009). Similarly, the 50/50 BS was found to be subjected to a maximum asymmetry of (50.78 ± 0.05) %.

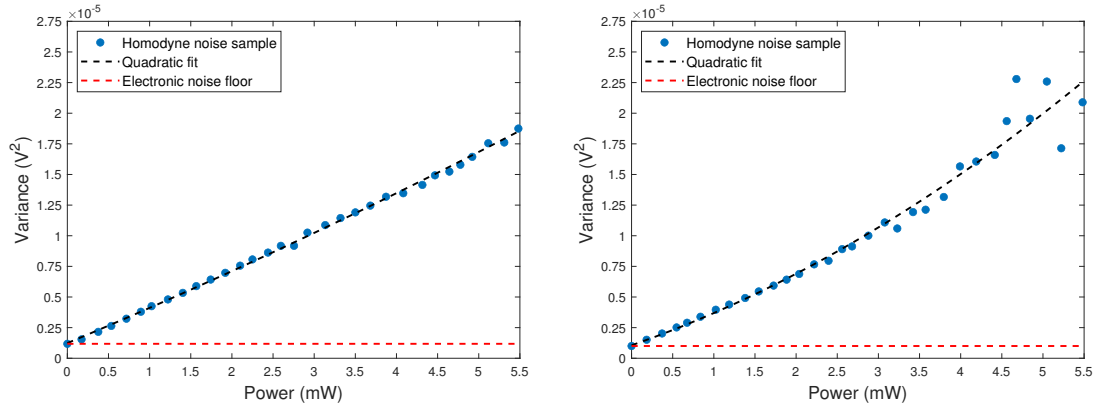
4.1.1 Characterization of the balanced detector

To guarantee that the LO output power is chosen so that quantum fluctuations dominate the measured noise, the characterization curve of the WL-BPD1GA balanced detector was also traced. As represented in Fig. 4.2a, the variance of the output signal was taken, for 2.5 M noise samples, at different LO powers, which were set by varying the optical attenuation of the VOA. As explored in section 3.1, the variance σ^2 of the measurements taken follows a quadratic dependency with the input power at BS2, P_{LO}:

$$\sigma^2 = aP_{\mathrm{LO}}^2 + bP_{\mathrm{LO}} + c, \tag{4.1}$$

where a represents the LO excess noise, b the shot noise contribution, and c the electronic noise floor. Here, a quadratic fit with $r^2 = 0.998$ yields $c = 1.24 \times 10^{-6}$ V^2, $b = 2.81 \times 10^{-6}$ V^2/mW, $a = 6.15 \times 10^{-8}$ V^2/mW^2. This clearly illustrates the good balancing condition of the homodyne scheme, as the variance follows an almost linear relation with the LO power. In these conditions, the increase in the signal's variance can mainly be attributed to the preponderance of shot noise and thus a higher QCNR can simply be obtained by increasing the impinging power. This maximizes the entropy obtained per sample and is thus the desirable operation region. Nonetheless, care should be taken to not saturate the TIA. Moreover, for a higher impinging power, slight asymmetries in the detection eventually result in the appearance of excess noise. However, this detection scheme presents an extremely long linear stage, with contributions dominated by quantum fluctuations in the region $P_{\mathrm{LO}} < \frac{b}{a} \approx 45.7$ mW. Consequently, to experimentally verify this quadratic power dependency, the characterization under a purposefully unbalanced condition is represented in Fig. 4.2b. The quadratic fit with $r^2 = 0.989$ now yields $c = 1.30 \times 10^{-6}$ V^2, $b = 2.06 \times 10^{-6}$ V^2/mW, $a = 3.32 \times 10^{-7}$ V^2/mW^2, and presents predominance of shot noise contributions for approximately $P_{\mathrm{LO}} < 6.20$ mW. Besides describing the homodyne noise, the characterization curve allows to express the detector voltage response in shot-noise units by dividing the acquired signal, expressed in physical units (Volts), by a conversion factor, k:

$$k = \sqrt{4bP_{\mathrm{LO}}}. \tag{4.2}$$



(a) (b)

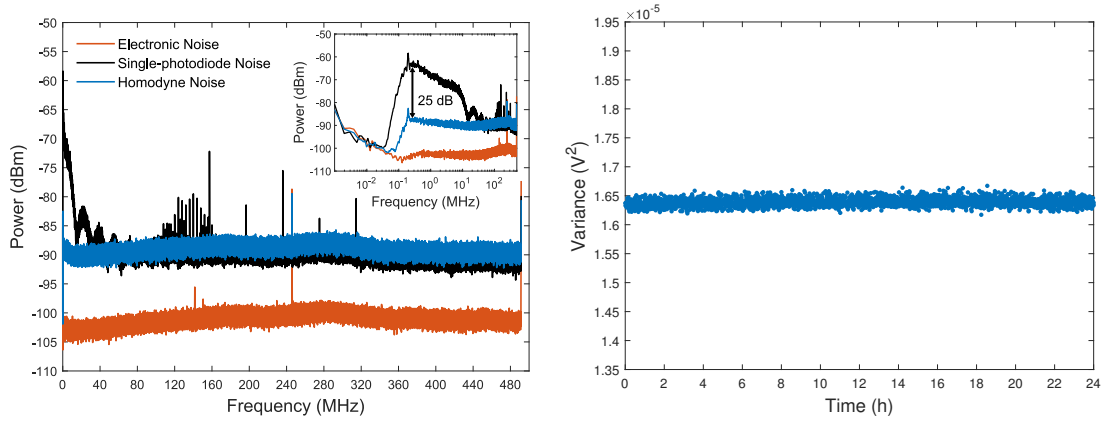
Fig. 4.2: Characterization curve of the balanced detector for (a) the good balancing condition determined by BS2 ($50/50 \pm 0.78\%$), and (b) under an intentionally unbalanced detection (1.3 dB attenuation in one output arm). Each variance was evaluated over 2.5 M noise samples.

This allows conversion of variances in volts to shot-noise units by dividing them by k^2. Here, k is defined so that the measured quadrature variance of a vacuum state, in shot noise units, is equal to $\frac{1}{4}$, in accordance with the theoretical values established in (2.22) [53].

4.1.2 Noise characterization

With the previous analysis supporting the detection scheme, the laser output power was set at 11 dBm, and the VOA was removed so that approximately 5.5 mW reach the input of the BS2. In Fig. 4.3a, the spectral power density of the measured homodyne noise is represented. As can be seen, the strong spectral contributions observed when only one of the photodiodes is illuminated are effectively rejected in the subtraction signal with a CMRR up to 25 dB. At low frequencies, the spectral band is defined by the high-pass filter imposed by the AC coupling of the detector and the ADC board, which allows forgoing the introduction of additional filtering. Nonetheless, strong contributions were observed at 245.76 MHz and 491.52 MHz. These, however, do not result from any classical contributions, but are intrinsic to the ADC and remain even with an idle channel. These spurs, located exactly at $\frac{f_s}{4}$ and $\frac{f_s}{2}$, result from a mismatch in the DC offset of the four time-interleaved cores employed by the ADS54J60 to reach the chosen sampling rate [73]. Akin to gain mismatches, these non-idealities are corrected by a dedicated circuit, which estimates and holds the internal DC offset after power up with no signal applied. This allows the complete removal of these contributions, and the scheme thus yields the flat power density curve expected for a viable QRNG. Unfortunately, variations in temperature will lead to an outdated estimation and the reappearance of these spectral spurs. Consequently, they should be continuously monitored and a new offset calibration made, if necessary. At room temperature, these variations proved to be negligible, allowing the continuous operation of the QRNG for long time periods. Finally, the spectral density of electronic noise was taken, confirming the preponderance of quantum noise.

In these conditions, an average variance of $1.64 \times 10^{-5}\,\mathrm{V}^2$ was observed over 1×10^9 samples. As shown in Fig. 4.3b, the scheme presents high stability over long periods of time. This indicates a stable balancing condition, and the absence of large fluctuations of the electronic noise floor over a period of at least 24 h, which is essential to the reliability of the implementation. Moreover, all the measured noise follows the expected null-mean Gaussian distribution, as shown in Fig. 4.4a. In fact, negligible means of -0.0171 mV and -0.0140 mV were respectively calculated for the homodyne noise and electronic noise distributions, both being smaller than the ADC bin width of 0.0290 mV. Here, once again, the high noise clearance obtained can be highlighted since a noise floor of $1.04 \times 10^{-6}\,\mathrm{V}^2$ was observed. Neglecting any excess noise from the LO and considering

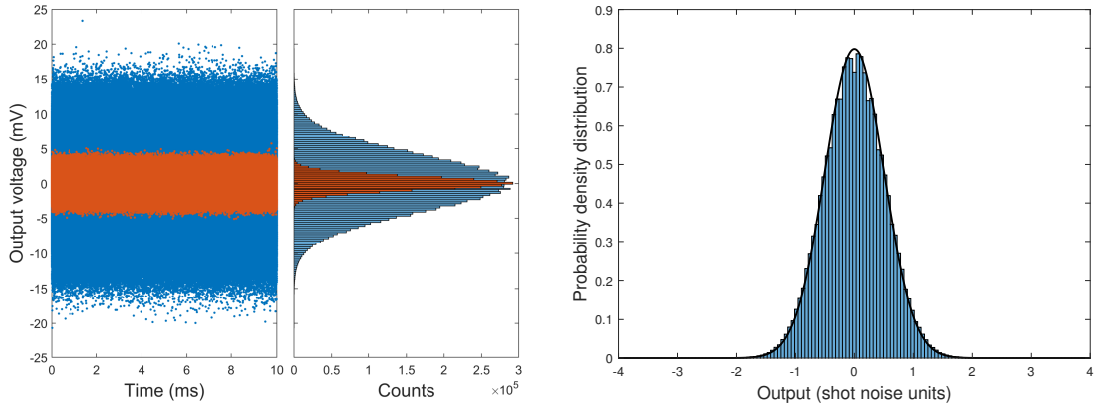


(a) (b)

Fig. 4.3: (a) Spectral power density taken for the homodyne noise (blue), electronic noise (orange), and for a single-photodiode (black). Inset highlights low-frequency contributions. (b) Time evolution of the noise variance. Each variance was evaluated over 503×10^3 samples.

---

the quantization noise, the variance of quantum contributions $\sigma_Q^2 = \sigma_M^2 - \sigma_E^2 - 2(\frac{\delta_d^2}{12})$ yields $1.54 \times 10^{-5}\,\mathrm{V}^2$, and a QCNR of approximately 11.7 dB was obtained. Moreover, the noise distribution can be converted from physical units to the phase space by following (4.2). As represented in Fig. 4.4b, the measured state closely follows the theoretical probability distribution curve for the quadrature values of a vacuum state defined in (2.23). Nevertheless, a variance of $\sigma_M^2 = 0.2644$ was calculated, which is slightly larger than the expected value of $\frac{1}{4}$ due to the presence of classical noise [53].

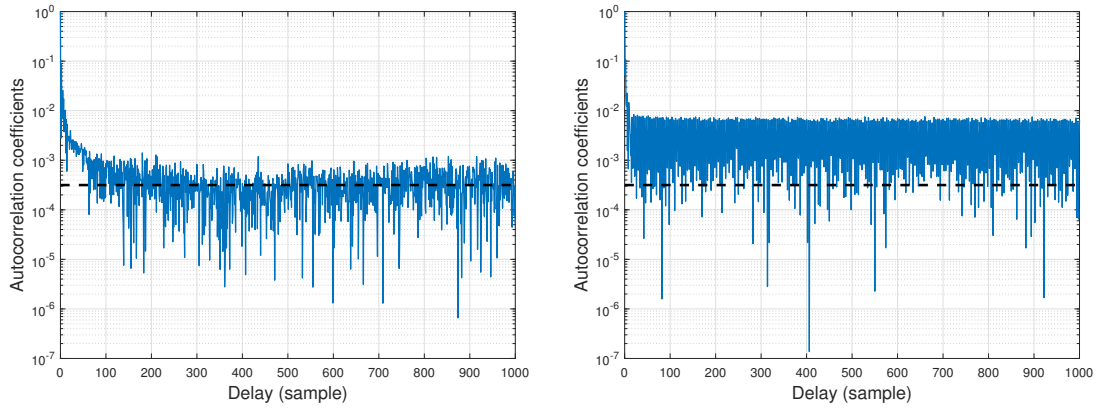


(a) (b)

Fig. 4.4: (a) Time representation of the total (blue) and electronic (orange) signal for 10 M noise samples. The electronic noise histogram is represented for 2.5 M samples. (b) Distribution of the total noise represented in shot-noise units for 10 M samples. Solid line shows the expected probability distribution for the quadrature of a vacuum-state.

In Fig 4.5a, a correlation analysis for 10 M points over a delay of 1×10^3 samples is represented. This acts as a basic statistical validation since, for a sufficiently large sample size L, the normalized autocorrelation coefficients of a white noise process are normally distributed around a null average value with a standard deviation of $\frac{1}{\sqrt{L}}$ [74]. In practice, the finite bandwidth of the signal and the presence of classical noise impose some residual correlations. Here, a mean value of 9.96×10^{-4} was observed, and the coefficients are largely well within the expected standard deviation of 3.16×10^{-4}

for truly random data of this sample size. Nonetheless, for delays up to 60 samples relatively high correlations are observed, which could compromise the security of the QRNG. These can be largely attributed to the non-ideal response of the TIA amplifier [75] and are effectively removed by the randomness extraction. Regardless, the correlations observed are consistent with the assumption of almost-uncorrelated samples and starkly contrast with the values observed for the electronic noise distribution shown in Fig. 4.5b. Here, a mean value of 1×10^3 is seen, and the coefficients largely fall outside the theoretically expected interval. This clearly illustrates the unreliability of electronic noise and the necessity to carefully quantify the entropy available for randomness generation.



(a) (b)

Fig. 4.5: Absolute autocorrelation coefficients for 10 M samples taken from (a) the measured total distribution and the (b) electronic noise. Dashed line represents the theoretical standard deviation for the autocorrelation function of 10 M truly random samples.

4.2 Entropy Estimation

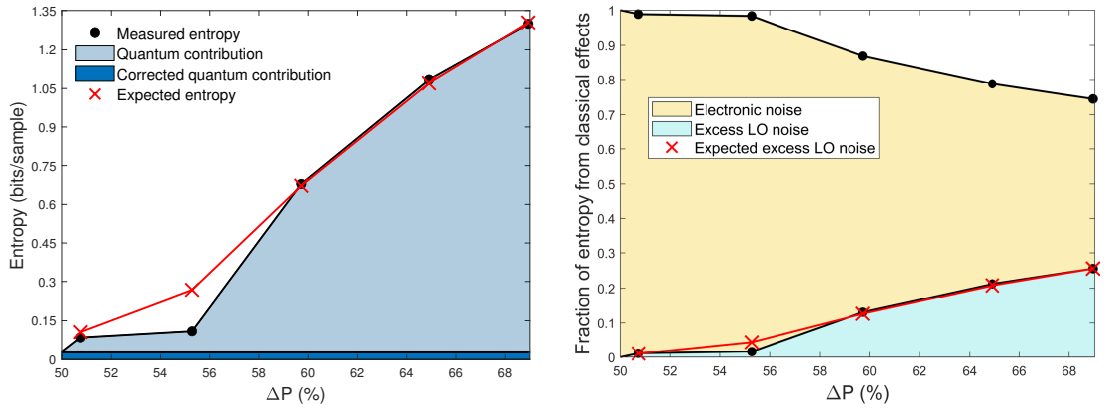
In the aforementioned conditions, the measured noise samples were initially subjected to the Shannon entropy estimation model described in section 3.2.1. Here, through (3.36), a maximum mutual information between the total noise distribution and the quantum signal of 1.99 bits was calculated for the observed QCNR. In practice, the binning of the distribution consistently converges to a sequence length of 4 bits, after which no significant gain in bits extracted is observed. The distribution is thus partitioned into 16 bins, as previously exemplified, yielding a mean extractable entropy of 1.29 bits per sample. Consequently, an extraction ratio, $\frac{H_q}{H_t}$, of approximately 0.323 is achieved, which clearly shows the inability of this framework to reach high extraction rates even when faced with a large noise clearance. Following this model, the QCNR must increase to improve the performance of the generator. As shown through (3.33), this can be achieved either by minimizing the electronic noise or simply increasing the LO power, which is not always possible due to the additional RIN contributions, H_{unbal}, that lead to an overestimation of the available quantum entropy.

4.2.1 Estimation of excess entropy due to an unbalanced detection

To study this effect, a slight variation on the experimental setup needs to be introduced since the following results pertain to the implementation explored in [57]. Specifically, the detector was here replaced by a ThorLabs PDB450C balanced photodetector with a coupled 8535 Inmet RF DC Block to remove low-frequency contributions, and the signal was sampled by an 8-bit Picoscope 6403 ADC set to a ±50 mV acquisition range. As seen in Fig. 4.6a, we measured the entropy

contributions as a function of the detection asymmetry $\Delta P = \frac{P_1}{P_{\text{total}}}$, which is defined as the ratio between the optical power measured at the output without the VOA, P_1, and the total impinging power, P_{total}. Here, the LO power was fixed at approximately 1.33 dBm to avoid saturating the TIA output signal. Posteriorly, the attenuation of the VOA at the BS2 output arm was increased to iterate over the detection's asymmetry. It should be noted that this is theoretically distinct from simply varying the BS transmittance since the total power that reaches the PDs decreases with the additional attenuation. The measured entropy, as can be seen in Fig. 4.6a, appears to increase with the imbalance of the detection. Since the total impinging optical power does not increase, it is trivial to attribute this to excess LO noise.

To obtain an estimation of H_{unbal}, we start by calibrating the measurement scheme and consider that the most balanced state achievable (asymmetry of 50.75%) has a negligible excess LO noise contribution. Assuming that H_{quant} remains relatively constant, all posterior increases are thus the result of introducing excess LO noise. As seen in Fig. 4.6b, for small asymmetries this contribution increases almost linearly. By contrast, as a consequence of a higher signal-to-noise ratio, the contribution from the electronic noise decreases in the same proportion that H_{unbal} increases. Thus, given a constant total entropy and impinging optical power, the fraction of entropy from classical effects is in reality constant and independent of the asymmetry. If the excess LO noise is unaccounted for, this results in more bits accessible to an eavesdropper. Naturally, these assumptions result in an overestimation of H_{quant}, since the measurement scheme is always slightly unbalanced. To obtain an acceptable estimation, a linearisation with $r^2 = 0.9523$ was performed, yielding $H_{\text{unbal}} = 0.0741\ (\Delta\text{P} - \frac{1}{2})$. Then, knowing the maximum possible asymmetry, we estimate that $H_{\text{unbal}} = 0.0554$ bits for our balanced implementation. We thus find a corrected quantum contribution of 0.0282 bit, which corresponds to a decrease of 66.3% relative to the original estimation. Unfortunately, these assumptions hold true only when no additional attenuation is introduced, and thus this method is best applied when only the BS ratio varies. Here, the decrease in P_{total} leads to a reduction in the quantum noise contributions with an increasing attenuation, and the corrected estimation should be adjusted accordingly. Nonetheless, the value obtained is an acceptable worst-case estimation for asymmetries close to a balanced detection.



(a) (b)

Fig. 4.6: (a) Quantum entropy contribution in function of the detection asymmetry. Dark blue shaded area shows the corrected H_{q}, when H_{unbal} is considered. (b) Fraction of entropy from classical effects. Red lines present the entropy values for the theoretically expected variances.

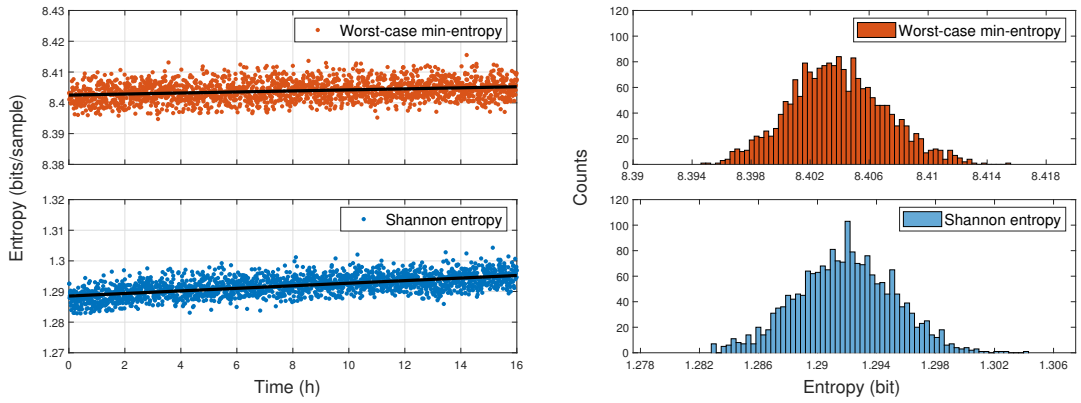
4.2.2 Worst-case conditional min-entropy

The previous results clearly demonstrate the high impact of excess LO noise under the Shannon entropy framework. Unfortunately, due to saturation of the TIA output, the same study is difficult to apply to this implementation at the chosen LO power. In an effort to improve the

extraction ratio without the necessity for an arbitrary increase in the QCNR, the model described in section 3.2.2 was implemented.

For the experimental conditions described in section 4.1.2, the min-entropy obtained from (3.45) yields an average value of approximately 8.40 bits, which results on an extraction ratio of 0.53. This corresponds to an immediate relative increase of 62.5% without any changes to the physical layer. With this model, the extraction ratio is now mainly limited by the acquisition range of the chosen ADC, which is much larger than the maximum amplitude of the measured signal. This increases the probability of an eavesdropper guessing an outcome, although this constraint is here partially compensated by the high resolution of the ADC. Nonetheless, the performance of the implementation could significantly be improved by using a more appropriate sampling range. In fact, if the optimized interval of 20 mV were to be used, approximately 13.97 bits per sample could be extracted without further changes to the physical layer. Alternatively, the output signal could be further amplified to the appropriate levels, although this would introduce additional noise.

In practice, despite the stability of the signal's average variance, small oscillations in its value also induce fluctuations in the entropy estimations, as represented in Fig. 4.7a. As expected from the previous analysis, these values are consistent over time and have no significant fluctuations. Nonetheless, a small upwards trend in the values of the Shannon entropy model is seen, being most likely due to a small increase of the thermal noise floor. As seen in Fig. 4.7b, the calculated entropies fall between $[1.2829, 1.3043]$ bits and $[8.3947, 8.4155]$ bits for the Shannon and min-entropy respectively, yielding similar variation amplitudes. Besides highlighting the necessity of regularly evaluating the contributions of the electronic noise, this shows that simply trusting the entropy assessment for any data set is inadequate. Naturally, a cautious approach should be taken, and solely considering the average values is insufficient for a secure real-time implementation. Consequently, the worst-case is considered, and to account for the possibility of some excess noise, a min-entropy of 8.39 bits was chosen, yielding an extraction ratio of 0.5244.



(a) (b)

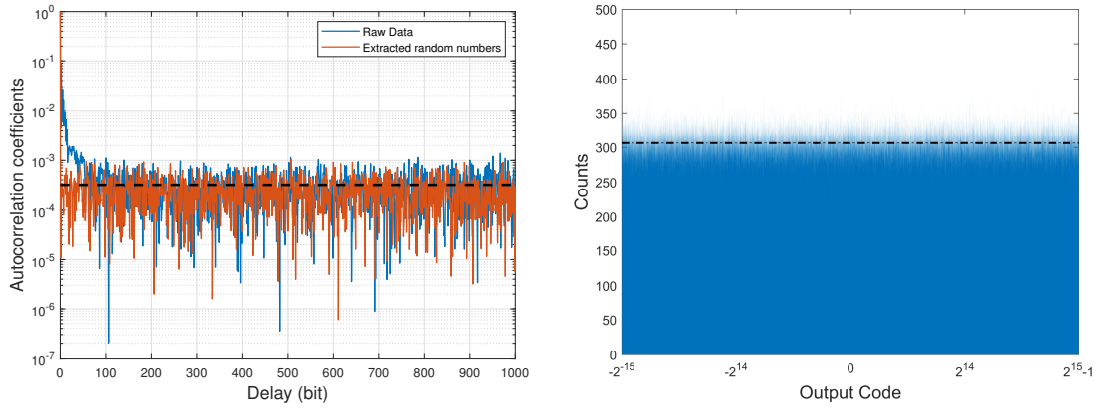
Fig. 4.7: (a) Evolution of the entropy estimation under both entropy estimation models. Each value was calculated over 503 808 samples, and the black lines represent the corresponding linear fits. (b) Distribution of the 1920 entropy estimation values acquired during the this time period.

In the aforementioned conditions, sets of 503 808 samples were continuously acquired by the Matlab application and subjected to the real-time Toeplitz extractor previously described. Considering the description in section 3.3.2, for the conventional Toeplitz multiplication the matrix parameters are set as $n = 4096$ and $m = 1933$, yielding an effective extraction ratio of 0.472 random bits from each raw ADC bit. Thus the security parameter for the hashed values is calculated through (3.50) as $\epsilon \approx 2^{-107}$. This value can easily be adjusted according to the security requirements by simply varying the matrix dimensions. With this configuration, considering the used sampling rate, a maximum theoretical generation rate of 7.42 Gbps can be achieved, if the computation constraints are disregarded. Unfortunately, the slow Toeplitz algorithm limits the effective

throughput to approximately 2 Mbps. Lastly, as described, the length-compatible Toeplitz multiplication was implemented to increase the efficiency of the randomness extractor. Here, each hash iteration was performed over blocks of 2.5×10^5 raw samples (4 Mbits), and posteriorly processed in smaller batches. Given the large input size, the effective extraction ratio can be increased to maintain the same security bound, since this parameter will drastically decrease with the matrix size chosen [41]. This minimizes the number of bits that are discarded by the randomness extraction algorithm and allows effective extraction ratios closer to the value defined by the min-entropy. The final implementation thus yields an effective extraction ratio of 0.5243 and $\epsilon \approx 2^{-105}$. This allows generation rates up to 8.23 Gbps, although the effective throughput is still limited by the hashing algorithm and thus highly dependent on the hardware used. For the configuration presented in section 3.1 a maximum effective generation rate of approximately 75 Mbps is expected. Removing this constraint should obviously be the focus of future work.

4.3 Statistical Validation

As a preliminary assessment of the effectiveness of the randomness extraction algorithm, the autocorrelation analysis was repeated for the extracted binary sequences. As can be seen in Fig. 4.8a, the Toeplitz-hashing algorithm successfully removes correlations from the raw sequence. In fact, a delay of one bit guarantees absolute coefficients inferior to 9.38×10^{-4}. This contrasts with the raw bit sequence, which presents the most significant correlations within a delay of 16 bits due to the resolution of the ADC. The validity of the randomness extraction is further proven by plotting a histogram of 16-bit integers derived from the QRNG output, which, as can be seen in Fig. 4.8b, follows the expected uniform distribution. These results clearly support the implementation but are not sufficient evidence of randomness.



(a) (b)

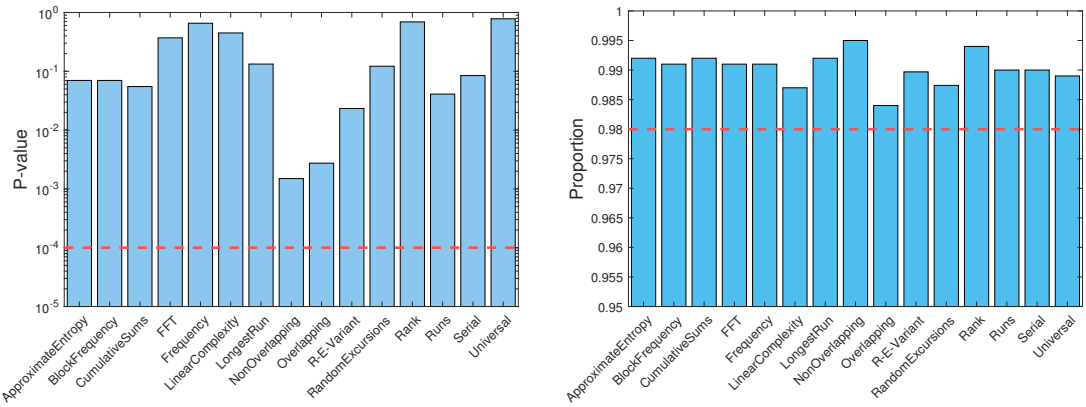
Fig. 4.8: (a) Autocorrelation coefficients for 16 M bits taken for the raw data and Toeplitz-hashed random bits. Dashed line represents the theoretical standard deviation for the autocorrelation function of 16 M truly random bits. (b) Distribution of 20 M 16-bit random numbers extracted from the raw data. Dashed line represents the expected number of outcomes for a given code.

To test the reliability of the implementation, the generator was subjected to an extensive set of statistical tests that search for evidence of non-random behavior in the output sequences. Note that, here, this usually means a deviation from the uniform distribution, and, consequently, the raw output is expected to fail the majority of tests even if perfectly random. Unfortunately, certifying a RNG is a futile task as there is no set of statistical tests that can conclusively validate a generator. An implementation should continuously be subjected to ever more stringent evaluations until a conclusive failure is obtained, after which design improvements are required. Moreover, it should be highlighted that it is the generator that is validated, never the random sequences themselves.

In fact, a good RNG is expected to produce some sequences that fail the statistical tests, and their absence is enough evidence of a poor implementation.

In this work, the standard NIST [6], Dieharder [8], and TestU01 [7] (both the SmallCrush and Crush batteries) statistical suites were applied. In total, 145 different tests and respective subtests were considered. Although describing each one is beyond the scope of this work, all evaluate the null hypothesis (that the sequence under test is random) and return a *P-value* that expresses the probability of a true random generator yielding a result less random than the one observed [6]. Given a chosen significance level α, which expresses the probability of Type I errors, if $P\text{-}value < \alpha$, the null hypothesis should be rejected. The same is done for $P\text{-}value > 1 - \alpha$ as it indicates that the generator produces sequences too close to uniformity. Moreover, under the null hypothesis, the *P-values* for different sequences under test should be uniformly distributed, and a certain proportion of sequences is expected to fail in any given run. Consequently, any statistical evaluation should be applied to multiple sequences of the generator, and two test passing criteria are established: uniformity of the *P-values* for a given test, and the minimum proportion of sequences that should pass. As an example, for $\alpha = 0.01$ and a given test run with $n = 1000$ sequences, approximately 10 sequences are expected to fail. The acceptable proportion range can be calculated as $(1 - \alpha) \pm 3\sqrt{\frac{\alpha(1-\alpha)}{n}}$ [6]. The uniformity of *P-values* can in its turn be evaluated through a goodness-of-fit test such as a Kolmogorov-Smirnov (KS) test, and its own value used to summarize the test result for multiple sequences.

The NIST statistical test results for approximately 10 Gbits are represented in Fig. 4.9. Here, the default significance level $\alpha = 0.01$ was chosen and 1000 sequences of 10 Mbits were subjected to the statistical evaluations. For any given sequence, the null hypothesis is rejected if the $P\text{-}value < 0.01$. The uniformity of the *P-values* of each statistical test is evaluated using a chi-squared test, yielding the respective $P\text{-}value_T$ [6]. These values are represented for each test in Fig. 4.9a. The generator is considered to pass a given test if $P\text{-}value_T \geq 0.0001$ [6]. Moreover, as seen in Fig. 4.9b, a minimum pass proportion of 980/1000 should be observed for all tests with the exception of the random excursions and random excursions variant assessments, where it is 855/873. As can be seen, all of the evaluations meet these criteria and thus we fail to reject the null hypothesis. Passing these NIST statistical tests is an excellent indicator of the quality of the generator and fulfills the certification standards employed in most literature works.

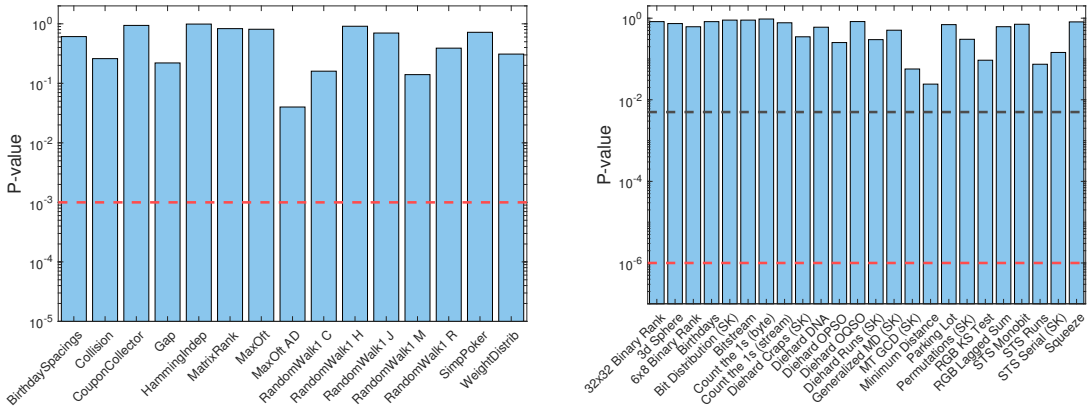


(a) (b)

Fig. 4.9: NIST test results for $\alpha = 0.01$ and a data size of 10 Gbits (1000 bit streams of 10 Mbits). To pass an test (a) $P\text{-}value_T$ should be larger than 1×10^{-4}, and (b) the proportion of sequences satisfying $P\text{-}value \geq 0.01$ should be ≥ 0.98. Red lines represent the minimum pass thresholds. For tests with multiple parameters the worst case is represented.

Nonetheless, as mentioned, the statistical validation is never complete and additional testing can be applied to better characterize the quality of the QRNG. Consequently, both the TestU01

and Dieharder statistical suites were provided with a random pool of approximately 232 Gbits, although the amount of randomness consumed by each battery depends on the applied tests. This provides enough numbers to minimize the number of times that the pool is rewound, which causes tests to iterate over the same sequences. In Fig. 4.10a, the results of the TestU01 SmallCrush battery are summarized. Here, blocks of 32 bits are used to obtain double-precision floating-point values in the interval $[0, 1]$, which are posteriorly tested. It provides a fast verification to detect if more stringent validation is worth applying. As can be seen, unsurprisingly, this battery fails to detect any deviation in the expected behavior of the generator output, and all *P-values* fall inside its significance threshold of $[0.001, 0.9990]$. This is also consistent with the results obtained with the Dieharder battery, as represented in Fig. 4.10b. Here, the default significance level of $\alpha = 0.000001$ is used to mark a given test result as failed, and a 0.005 threshold to flag a weak result. Furthermore, the battery was configured to resolve ambiguity mode. This progressively increases the amount of numbers tested when a weak result is found until the *P-value* is either within the acceptable range or the test has conclusively failed. Given these parameters, the Dieharder battery is significantly more stringent than the previous statistical suites, and its failure is highly significant. Here, a preliminary run returned 2 weak results on *Diehard OPSO* with *p-value* $= 0.9991$ and *Diehard Minimum Distance* with 0.0041 . Posterior analysis with increased statistical power conclusively resolved this uncertainty, and thus, again, we fail to reject the null hypothesis. Nonetheless, it should be highlighted that some rewinds of the bit file still occur during the suite run, and analysis with larger random pools should be made in the future.



(a) (b)

Fig. 4.10: (a) Results for TestU01 SmallCrush applied with $\alpha = 0.001$. Line represents the significance level. (b) Results for the Dieharder battery set to resolve ambiguity mode with $\alpha = 0.000001$. Lines represent the weak (black) and fail (red) threshold values. For tests with multiple *p-values* a KS test is applied to obtain a representative value.

Given these results, we failed to find evidence of non-random behavior in the QRNG output, illustrating the reliability of the implementation. Obviously, this does not certify randomness and only means that no evidence of non-randomness was observed in this specific instance. This analysis should be continuously expanded until some weakness is found. With this objective, we applied the TestU01 Crush battery, which is known for being hard to pass for many standard RNGs [76]. Note that due to the small size of the data pool, the statistical tests were applied to the same number sequences, and the file rewound between each one. A preliminary run revealed that 94 out of the 96 applied tests successfully passed, with two failures: one in the *RandomWalk1 H* test, and the other in the *LinearComp*. To assess the significance of these results, the suspect tests were sequentially repeated for non-overlapping sequences. The results are summarized in Table. 4.1. Here, only one sequence failed the *RandomWalk1 H*, while three failures were observed for the linear complexity test. This could indicate that the former is the result of a statistical anomaly. However, both cases failed to achieve the pass proportion threshold for the original

significance level $\alpha = 0.001$. Moreover, the worst *P-value* of the *LinearComp* test decisively converges to 1, which indicates a conclusive failure.

Table 4.1: TestU01 Crush: Results for the repeated application of the suspect tests. The worst P-value is represented. Here eps means a value $< 1.0 \times 10^{-300}$ and eps1 $< 1.0 \times 10^{-15}$.

Statistical Test	Parameters	P-value	Number of Tests	Pass Proportion
RandomWalk1 H	L = 10000	0.9997	50	0.98 (minimum 0.9856)
LinearComp	r = 0	1 - eps1	200	0.985 (minimum 0.9923)

Consequently, we are forced to reject the null hypothesis and conclude that there is sufficient evidence for non-randomness in the generator output. Nonetheless, a more exhaustive analysis of the Crush battery results is necessary, given the limitations here imposed by the size of the data being tested. It stays unclear if these results are a failure of the QRNG or a limitation of the statistical analysis. Integration of these batteries in the Matlab algorithm could help mitigate the constraints of feeding an adequate amount of RNs to the statistical tests. Nevertheless, a possible reason for these results originates from the assumption that the seed of the Toeplitz matrix is truly random. In fact, pseudo-random numbers from the Mersenne Twister PRNG were used, which is known to fail the linear complexity tests of the Crush library [76]. Thus another randomness source, preferably a TRNG, should be chosen. Despite an exhaustive evaluation eventually rejecting this implementation, this does not imply the absence of useful randomness or the inadequacy of the generation scheme, but merely suggests future design improvements. The necessity of using the TestU01 Crush battery to detect any biases in the QRNG output highlights the number of statistical tests passed, which goes beyond most certification efforts.

Chapter 5

Time-interleaved QRNG within a classical communication channel

In this chapter, an alternative QRNG scheme that is time-interleaved with a QPSK tributary signal within a coherent classical communication channel is proposed in an effort to remove the need for a dedicated generation device. This greatly reduces the cost of implementation since it allows integration into already existing optical systems, which were not purposefully implemented to support quantum randomness generation. After a brief description of the generation scheme, the multi-purpose function of the implementation is certified in section 5.1.1 by retrieving the classical data transmitted. Posteriorly, the QRNG operation is characterized in section 5.1.2 to assure the preponderance of quantum noise, and a basic validation is performed in section 5.1.3 to assess the quality of the RNs obtained.

5.1 Experimental Setup

A schematic representation of the proposed QRNG scheme is shown in Fig. 5.1. A heterodyne detection scheme was considered for the transmission of the QPSK signal. Although it requires a more complex digital signal processing when compared with the conventional homodyne approach, this allows to simplify the experimental setup since a second balanced detector and a 90° optical hybrid are no longer necessary [77]. At the Tx side, a 1550 nm continuous-wave laser (Yenista OSICS Band C/AG TLS) at 10 dBm is split by a 35/65 BS (BS1) formed by the combination of a Polarization Beamsplitter (PBS) and a Polarization Controller (PC). The 8.10 dBm beam is posteriorly sent towards a balanced BS (BS2) where it acts as the LO in the coherent receiver. Meanwhile, the polarization of the second beam is set by another PC to maximize the output

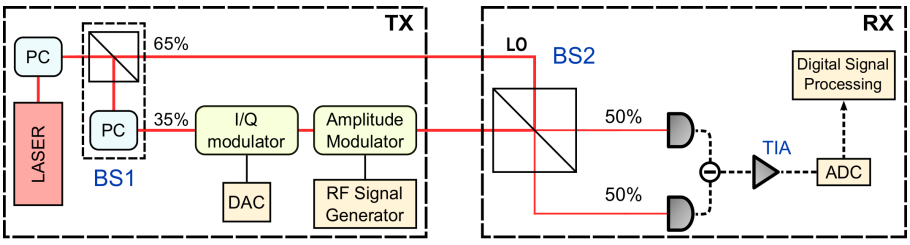


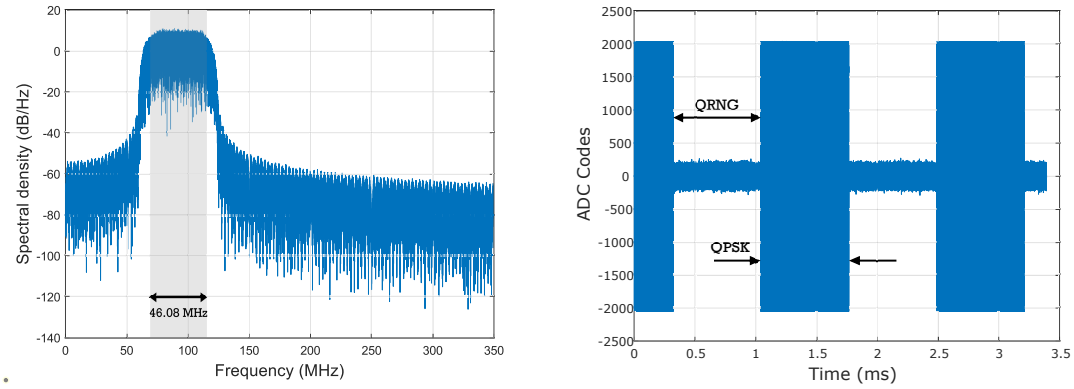
Fig. 5.1: Schematic representation of the experimental setup for the time-interleaved QRNG. An amplitude modulator allows to alternately perform heterodyne detection over the QPSK signal, or obtain a balanced homodyne detection scheme with a vacuum state at one of the input ports [58].

power of a u2t Photonics I/Q optical modulator. Single sideband modulation is thus performed by the I/Q modulator using a SHF 807 RF driver and the signal provided by a Digital-to-analog

converter (DAC, Texas Instruments DAC38J84) running at a 1474.56 MSa/s sampling rate. The electrical modulation contains a QPSK signal, $y(t) = q(t)e^{i2\pi f_Q t}$, upconverted to $f_Q = 92.16$ MHz, where:

$$q(t) = h_{\mathrm{rc}}(t) \circledast \sum_k a(k)\delta(t - kT). \tag{5.1}$$

Here, h_{rc} is a root-raised-cosine filter with roll-off factor $\beta = 0.4$, $a(k)$ represents the complex-valued QPSK symbols transmitted $a(k) \in \{\exp(i\frac{\pi}{4}), \exp(i\frac{3\pi}{4}), ..., \exp(i\frac{7\pi}{4})\}$, and T is the symbol period [77]. As can be seen in Fig. 5.2a, a symbol rate of 46.08 MBaud was chosen, which results on a maximum optical link throughput of 92.16 Mbps. An acousto-optic amplitude modulator (Gooch & Housego 26035-2-1.55-LTD) with a 40 dB extinction ratio and a 35 MHz operating frequency was posteriorly employed to impose on-off shift keying upon the QPSK signal. The driving signal was provided by an HP 8116A signal generator, and rectangular pulses with an amplitude of 5 V and a 50% duty cycle at a frequency of 700 Hz were used.



(a) (b)

Fig. 5.2: (a) Power spectral density of the single-polarization QPSK signal. Highlighted band represents the signal spectral bandwidth defined by the chosen symbol rate. (b) Time representation of the interleaved operation. Higher amplitude periods correspond to classical data transmission.

Finally, at the receiving side, heterodyne detection is performed with a 1.6 GHz-balanced receiver (Thorlabs PDB480AC). The resulting signal is acquired at 2949.12 MSa/s by a ADC (Texas Instruments ADC32RF45) configured for 12 bits resolution and the corresponding offline digital signal processing routine is applied to either retrieve the transmitted symbols or extract RNs. As can be seen in Fig. 5.2b, this setup allows interleaving the classical data transmission with randomness generation by regularly removing the QPSK tributary signal, which reduces the implementation to a homodyne detection scheme with the vacuum-state as the input. Unfortunately, in reality, the impinging signal will never be completely removed due to the finite extinction ratio of the amplitude modulator, and the vacuum state can be compromised. To mitigate this problem, an amplitude modulator with a high extinction ratio was purposefully chosen. With the chosen pulse parameters, roughly 0.714 ms of QPSK communication are obtained for every period, which is enough to transmit a pre-chosen periodic sequence of 65 536 bits. These constraints are necessary since the message is not synchronized with this transmission window. Obviously, a realistic communication system will rarely obey these characteristics, and no fixed transmission period will be able to guarantee the detection of all symbols transmitted. Consequently, although not here considered, a synchronization mechanism between the two operation modes and the data transmission is expected for supporting a practical application.

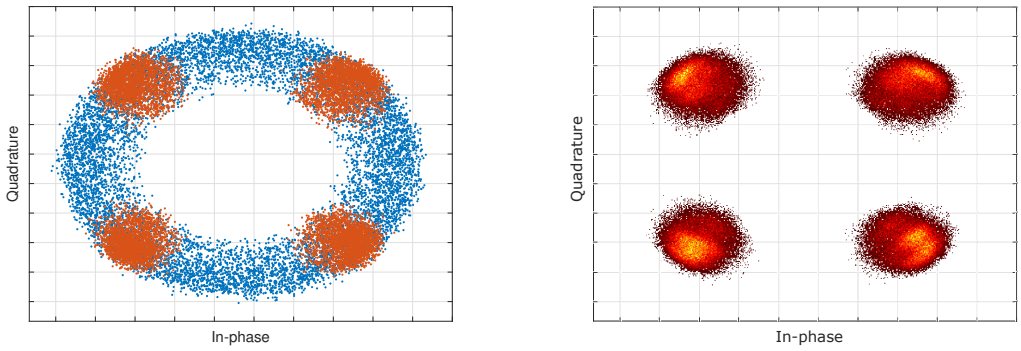
5.1.1 QPSK Transmission

In an effort to assess the viability of the two operation modes, we start by retrieving the classical data transmission. At the detector side, the measured signal is down-converted such that

$x(t) = y(t)e^{(-i2\pi f_Q t_2)}$, t_2 being the arbitrary time at the receiver. Here, to correctly retrieve the sequence, the frequency shift of ± 35 MHz induced by the acousto-optic modulator in the QPSK signal needs to be considered. This originates two distinct spectral lobes centered, respectively, at 92.16 ± 35 MHz. Here, the higher frequency was chosen to retrieve the QPSK signal. In a practical application, the LO would typically be performed by a second laser at the receiver, which is not frequency locked with the transmitter laser and thus introduces an additional frequency shift [78]. In this implementation, however, no frequency estimation routine was considered since the LO and the QPSK signal are derived from the same laser, and no frequency offset is introduced. Lastly, phase correction must be applied. The QPSK signal is again subjected to the root-raised-cosine filter, performing matched filtering. As can be seen in Fig. 5.3a there is still an arbitrary phase rotation of the constellation $\phi(t) = 2\pi f_Q(t - t_2)$. At this point, the downconverted signal can be described as $x(t) = \exp\left(i\frac{2k+1}{4}\pi + i\theta(t)\right)$, where $k = 0, .., 3$, and $x^4(t) = \exp\left(i\pi + i4\theta(t)\right)$. Consequently, a blind phase estimation algorithm can be implemented, where the phase difference between the signal and LO is estimated as:

$$\tilde{\theta}(p) = \frac{1}{4}\arg\left[\frac{1}{2L+1}\sum_{l=-L}^{L} x_i^4(p+l)\right], \tag{5.2}$$

with a moving average of $2L + 1$ samples [78]. Here, $L = 10$ was chosen, and the retrieved QPSK constellations, before and after phase correction, are represented in Fig. 5.3a. As can be seen, the constellation before the phase correction is simply a continuous rotation of the compensated one. Finally, the fourfold ambiguity of the constellation is resolved by minimizing the Bit Error Rate (BER) of the known binary sequence. After this digital signal processing, the transmitted binary sequence was recovered in its entirety with a null BER, which is expected since a back-to-back scenario was considered. Nevertheless, a relatively high amplitude noise was observed, which could seriously compromise the QPSK transmission over a fiber-optic link. This originates in the polarization mismatch between the signal and the LO and thus a careful alignment should be made [77]. Alternatively, a polarization diverse coherent receiver can be employed to eliminate the polarization sensitivity. Moreover, an analysis of the BER performance in transmission over a fiber-optic link is necessary and is here left as future work. Nevertheless, the clean QPSK constellation retrieved, seen in Fig. 5.3b, supports the multi-purpose function of the scheme.

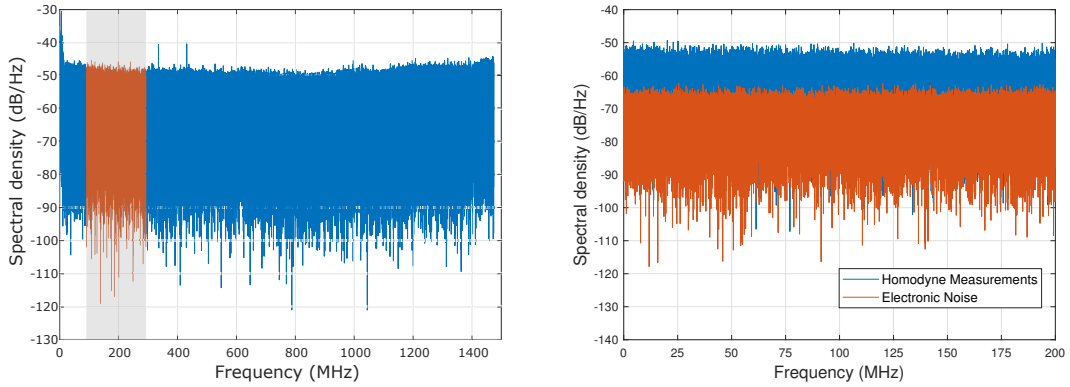


(a) (b)

Fig. 5.3: (a) QPSK constellation before (blue) and after (orange) the blind phase correction for a sequence of 10 k samples. (b) Total received QPSK constellation diagram with 156 224 symbols.

5.1.2 Noise characterization

In Fig. 5.4a, the power spectral density of the homodyne measurements, taken during the QRNG operation window, is displayed. As expected, a relatively flat power density level is attained, although strong spectral contributions can be observed at low frequencies as a consequence

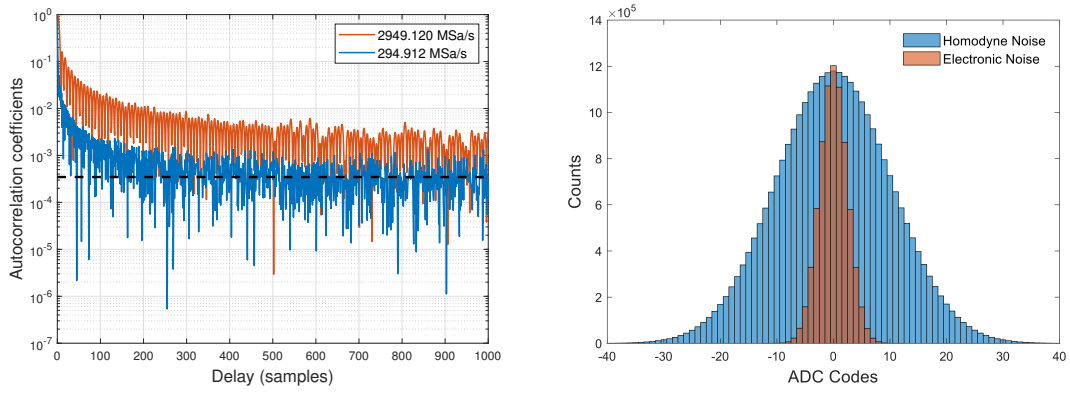


(a) (b)

Fig. 5.4: (a) Power spectral density taken during the QRNG operation. Highlighted 200 MHz frequency band is selected to perform randomness extraction. b) Spectral density after band selection for the homodyne measurements (blue) and the electronic noise (orange).

---

of flicker noise and the finite common-mode rejection ratio of the detector. To remove these contributions, a 200 MHz spectral band free of strong contributions and with high noise clearance, centered around 192.16 MHz, was digitally selected by a rectangular bandpass filter. As can be seen in Fig. 5.4b, the same process was applied to the detector's electronic noise measurements, and the quantum noise clearance was found to be above 10 dB, confirming a preponderance of quantum fluctuations. Although randomness extraction was here performed over a single spectral side-band, this technique can be expanded to extract RNs from multiple non-overlapping channels to increase the generation rate [42].



(a) (b)

Fig. 5.5: (a) Correlation coefficients over 8.3 M noise samples at 2949.12 MSa/s, and after downsampling by a factor of 10. (b) Noise distribution of 7.9 M homodyne measurements and 1.9 M electronic noise samples. Each ADC code represents 0.33 mV.

The previous spectral selection limits the signal to a frequency band of 200 MHz, and thus a maximum sampling rate of 400 MHz is expected to avoid randomness overlapping, as given by the Nyquist sampling theorem. Consequently, the signal was downsampled by a factor of 10, obtaining an effective sampling rate of 294.912 MSa/s. The necessity of downsampling the signal becomes clear in Fig. 5.5a, where clear correlations emerge for the higher sampling rate. By contrast, the analysis of the downsampled signal shows a clear convergence to the theoretically expected result of 3.4683×10^{-4} . Although the bandpass filter imposes some high coefficients at low delays, one sample guarantees coefficient values inferior to 1×10^{-1}. Furthermore, a histogram with 7.5 M

measurements and 1.9 M samples of electronic noise was plotted to confirm that the noise follows the expected Gaussian distribution. These results are shown in Fig. 5.5b, where a QCNR of 12 dB was obtained. Means of approximately 0.0035 mV and −0.0011 mV were calculated for the homodyne and electronic noise samples, respectively, which are sufficiently low to be taken as indicators of a balanced homodyne detection.

5.1.3 Statistical Validation

With the characterization performed in section 5.1.2, the randomness extraction algorithm described in chapter 3 was applied offline to approximately 27.7 M samples to extract true random numbers. Here, the worst-case conditional min-entropy model was considered, and the SHA-512 cryptographic hash function was chosen as the randomness extractor due to its simplicity and relatively high postprocessing speed. Considering the ADC resolution of 12 bits and a sampling range of 1.65 V, the min-entropy yields 4.58 bits per sample, and a total of 126.8 M uniformly distributed bits were extracted. Under these circumstances, a theoretical maximum generation rate of 1.3 Gbps can be observed, which yields approximately 928.2 Mbits in each QRNG operation cycle. Moreover, the QRNG performance still has plenty of opportunities for further improvement by extending the bandwidth of the detector available for randomness generation. Unfortunately, the randomness extraction limits the effective throughput to 1.68 Mbps and constitutes the main limitation of this implementation. Further efforts should be taken to improve the extraction rate, for example, by replacing the SHA-512 hashing with the length-compatible Toeplitz randomness extractor described in chapter 3. This would allow an immediate improvement of up to 50 Mbps. Finally, to evaluate the quality of the extracted RNs, a basic statistical validation was applied. Here, given the constraint on the effective generation rate, only the NIST statistical test suite was used. As can be seen in Table. 5.1, the raw data fails almost all statistical tests due to its Gaussian distribution and the presence of classical contributions. Meanwhile, the postprocessed variant passes all evaluations, which confirms the necessity of the randomness extraction algorithm and is a good indicator of quality for the implemented generator. This simple validation rules out the presence of the most easily identifiable patterns and indicates that the QRNG can cautiously be used as a source of high-quality entropy. Nevertheless, a more stringent statistical validation is necessary, with the application of other randomness test suites and a larger sampling pool, to rule out any failure of the ES. This is especially important given the lack of proof for the purity of the vacuum state, which can be compromised due to contamination from the QPSK signal. If the vacuum state cannot be trusted, a double homodyne measurement scheme can be employed to retrieve both quadratures and arrive at a source-independent implementation [53].

Table 5.1: Results of the NIST statistical test suite, with $\alpha = 0.01$ for a sequence of 1 268 689 bits. The minimum proportion to pass is 96/100, except for the *random excursions* tests where 60/63 is accepted. When multiple *p-values* exist, the smaller proportion is shown.

	Raw Data	Postprocessed variant		
Statistical Test	Result	P-value	Proportion	Result
Frequency	FAILED	0.249284	100/100	PASSED
BlockFrequency	FAILED	0.867692	99/100	PASSED
CumulativeSums	FAILED	0.514124	100/100	PASSED
Runs	FAILED	0.574903	100/100	PASSED
LongestRun	FAILED	0.122325	100/100	PASSED
Rank	PASSED	0.759756	100/100	PASSED
FFT	FAILED	0.213309	97/100	PASSED
NonOverlappingTemplate	FAILED	0.162606	96/100	PASSED
OverlappingTemplate	FAILED	0.334538	100/100	PASSED
Universal	FAILED	0.514124	100/100	PASSED
Approximate entropy	FAILED	0.319084	98/100	PASSED
Random excursions	FAILED	0.392456	62/63	PASSED
Random-excursions variant	PASSED	0.723129	61/63	PASSED
Serial	FAILED	0.153763	99/100	PASSED
LinearComplexity	PASSED	0.739918	99/100	PASSED

Chapter 6

Conclusion

In this work, a real-time QRNG framework based on probing the quadrature amplitude fluctuations of a vacuum state was analyzed and experimentally demonstrated under a laboratory setting. A focus on achieving a secure high-speed implementation that can pass the standard testing tools using only relatively low-cost components, and that provides a comprehensive randomness proof was made. Furthermore, efforts were taken to assess the viability of integrating this randomness source within a classical communication channel to further reduce the cost of the implementation.

With this objective, a brief introduction of the quantum optics and information theory principles that support the generation framework was provided, describing the expected quadrature behavior for the vacuum state of the electromagnetic field. Posteriorly, the different stages of the vacuum-based QRNG framework were described. Here, a variance model for the output noise of the physical layer was developed considering the quantization noise imposed by the ADC. Moreover, a comparative analysis of the two main entropy estimation methods employed in the literature was made, highlighting their theoretical limits. The conditional min-entropy was shown to greatly improve the extraction ratio by accounting for the entire resolution of the ADC. A description of the two considered randomness extractors was also presented, and their performance was compared. The length-compatible Toeplitz-hashing algorithm showed the potential to process 143.29 M raw bits per second and was thus preferred for the final implementation.

As mentioned, two distinct generation schemes were considered. For the dedicated implementation, results of the variance characterization curve of the homodyne detector employed are presented, which confirm the desired linear dependence with the LO optical power. This identifies the operation region where quantum contributions are preponderant and allows to select the operating power for the LO. After assuring a reliable measurement system, a careful characterization of the output noise reveals that it closely follows the expected behavior, with no strong spectral contributions present, and guarantees its stability over a 24-hour time window. Nonetheless, an autocorrelation analysis reveals the low-order correlations induced by the non-ideal response of the TIA. Furthermore, the performance of the entropy estimation methods was evaluated, and a method to quantify the excess entropy contribution introduced by an unbalanced detection was proposed for the Shannon entropy model. Nevertheless, this contribution was considered negligible in the homodyne scheme implemented. For the chosen conditions, a clear preponderance of quantum noise was obtained, and the generation scheme was shown to support output rates up to 8.23 Gbps with a security parameter of 2^{-105}. Unfortunately, the effective generation rate is still severely restricted by the extraction algorithm, being its main limitation.

Rigorous validation of the dedicated scheme was posteriorly applied. The final setup passed all evaluations of the NIST, Dieharder, and TestU01 SmallCrush randomness test suites. However, two inconclusive failures in the Crush battery were obtained, which could originate from the use of the Mersenne Twister PRNG to seed the Toeplitz matrices. Consequently, an alternative randomness source should be considered, and further validation is required. Despite this, the extracted RNs pass a proportion of 98.6% of the considered tests, which highlights the viability of the generation scheme. Further work is necessary to confidently identify the cause of these results

and accordingly adjust the implementation design.

Finally, a time-interleaved QRNG within a classical communication channel was proposed and validated. By imposing on-off keying modulation on the transmission channel, the input signal is removed and a balanced homodyne detection is obtained. Here, if not limited by the extraction algorithm, a maximum output rate of 1.3 Gbps can be achieved. In a realistic application, a method to synchronize the two operation modes with the transmitted data should be explored. Meanwhile, the finite extinction rate of the amplitude modulator can lead to contamination of the vacuum state, which opens security loopholes, and thus further security analysis is required. Alternatively, measuring both quadratures could be explored to derive a source-independent scheme. Nonetheless, the RNs pass the standard NIST randomness test suite, which clearly supports the proposed framework, although stringiest validation tests should also be applied to identify any statistical deviations.

In conclusion, we fulfilled all the proposed objectives. Future work should focus on removing the computational constraints imposed by the randomness extraction algorithm, for example, by employing Field-programmable Gate Arrays (FPGAs). Moreover, the available generations rates can further be increased by optimizing the ADC range used. Since this is not possible with the chosen board, increasing the TIA gain could be explored. In its current form, the physical layer of the dedicated implementation presents an upper bound of extractable min-entropy of approximately 14 bits. Generation rates can further be improved by increasing the LO power, or the ADC sampling rate. However, besides improving the output rate, further security considerations can be included, for example, by exploring a source-independent implementation employing double homodyne detection. This would increase the resilience of the generator against external perturbations. Within this objective, the behavior of the implementation under an attack by a malicious adversary should also be explored. Finally, replacing the bulkier lab setup with a compact self-contained solution would be a fundamental step to increase competitiveness with software implementations.

Bibliography

[1] Pierre Simon LaPlace. *Essai philosophique sur les probabilités*. Courcier, 1814.

[2] George Markowsky. The sad history of random bits. *Journal of Cyber Security and Mobility*, 3:1–24, Jan 2014.

[3] Marco Piani, Michele Mosca, and Brian Neill. Quantum Random-Number Generators: Practical Considerations and Use Cases. Technical Report January, EvolutionQ, 2021. Availbable online: `https://evolutionq.com/quantum-safe-publications/qrng-report-2021-evolutionQ.pdf`.

[4] Donald E. Knuth. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*. Addison-Wesley, 3 edition, 1998.

[5] A.N. Kolmogorov. On tables of random numbers. *Theoretical Computer Science*, 207(2):387–395, 1998.

[6] Andrew Rukhin, Juan Soto, James Nechvatal, et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. *NIST special publication 800-22, National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA*, 2010.

[7] Pierre L'Écuyer and Richard Simard. A Software Library in ANSI C for Empirical Testing of Random Number Generators, 2013. Available at `http://simul.iro.umontreal.ca/testu01/guideshorttestu01.pdf` (accessed on 1 September 2020).

[8] David Bauer Robert G. Brown, Dirk Eddelbuettel. Dieharder: A Random Number Test Suite, 2020. (Duke University Physics Department, 2021).

[9] Antonio Acín and Lluis Masanes. Certified randomness in quantum physics. *Nature*, 540(7632):213–219, Dec 2016.

[10] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. Quantum random number generators. *Rev. Mod. Phys.*, 89:015004, Feb 2017.

[11] Marcin M. Jacak, Piotr Jóźwiak, Jakub Niemczuk, and Janusz E. Jacak. Quantum generators of random numbers. *Scientific Reports*, 11(1):1–21, 2021.

[12] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, et al. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, Apr 2014.

[13] R. Gennaro. Randomness in cryptography. *IEEE Security Privacy*, 4(2):64–67, 2006.

[14] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978.

[15] Christian Kollmitzer, Stefan Schauer, Stefan Rass, and Benjamin Rainer, editors. *Quantum Random Number Generation Theory and Practice: Theory and Practice*. Springer International Publishing, Cham, 2020.

[16] Jan Bouda, Matej Pivoluska, Martin Plesch, and Colin Wilmott. Weak randomness seriously limits the security of quantum key distribution. *Phys. Rev. A*, 86:062308, Dec 2012.

[17] Mariano Lemus, Mariana F. Ramos, Preeti Yadav, et al. Generation and distribution of quantum oblivious keys for secure multiparty computation. *Applied Sciences*, 10(12), 2020.

[18] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. Cryptanalytic attacks on pseudorandom number generators. In Serge Vaudenay, editor, *Fast Software Encryption*, pages 168–188, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg.

[19] A. K. Lenstra, James P. Hughes, Maxime Augier, et al. Ron was wrong, whit is right. *IACR Cryptol. ePrint Arch.*, 2012:64, 2012.

[20] Davide G. Marangon, Giuseppe Vallone, and Paolo Villoresi. Random bits, true and unbiased, from atmospheric turbulence. *Scientific Reports*, 4(1):5490, Jun 2014.

[21] Lishuang Gong, Jianguo Zhang, Haifang Liu, et al. True random number generators using electrical noise. *IEEE Access*, 7:125796–125805, 2019.

[22] Jen-Chieh Hsueh and Vanessa H.-C. Chen. An ultra-low voltage chaos-based true random number generator for iot applications. *Microelectronics Journal*, 87:55–64, 2019.

[23] Berk Sunar, William J. Martin, and Douglas R. Stinson. A provably secure true random number generator with built-in tolerance to active attacks. *IEEE Transactions on Computers*, 56(1):109–119, 2007.

[24] Greg Taylor and George Cox. Digital randomness. *IEEE Spectrum*, 48(9):32–58, 2011.

[25] Mathilde Soucarros, Cécile Canovas-Dumas, Jessy Clédière, et al. Influence of the temperature on true random number generators. In *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*, pages 24–27, 2011.

[26] A. Theodore Markettos and Simon W. Moore. The frequency injection attack on ring-oscillator-based true random number generators. In Christophe Clavier and Kris Gaj, editors, *Cryptographic Hardware and Embedded Systems - CHES 2009*, pages 317–331, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[27] Pierre Bayon, Lilian Bossuet, Alain Aubert, et al. Contactless electromagnetic active attack on ring oscillator based true random number generator. In Werner Schindler and Sorin A. Huss, editors, *Constructive Side-Channel Analysis and Secure Design*, pages 151–166, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[28] S. Pirandola, U. L. Andersen, L. Banchi, et al. Advances in quantum cryptography. *Adv. Opt. Photon.*, 12(4):1012–1236, Dec 2020.

[29] Xiongfeng Ma, Feihu Xu, He Xu, et al. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Phys. Rev. A*, 87:062327, Jun 2013.

[30] Michael Gude. Concept for a high performance random number generator based on physical random phenomena. *Frequenz*, 39(7-8):187–190, 1985.

[31] Anthony Martin, Bruno Sanguinetti, Charles Ci Wen Lim, et al. Quantum random number generation for 1.25-GHz quantum key distribution systems. *Journal of Lightwave Technology*, 33(13):2855–2859, 2015.

[32] Lac Nguyen, Patrick Rehain, Yong Meng Sua, and Yu-Ping Huang. Programmable quantum random number generator without postprocessing. *Opt. Lett.*, 43(4):631–634, Feb 2018.

[33] Mathew R. Coleman, Kaylin G. Ingalls, John T. Kavulich, et al. Parity-based, bias-free optical quantum random number generation with min-entropy estimation. *J. Opt. Soc. Am. B*, 37(7):2088–2094, Jul 2020.

[34] M. Fiorentino, C. Santori, S. M. Spillane, et al. Secure self-calibrating quantum random-bit generator. *Phys. Rev. A*, 75:032334, Mar 2007.

[35] Philip J. Bustard, Duncan G. England, Josh Nunn, et al. Quantum random bit generation using energy fluctuations in stimulated Raman scattering. *Opt. Express*, 21(24):29350–29357, Dec 2013.

[36] Feihu Xu, Bing Qi, Xiongfeng Ma, et al. Ultrafast quantum random number generation based on quantum phase fluctuations. *Opt. Express*, 20(11):12366–12377, May 2012.

[37] You-Qi Nie, Leilei Huang, Yang Liu, et al. The generation of 68 Gbps quantum random number by measuring laser phase fluctuations. *Review of Scientific Instruments*, 86(6):063105, 2015.

[38] Xiongfeng Ma, Xiao Yuan, Zhu Cao, et al. Quantum random number generation. *npj Quantum Information*, 2(1):1–9, 2016.

[39] Xiao-Guang Zhang, You-Qi Nie, Hongyi Zhou, et al. Note: Fully integrated 3.2 Gbps quantum random number generator with real-time extraction. *Review of Scientific Instruments*, 87(7):076102, 2016.

[40] Leilei Huang and Hongyi Zhou. Integrated Gbps quantum random number generator with real-time extraction based on homodyne detection. *J. Opt. Soc. Am. B*, 36(3):B130–B136, Mar 2019.

[41] Ziyong Zheng, Yichen Zhang, Weinan Huang, et al. 6 Gbps real-time optical quantum random number generator based on vacuum fluctuation. *Review of Scientific Instruments*, 90(4):043105, 2019.

[42] Xiaomin Guo, Chen Cheng, Mingchuan Wu, et al. Parallel real-time quantum random number generator. *Opt. Lett.*, 44(22):5566–5569, Nov 2019.

[43] Tobias Gehring, Cosmo Lupo, Arne Kordts, et al. Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information. *Nature Communications*, 12, 01 2021.

[44] Dinka Milovančev, Nemanja Vokić, Christoph Pacher, et al. Towards integrating true random number generation in coherent optical transceivers. *IEEE Journal of Selected Topics in Quantum Electronics*, 26(5):1–8, 2020.

[45] Christian Gabriel, Christoffer Wittmann, Denis Sych, et al. A generator for unique quantum random numbers based on vacuum states. *Nature Photonics*, 4(10):711–715, 2010.

[46] T. Symul, S. M. Assad, and P. K. Lam. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Applied Physics Letters*, 98(23):231103, 2011.

[47] Meltem Sönmez Turan, Elaine Barker, John Kelsey, et al. Recommendation for the Entropy Sources Used for Random Bit Generation. *NIST special publication 800-90B, National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA*, 2018.

[48] J. Y. Haw, S. M. Assad, A. M. Lance, et al. Maximization of extractable randomness in a quantum random-number generator. *Phys. Rev. Applied*, 3:054004, May 2015.

[49] Zhenguo Lu, Jianqiang Liu, Xuyang Wang, et al. Quantum random number generator with discarding-boundary-bin measurement and multi-interval sampling. *Optics Express*, 29, 03 2021.

[50] Weinan Huang, Yichen Zhang, Ziyong Zheng, et al. Practical security analysis of a continuous-variable quantum random-number generator with a noisy local oscillator. *Phys. Rev. A*, 102:012422, Jul 2020.

[51] Leilei Huang, Hongyi Zhou, Kai Feng, and Chongjin Xie. Quantum random number cloud platform. *npj Quantum Information*, 7(1):1–7, 2021.

[52] Bing Bai, Jianyao Huang, Guan-Ru Qiao, et al. 18.8 Gbps real-time quantum random number generator with a photonic integrated chip. *Applied Physics Letters*, 118(26):264001, 2021.

[53] Marco Avesani, Davide G. Marangon, Giuseppe Vallone, and Paolo Villoresi. Source-device-independent heterodyne-based quantum random number generator at 17 Gbps. *Nature Communications*, 9(1):1–7, 2018.

[54] David Drahi, Nathan Walk, Matty J. Hoban, et al. Certified quantum random numbers from untrusted light. *Phys. Rev. X*, 10:041048, Dec 2020.

[55] P.R. Smith, D.G. Marangon, M. Lucamarini, et al. Out-of-band electromagnetic injection attack on a quantum random number generator. *Phys. Rev. Applied*, 15:044044, Apr 2021.

[56] Ferreira, Maurício J. and Silva, Nuno A. and Pinto, Armando N. and Muga, Nelson J. Homodyne noise characterization in quantum random number generators. In *2021 Telecoms Conference (ConfTELE)*, pages 1–6, Leiria, Portugal, 2021.

[57] Ferreira, Maurício J. and Silva, Nuno A. and Pinto, Armando N. and Muga, Nelson J. Characterization of a quantum random number generator based on vacuum fluctuations. *Applied Sciences*, 11(16), 2021.

[58] Maurício Ferreira and Daniel Pereira and Nelson Muga and Nuno Silva and Armando Pinto. Time-interleaved quantum random number generation within a coherent classical communication channel. In *Anais do I Workshop de Comunicação e Computação Quântica*, pages 37–42, Porto Alegre, RS, Brasil, 2021. SBC.

[59] Rodney Loudon. *The Quantum Theory of Light*. Oxford University Press, 3 edition, 2000.

[60] S. Haroch. Course 2 - mesoscopic state superpositions and decoherence in quantum optics. In Daniel Estève, Jean-Michel Raimond, and Jean Dalibard, editors, *Quantum Entanglement and Information Processing*, volume 79 of *Les Houches*, pages 55–159. Elsevier, 2004.
[61] Eugene Merzbacher. *Quantum Mechanics*. Wiley, 3 edition, 1998.
[62] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, USA, 2006.
[63] National Institute of Standards and Technology (NIST). Secure Hash Standard (SHS) (FIPS PUB 180-4). *Federal Information Processing Standards Publication*, 180-4(August):36, 2015.
[64] Margarida Almeida, Daniel Pereira, M. Facão, et al. Impact of imperfect homodyne detection on measurements of vacuum states shot noise. *Optical and Quantum Electronics*, 52, 11 2020.
[65] Stefano Bottacchi. *Noise and Signal Interference in Optical Fiber Transmission Systems*. John Wiley & Sons, Ltd, 2008.
[66] Govind P. Agrawal. *Lightwave Technology: Telecommunication Systems*. John Wiley & Sons, Ltd, 2005.
[67] W. R. Bennett. Spectra of quantized signals. *The Bell System Technical Journal*, 27(3):446–472, 1948.
[68] Salil P. Vadhan. Pseudorandomness. *Foundations and Trends in Theoretical Computer Science*, 7(1–3):1–336, 2012.
[69] Ç.K. Koç. *Open Problems in Mathematics and Computational Science*. Springer International Publishing, 2015.
[70] Jan (2019). DataHash (`https://www.mathworks.com/matlabcentral/fileexchange/31272-datahash`), MATLAB Central File Exchange. Retrieved September 1, 2020.
[71] Xiangyu Wang, Yichen Zhang, Song Yu, and Hong Guo. High-speed implementation of length-compatible privacy amplification in continuous-variable quantum key distribution. *IEEE Photonics Journal*, PP:1–1, 04 2018.
[72] Masahito Hayashi and Toyohiro Tsurumaru. More efficient privacy amplification with less random seeds via dual universal hash function. *IEEE Transactions on Information Theory*, 62(4):2213–2232, 2016.
[73] Texas Instruments Incorporated. *ADS54J60 Dual-Channel, 16-Bit, 1.0-GSPS Analog-to-Digital Converter*, April 2019. Rev. D.
[74] G. E. P. Box and David A. Pierce. Distribution of residual autocorrelations in autoregressive-integrated moving average time series models. *Journal of the American Statistical Association*, 65(332):1509–1526, 1970.
[75] Yong Shen, Liang Tian, and Hongxin Zou. Practical quantum random number generator based on measuring the shot noise of vacuum states. *Phys. Rev. A*, 81:063814, Jun 2010.
[76] Pierre L'Ecuyer and Richard Simard. Testu01: A C library for empirical testing of random number generators. *ACM Trans. Math. Softw.*, 33(4), August 2007.
[77] Sebastian Kleis, Max Rueckmann, and Christian G. Schaeffer. Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals. *Opt. Lett.*, 42(8):1588–1591, Apr 2017.
[78] M. S. Faruk and S. J. Savory. Digital signal processing for coherent transceivers employing multilevel formats. *Journal of Lightwave Technology*, 35(5):1125–1141, 2017.