Characterization of a Quantum Random Number Generator Based on Vacuum Fluctuations

Maurício J. Ferreira 1,2,*, Nuno A. Silva 2, Armando N. Pinto 2,3 and Nelson J. Muga 2

1 Department of Physics, University of Aveiro, 3810-193 Aveiro, Portugal
2 Instituto de Telecomunicações, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal; nasilva@ua.pt (N.A.S.); anp@ua.pt (A.N.P.); muga@ua.pt (N.J.M.)
3 Department of Electronics, Telecommunications and Informatics, University of Aveiro, 3810-193 Aveiro, Portugal
* Correspondence: mauricioferreira@ua.pt

Abstract: Quantum random number generators (QRNGs) are currently in high demand across a large number of cryptographic applications as secure sources of true randomness. In this work, we characterize the conditions from which randomness can be extracted in a QRNG based on homodyne measurements of vacuum fluctuations by assessing the impact of experimental limitations, such as the digitizer resolution or the presence of excess local oscillator (LO) noise due to an unbalanced detection. Moreover, we propose an estimation method to quantify the excess entropy contribution introduced by an unbalanced detection and analyze the implementation of the post-processing algorithm. Finally, we submitted the generated numbers to a set of statistical tests to assess the quality of its output randomness and verified that it passes the standard libraries.

Keywords: random number generation; homodyne detection; vacuum fluctuations; shot noise; randomness extraction

1. Introduction

Reliable random numbers (RNs) fulfil an essential role in multiple applications, such as gambling, computer simulations, statistical analysis, or cryptography [1,2]. Traditionally, pseudo-random number generators (PRNGs) have been able to suppress this demand through fast, and easily implemented deterministic algorithms. Unfortunately, their output is only dependent on an initial seed and the algorithm itself, and, therefore, becomes predictable to an adversary with enough computational resources, as an inherent periodicity can be found [2,3]. As a result, their implementation is not suitable for critical applications, such as quantum key distribution (QKD), where true unpredictability is required [4,5]. In answer to these shortcomings, hardware-based implementations have been developed. These extract randomness from measurements of some apparently unpredictable physical process, such as atmospheric or electrical noise [6,7]. However, such devices are generally slow and difficult to implement as the yielded entropy is hard to quantify due to their susceptibility to practical imperfections or external manipulation by a malicious adversary, which can compromise the quality of their output [8]. Additionally, it is hard to give a convincing argument for the randomness yielded by some of these devices, as many implementations simply rely on ignorance about the entropy source rather than intrinsic randomness. If the physical process measured is deterministic, such as the case of classical phenomena or a chaotic system, the final result is nonetheless still fundamentally predictable, and reasonable doubts about the randomness of the output can be posed [1].

In contrast to PRNGs, QRNGs explore the intrinsic probabilist nature of quantum phenomena as their source of randomness. Several implementations have been proposed, including generation schemes based on detection of radioactive decays [9,10], but most schemes explore the properties of quantum optics through protocols, such as measurements of photon polarization states [11], amplified spontaneous emission [12–14], photon...
arrival times [15–18], or phase noise from selected light sources [19,20]. Recently, some fully integrated solutions have also materialized by employing photonic integrated circuits, which removes the need for bulky implementations [21–26]. This is an important first step to reach mass deployment and allow these implementations to compete with the versatility shown by PRNGs. Unfortunately, further work is necessary to integrate all components into a single compact package, as customized designs and expensive electronic components are frequently the required trade-off. Furthermore, achieving a high-performance integrated randomness platform is technically challenging, as considerations, such as the presence of dark currents, or the responsivity and the bandwidth of the photodetectors significantly impact the generation rates achievable [25]. Perhaps one of the most promising and well-researched implementations employs homodyne measurements of the fluctuations of a vacuum-state as its entropy source, with several recent high-rate generation schemes being proposed [26–31]. This approach offers high generation rates using a simpler setup than heterodyne-based QRNGs, can potentially be implemented with widely available technologies and shows high potential for on-chip integration due to the low number of components required. Furthermore, the vacuum state is easily obtained and can not be reproduced by an attacker, which provides resilience against external perturbations [27]. Despite this, several challenges are still present, such as assuring a good balancing condition or a significant quantum noise level, which can lead to the introduction of security loopholes [32].

In this work, we propose a method to quantify the excess entropy contribution resultant from an unbalanced homodyne detection in a vacuum-based generation scheme and obtain an estimation of at least 0.0554 bit for the considered balancing condition. Moreover, we analyze the impact of practical limitations on the performance of the implementation. Under these conditions, the implementation shows the potential to deliver a rate of 19.53 Mbit/s. By treating all classical noise as knowable to an eavesdropper, we obtain unbiased true random numbers that pass a 98.1% proportion of the applied state-of-the-art statistical evaluations.

This paper is organized into 5 sections. In Section 2 we present a theoretical description of the vacuum-based QRNG. Posteriorly, in Section 3, we describe the experimental implementation. In Section 4 we analyze the impact of practical imperfections and propose our entropy estimation method. Moreover, we apply a set of statistical tests to assess the quality of the implementation. Finally, in Section 5, a brief conclusion is presented.

2. Theoretical Description

In Figure 1, a schematic model of a homodyne detection scheme is illustrated. Here, the local oscillator, represented by the destruction operator $\hat{a}_{LO}(t)$, is directed towards a lossless beamsplitter (BS), where one of the input ports is kept blocked so that only the vacuum state, $\hat{v}_s(t)$, is present at the second input port.
Considering a certain complex reflection coefficient, $\mathcal{R}$, we can define the BS imbalance, $\Delta$, as $|\mathcal{R}|^2 = (\frac{1}{2} + \Delta)$ [33]. Under these assumptions, the output signals, $\hat{d}_{3,4}(t)$, can be described as given by the input–output relations for a lossless BS [34]:

$$
\hat{d}_3(t) = i\sqrt{\frac{1}{2} + \Delta} \hat{a}_{\text{LO}}(t) + i\sqrt{\frac{1}{2} - \Delta} \hat{a}_s(t) \\
\hat{d}_4(t) = \sqrt{\frac{1}{2} - \Delta} \hat{a}_{\text{LO}}(t) + i\sqrt{\frac{1}{2} + \Delta} \hat{a}_s(t).
$$

(1)

Subsequently, the output signals are attenuated by two VOAs, modeled as two lossless BS, and detected by two photodiodes. Here, the VOAs are introduced to allow for balancing of the HD, since neither the BS nor the photodetectors are ideal in a realistic application. In this framework, the efficiency of the photodetectors is modeled by imposing a virtual BS before a theoretical perfect photodetector. As illustrated, one of the output signals of the virtual BS will be lost while the other, $\hat{d}_{3,4}(t)$, is directly received by the detector. Here, $\hat{d}_{3,4}(t)$ and $\hat{d}_{\text{VOA3,VOA4}}(t)$ denote, respectively, the vacuum states of the VOA$_{3,4}$ and the respective photodiodes. Analogously to Equation (1):

$$
\hat{d}_3(t) = i\sqrt{\frac{1}{2} + \Delta} \eta_3 \hat{a}_{\text{LO}}(t) + i\sqrt{\frac{1}{2} - \Delta} \eta_3 \hat{a}_s(t) \\
+ i\sqrt{\eta_3(1 - \eta_{\text{VOA3}})} \hat{d}_{\text{VOA3}}(t) + i\sqrt{1 - \eta_3} \hat{d}_3(t) \\
\hat{d}_4(t) = i\sqrt{\frac{1}{2} - \Delta} \eta_4 \hat{a}_{\text{LO}}(t) + i\sqrt{\frac{1}{2} + \Delta} \eta_4 \hat{a}_s(t) \\
+ i\sqrt{\eta_4(1 - \eta_{\text{VOA4}})} \hat{d}_{\text{VOA4}}(t) + i\sqrt{1 - \eta_4} \hat{d}_4(t),
$$

(2)

where $\eta_{3,4}$ denote the quantum efficiency of each photodetector, and $\eta_{\text{VOA3,VOA4}}$ express the transmissivities of each VOA [33].

The photocurrents yielded in each photodetector, $\hat{i}_{3,4}(t)$, are posteriorly subtracted and amplified by a transimpedance amplifier (TIA). Thus, in an ideally balanced scenario, any fluctuations common to both detectors are cancelled and only fluctuations in photon arrivals are measured, the so-called shot noise [33,35]. In reality, the presence of excess noise is unavoidable, and the output signal will always contain at least electronic noise. The resultant output voltage, $\hat{V}_H(t)$, is given by the convolution, $\otimes$, between the difference current, $\hat{i}_H$, and the detector’s impulse response function, $h(t)$:

$$
\begin{bmatrix}
\hat{V}_H(t) = G_{\text{TIA}} [\hat{i}_e(t) + \hat{i}_H(t)] \otimes h(t) \\
\hat{i}_H(t) = q [\hat{d}_3^*(t)\hat{d}_3(t) - \hat{d}_4^*(t)\hat{d}_4(t)]
\end{bmatrix},
$$

(3)

where $\hat{i}_e$ is the amplifier electronic noise, $G_{\text{TIA}}$ is the transimpedance amplifier gain, $q$ is the charge of the electron, and $\hat{d}_{3,4}^*(t)\hat{d}_{3,4}(t)$ corresponds to the photon flux of each output beam. Here, the normalized impulse response function, $h(t)$, should consider both the impact of finite bandwidth of the photodetectors and the TIA’s time response. Nonetheless, this function can be mainly characterized by the latter contribution due to the much lower bandwidths typically presented by the amplifier. Consequently, in this analysis, an equal ideal response, $h_p(t)$, was considered for both photodiodes, such that $h_p(t) = \delta(t)$. Under these approximations, the impulse response function can be approximated in the frequency domain by a Butterworth filter:

$$
|H(w)|^2 = \frac{1}{1 + (\frac{w}{2\pi f_0})^{2n}},
$$

(4)
where $n$ is the filter-order, and $\Delta f$ is the detector’s bandwidth [36]. In its turn, the strong coherent laser signal can be described as:

$$\hat{a}_{LO}(t) = \hat{a}(t) \exp(i(\omega_{LO}t + \theta(t))),$$

where $\hat{a}(t)$ is the time-dependent photon flux, $\omega_{LO}$ the frequency and $\theta(t)$ the initial phase of the laser [33]. Here, the time-dependence of the initial phase implies the existence of phase noise. This, however, does not result in an additional noise contribution as long as no phase shift, $\Delta \phi$, is present between the output beams of the beamsplitter. In this analysis, identical optical path lengths are considered for both output arms, such that $\Delta \phi = 0$, and its contribution can be disregarded. Considering a null mean electronic current, identical optical path lengths are considered for both output arms, such that $\Delta \phi = 0$, and its contribution can be disregarded. Considering a null mean electronic current, $\hat{a}(t)$, and $\hat{a}(t) = \sqrt{F + \Delta f_{LO}(t)}$, where $F$ is the time-independent mean photon flux and $\Delta f_{LO}(t)$ denotes the intensity fluctuations, the expected output voltage is given by:

$$\langle \hat{V}_H(t) \rangle = qG_{TIA}\gamma F \otimes h(t),$$

where:

$$\gamma = \left(\frac{1}{2} + \Delta\right)\eta_3\eta_{VOA3} - \left(\frac{1}{2} - \Delta\right)\eta_4\eta_{VOA4}. \quad (7)$$

The voltage variance, $\sigma_H^2(t)$, can be obtained from the autocovariance function, $K(\tau)$, evaluated at $\tau = 0$. For a ergodic stationary stochastic process, and assuming that:

$$\begin{aligned}
\langle \hat{a}_H(t_1)\hat{a}_H(t_2) \rangle &= 2k_B T \delta(t_1 - t_2) \\
\langle \Delta f_{LO}(t_1)\Delta f_{LO}(t_2) \rangle &= RIN^2 \delta(t_1 - t_2),
\end{aligned} \quad (8)$$

where $k_B$ is the Boltzmann constant, $T$ the temperature, $R$ the load resistance of the TIA, and $RIN$ represents the average relative intensity noise (RIN) over the detector’s bandwidth [36], the autocovariance function can be calculated through Equations (3) and (6) as:

$$K(\tau) = \left[2G_{TIA}^2 \frac{k_B T}{R} + q^2G_{TIA}^2\beta F + q^2G_{TIA}^2 RIN \gamma^2 F^2\right] \int_{-\infty}^{+\infty} d\tau' h(t - \tau')h(t - \tau' + \tau),$$

where:

$$\beta = \left(\frac{1}{2} + \Delta\right)\eta_3\eta_{VOA3} + \left(\frac{1}{2} - \Delta\right)\eta_4\eta_{VOA4}. \quad (10)$$

This cross-correlation can be greatly simplified through the Wiener-Khinchin theorem. Abiding by the previous definitions, we obtain the analytical expression:

$$\sigma_H^2(t = 0) = \frac{2\pi}{3}G_{TIA}^2 \Delta f \left[2\frac{k_B T}{R} + q^2\beta F + q^2RIN \gamma^2 F^2\right] + \frac{\delta_q^2}{12}, \quad (11)$$

for a Butterworth’s filter of order $n = 3$, considering $t = \tau = 0$. Here, we considered the quantization error of an analog to digital converter (ADC) with a bin width of $\delta_q$, which yields a quantization error variance of $\frac{\delta_q^2}{12}$ [37].

Finally, it is possible to rewrite the Equations (6) and (11) in function of the wavelength-dependent responsivity, $\mathcal{R}(\lambda)$, and the optical power of the LO, $P_{LO}$. Assuming that $\eta_3 = \eta_4$:

$$\begin{aligned}
\langle \hat{V}_H(t) \rangle &= G_{TIA}\gamma' \\
\sigma_H^2(t = 0) &= \frac{2\pi}{3}G_{TIA}^2 \Delta f \left[2\frac{k_B T}{R} + q\beta' + qRIN \gamma^2 F^2\right] + \frac{\delta_q^2}{12},
\end{aligned} \quad (12)$$

where:

$$\begin{aligned}
\beta' &= \mathcal{R}(\lambda)P_{LO}\left[\left(\frac{1}{2} + \Delta\right)\eta_{VOA3} + \left(\frac{1}{2} - \Delta\right)\eta_{VOA4}\right] \\
\gamma' &= \mathcal{R}(\lambda)P_{LO}\left[\left(\frac{1}{2} + \Delta\right)\eta_{VOA3} - \left(\frac{1}{2} - \Delta\right)\eta_{VOA4}\right].
\end{aligned} \quad (13)$$
As described, this detection scheme yields an outcome defined by four main noise sources. In addition to electronic noise, which is independent of the incident optical power, excess LO noise, quadratically dependent on the impinging power, can appear as a consequence of the inability to completely cancel fluctuations of the local oscillator [35,38]. Particularly, quantum noise, whose variance is proportional to the LO power, is always present [33]. It is from these contributions that randomness can be extracted, as quantum noise measurements are proportional to the quadrature amplitude of the vacuum state, and, thus, obey a Gaussian distribution whose inherent uncertainty is guaranteed by quantum mechanics [39]. Finally, a small additional variance contribution is introduced by the quantization error in the uniform quantizer. The total variance is simply the sum of these contributions, and, thus, a preponderance of quantum noise should be guaranteed to preserve the generator’s output statistical quality.

3. Materials and Methods

A schematic representation of the implemented QRNG is shown in Figure 2. A continuous-wave laser at 1550.92 nm is used as the LO, and an optical bandpass filter (OBF) is applied to suppress its sideband frequencies. Posteriorly, the LO is split by a 90/10 BS (BS1) such that an optical power meter (OPM) in the 10% output arm allows real-time monitoring of the power level without tampering with the setup. The LO is then split by a second BS (BS2) with one of its input ports blocked to assure the purity of the vacuum state. After the BS2, the resulting output beams are detected by a pair of photodiodes on a ThorLabs PDB450C balanced amplified photodetector with an output bandwidth of 45 MHz. A VOA is placed in one of the output arms to allow precise adjustments of the BS2 splitting ratio. To better account for the differences in the responsivity of the photodiodes, the attenuation was set, such that the photocurrents measured were indistinguishable. The subsequent signal is amplified with a TIA and finally digitized by an 8-bit Picoscope 6403D ADC with a ±50 mV acquisition range.

![Figure 2. Schematic representation of the implemented QRNG. A laser is split by a BS with one of its input ports blocked (BS2) and the subsequent photocurrents are subtracted. The resulting signal, \(i_1 - i_2\), is amplified, digitized, and processed to obtain a string of unbiased random bits.](image)

As previously described, the homodyne measurements also contain unwanted noise, such as electronic noise that is intrinsic to the electronic components in the experimental setup. Consequently, the RNs yielded by the QRNG are never truly random but contain simultaneously quantum and classical contributions. A randomness extraction process is thus required to suppress these contributions and attain secure true RNs since all classical noise can, in principle, be known and manipulated by an adversary. Consequently, the raw measurements are at last subjected to a post-processing algorithm that outputs a sequence of uniformly distributed random bits. This process requires obtaining a uniform distribution, quantifying the entropy that originates from quantum phenomena, \(H_{\text{quant}}\), and applying a randomness extractor.

Initially, to obtain a sequence of uniformly distributed bits, a binning process is applied to the Gaussian distribution of homodyne measurements. Here, a bit sequence of length \(n\) is assigned to all outcomes that fall in the same bin and, therefore, \(n\)-bit unbiased RNs
are produced. The sequence length merely depends on the number of bins used, such that $2^n$ bins are required for a sequence of $n$ bits [27,28]. The total entropy, $H_{\text{total}}$, yielded by a bit sequence obtained through the binning process is given by the Shannon entropy, for a uniform distribution $X$:

$$H_{\text{total}}(X) = -\sum_{i=1}^{2^n} p_i \log_2 p_i = \log_2(p_i) = n,$$  \hspace{1cm} (14)

where $p_i$ is the probability of finding a sample on the $i$-th bin [40]. This same process can also be applied to assess the contribution of electronic noise. As such, measurements of these fluctuations are taken by removing the LO and the same binning is superimposed to its distribution. The entropy contribution originating from the electronic noise is given by:

$$H_{\text{elec}} = -\sum_{i=1}^{2^n} p_i^e \log_2 p_i^e,$$  \hspace{1cm} (15)

where $p_i^e$ is the probability of finding an electronic noise measurement in each bin. Although this quantity is relatively constant, periodic evaluations of the noise level can be made to ensure that it does not increase [27,41]. This constitutes the major contribution to the fraction of entropy originating from classical effects, $H_{\text{class}}$. Nonetheless, on a practical generation scheme, an additional component will be introduced by excess LO noise due to an unbalanced detection, $H_{\text{unbal}}$, such that:

$$H_{\text{class}} = H_{\text{elec}} + H_{\text{unbal}}.$$  \hspace{1cm} (16)

Through this method, we can establish the fraction of randomness that is possible to extract from each sample without compromising the generator’s outcome:

$$H_{\text{quant}} = H_{\text{total}} - H_{\text{class}}.$$  \hspace{1cm} (17)

As all entropies calculated depend on the binning applied, it is advantageous to find the binary sequence length $n$ that maximizes the effective bits that can be extracted from each sample. Finally, the measurements are submitted to a randomness extractor, as described in Section 4.3.

4. Results and Discussion

To verify that there is a preponderance of quantum noise over electronic noise, the spectral density power was taken both with and without the LO, considering an input power of 12 dBm, as can be seen in Figure 3.

![Figure 3](image-url)

**Figure 3.** The power spectral density (PSD) when the LO is on (upper lines) and off (lower lines). Inset focus on low-frequency contributions. The introduction of the DC block suppresses the observed low frequency contributions, with no visible difference in the remaining spectral noise.
For both cases, the high-frequency domain is defined by the cut-off frequency from the detector’s bandwidth at 45 MHz. Moreover, strong spectral contributions were observed at low frequencies. These can arise both from electric hum and an imperfect subtraction of the photocurrents since the HD has a finite common-mode rejection ratio of 30 dB. To suppress these frequencies, as well as flicker noise associated with the electrical circuit, an 8535 Inmet RF DC Block was applied after the amplification step. It acts as a high-pass filter, blocking all frequency components inferior to 7 kHz. Consequently, the spectral curve below 40 MHz yields the relatively flat power density required for unbiased random number generation. In fact, no strong spectral peaks are observed for this interval, and the total noise clearance over electronic noise was measured to be at least 5 dBm. This clearly shows the difficulty in obtaining an expressive quantum to classical noise ratio (QCNR), which limits the available quantum entropy.

4.1. Estimation of Entropy Due to Detection Unbalancing

As shown through Equation (12), an increase in the QCNR can be made by minimizing the electronic noise, for example, by controlling the setup temperature or using a detector with a lower noise floor. Unfortunately, such methods increase costs and introduce complexity to the implementation. Alternatively, a simple increase in the laser’s optical power can be made, since the shot noise variance increases linearly with the impinging power. Unfortunately, this is not always possible, as excess noise quadratically dependent on the LO power also appears as a consequence of an unbalanced detection, either due to a BS imbalance, different path losses, or different photodetector’s efficiencies between each path. To experimentally verify the presence of this quadratic power dependency, the detector’s characterization curve was obtained for an unbalanced condition by introducing a VOA before the BS1 and varying the LO optical power, as can be observed in Figure 4. Here, each variance was evaluated over 15.625 \times 10^7 noise samples, and the electronic noise level was assumed to remain constant throughout the experimental process. As expected by the theoretical description, the variance, \( \sigma^2 \), follows a quadratic dependency with the input power at BS2, \( P_{LO} \):

\[
\sigma^2 = aP_{LO}^2 + bP_{LO} + c. \quad (18)
\]

A regression with \( r^2 = 0.9853 \) allows to obtain the coefficients: \( c = 7.652 \times 10^{-7} \text{V}^2 \), \( b = 2.708 \times 10^{-7} \text{V}^2/\text{mW} \), \( a = 3.277 \times 10^{-7} \text{V}^2/\text{mW}^2 \). This clearly highlights the quadratic dependency of the variance with the input power and illustrates the importance of achieving a well-balanced detection. As represented in Figure 4, the electronic noise level is independent of the optical power. Nonetheless, for an unbalanced detection, two distinct regions emerge. For low LO powers, the variance is dominated by these intrinsic electronic noise contributions and its increase can be mainly attributed to shot noise, which grows linearly with \( P_{LO} \). For higher impinging power, however, the excess RIN noise becomes more significant and constitutes the majority of the total noise due to the observed quadratic dependency. As described in Section 2, its impact is dependent on the balancing condition of the detection scheme.

At a given LO power, this manifests itself as an additional entropy contribution, \( H_{\text{unbal}} \), dependent on the scheme unbalancing, that should be correctly quantified to avoid overestimating the available quantum entropy, thus compromising the generator output. With this objective, we assessed the entropy contributions as a function of the homodyne detection unbalance, as represented in Figure 5.
Here, the LO power was fixed at approximately 1.33 dBm to avoid saturating the TIA output signal. Posteriorly, the path attenuation was changed through the employment of a VOA, so that we can iterate over the detection’s asymmetry $\Delta P = \frac{P_1}{P_{\text{total}}}$, defined as the ratio between the optical power measured at the output without the VOA, $P_1$, and the total impinging power, $P_{\text{total}}$. It should be noted that this is theoretically distinct from simply varying the BS transmittance since the total power that reaches the photodetectors decreases with the additional attenuation. The electronic and quantum noise contribution were calculated as described in Section 3 for practical asymmetries of 50.75%, 55.28%, 59.72%, 64.90%, and 68.93%, yielding respective quantum contributions of 0.0836, 0.1085, 0.6793, 1.083, and 1.298 bit from a total entropy of 5 bits. Additionally, a comparison with the theoretically expected values, obtained through Equation (11), is also presented, considering a measured RIN of $-135$ dB/Hz. The measured entropy, as can be seen in Figure 5a, appears to increase with the detection unbalancing. Since the total impinging optical power does not increase, it is trivial to attribute this to excess LO noise, and we conclude that a larger asymmetry increases the impact of the excess LO noise on the measured entropy.
To quantify $H_{\text{unbal}}$, 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 $H_{\text{quant}}$ remains relatively constant, all posterior increases are thus the result of introducing excess LO noise. As seen in Figure 5b, this contribution increases linearly with the asymmetry. By contrast, as a consequence of a higher signal-to-noise ratio, the contribution from the electronic noise decreases in the same proportion that $H_{\text{unbal}}$. We thus find that 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, our assumptions result in an overestimation of $H_{\text{quant}}$, since our measurement scheme is always slightly unbalanced. To obtain an acceptable estimation, we performed a linearisation with $r^2 = 0.9523$ of the $H_{\text{unbal}}$ values, which yields $H_{\text{unbal}} = 0.0741\Delta P$. 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, 66.3% lower than originally measured. Unfortunately, these assumptions hold true only when no additional attenuation is introduced. Here, the decrease in $P_{\text{total}}$ leads to a reduction in the quantum noise contributions with an increasing attenuation, and thus this value should be adjusted accordingly. Nonetheless, the value obtained is an acceptable estimation for asymmetries close to a balanced detection. Although the electronic noise is still the major contribution to a balanced system, this method allows us to increase the QRNG security by discarding these insecure bits.

4.2. Noise Characterization

The electronic components within the homodyne detector induce correlation between samples taken at different instants of time in the digitizer. To ensure uncorrelated measurements and avoid randomness overlapping, a sampling rate of 39.06 MSa/s was chosen. Ideally, a sampling rate inferior to twice the detector’s bandwidth should be used, as described by the Nyquist sampling theorem. In Figure 6, the correlation coefficients were evaluated over $15.6 \times 10^6$ data points for a maximum delay of 100 samples. As can be seen, these rapidly drop to below $1.9 \times 10^{-3}$ at 12 dBm and $6.8 \times 10^{-4}$ for electronic noise samples. Although they never reach zero due to the signal’s finite bandwidth, these low values hint at a negligible correlation between samples, which is essential for any reliable random number generator.

![Figure 6. Correlation coefficients for (a) electronic noise samples and (b) noise samples taken at a LO power of 12 dBm. At the chosen sampling rate, the delay between two consecutive samples is approximately 25.6 ns.](image)

For this implementation, we obtain a QCNR value of approximately 5 dB with an electronic noise variance of $0.67\text{ mV}^2$. Approximately $17 \times 10^9$ noise samples were recorded, as well as periodical evaluations of the electronic noise, and a histogram for $10^7$ samples was plotted to verify that all noise follows the expected Gaussian distribution, as can be
seen in Figure 7. Means of 0.1004 mV and −0.1360 mV were calculated for the homodyne and electronic noise samples, respectively. These values could hint at a slightly unbalanced detection but are low enough to be disregarded. Each represented bin corresponds to a unique ADC value, which shows the concentration of measurements on a small number of bins due to the ADC resolution and acquisition range available.

Figure 7. Distribution of the homodyne measurements and electronic noise for $10^7$ samples taken at 12 dBm. Here, each bin corresponds to a unique ADC value.

Here, the ADC resolution and acquisition range also present another 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 [43]. Thus we misrepresent the Gaussian distribution and necessarily limit the randomness that can be extracted. The necessity to lower the extraction ratio in this situation is made obvious 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. This can partially be compensated by increasing the ADC resolution and, thus, diminishing the outcome probability of each 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. For the chosen ADC, at most, only 256 unique values can be represented. Furthermore, the selected ±50 mV acquisition range results in a large portion of the ADC range not being utilized. This further limits the performance of our implementation and, ideally, a more appropriate interval should be considered [43].

4.3. Randomness Extraction

With the aforementioned conditions, the effective entropy of our implementation converges to a sequence length of 4 bit, after which no significant increase in the effective bits extracted is achieved. This can be seen in Figure 8. The distribution is thus divided into 16 bins and the measurements are assigned to a 4-bit Gray sequence. The electronic noise yields a contribution of roughly 3.50 bit, which corresponds to an extraction ratio of 0.50 bit from each sample. As expected, due to the QCNR value of 5 dB obtained, only a relatively small portion of bits is available to generate true RNs, which constitutes the main technical challenge of this implementation.
Two distinct randomness extractors were applied to the unprocessed bits: the SHA-512 cryptographic hash function and the Toeplitz-hashing extractor. The desired extraction ratio is achieved by hashing data subsets of appropriate length and merging the results. For the Toeplitz implementation, pseudorandom numbers are used as a seed of the hashing matrix, which can potentially influence the final RN security [44]. Ideally, sacrificing part of the QRNG output should be explored or, since this method constructs a strong extractor, a second source of randomness can be used to obtain a reusable seed [45]. The raw bits were thus subdivided into sequences of $2^{12}$ bits ($n = 4096$) and hashed with different seeds. The output sequence length, $m$, of the Toeplitz hashing algorithm is chosen, such that the ratio is lower than the maximum allowed:

$$m = \lfloor 2^{12} p \frac{H_{\text{quant}}}{H_{\text{total}}} \rfloor,$$

where $p$ was arbitrarily chosen as 80% to account for any potential entropy overestimation. Thus approximately 0.10 random bits are obtained from each raw bit. By contrast, this consideration was disregarded for the SHA-512 extractor, and thus an extraction ratio of approximately 0.13 random bits for each raw bit is roughly preserved. In this case, the output length $m$ is set as 512 bit and the input sequence length is chosen such that:

$$n = \lceil 512 \frac{H_{\text{total}}}{H_{\text{quant}}} \rceil. \quad (20)$$

The post-processing execution time severely limits the final bit rate since the algorithm implementation is incapable of keeping pace with the physical data generation rate. As such, a rate of 278 kbit/s and 1.68 Mbit/s were reached with the Toeplitz and SHA-512 extractor, respectively. Nevertheless, this setup could theoretically achieve approximately 19.69 Mbit/s.

4.4. Randomness Validation

To complement the validation of the implemented QRNG, a sample size of 6.8 Gbit was subjected to three state-of-the-art suites of randomness tests: the TestU01’s SmallCrush library [46], Dieharder test battery [47], and NIST SP 800-22 statistical suite [48]. These results are, respectively, represented in Tables A1–A3 for data subjected to both random extractors. As can be seen, the output of both extractors passes the majority of statistical tests, which shows the effectiveness of the post-processing stage and is an excellent indicator of quality for the implement generator. No discernible difference was identified between the quality of the hashed variants. Nonetheless, the SHA-512 extractor implementation is
significantly faster. However, in the NIST statistical suite (Table A3), it should be mentioned the failure of the OverlappingTemplate test. As described in [48], this test detects deviations in the expected number of occurrences of a given bit pattern $B$ with a certain length $m$. With this objective, each bit sequence was divided into substrings of 1032 bit and a 1-bit sliding window was used to search for a 9-bit run of ones. Streams with too many or too few occurrences of 9-bit runs of ones will conclusively be rejected with a $p$-value $\leq 0.01$. For multiple runs of the test, a uniform distribution of $p$-values is expected to occur, and a minimum of 488 runs must pass. In the OverlappingTemplate test, only 484 sequences satisfied this condition for the SHA-512 extractor variant. Conversely, 487 sequences passed this evaluation with the Toeplitz extractor, which indicates a marginally better result. A similar result can be seen in the distribution of $p$-values represented in Figure 9a,b for the SHA-512 and Toeplitz-hashed variants, respectively. Here, the former clearly shows a more pronounced deviation from a uniform distribution, with 20.6% of the values contained between $[0,0.1]$. Yet, the failure of both data variants is significant as it implies a flaw in the entropy source, entropy evaluation, or the randomness test itself, and not in the implementation of a particular randomness extractor. Consequently, although a conclusive reason for the observed result is difficult to give, a more extensive characterization of the entropy source and the raw output should be made to assess any potential correlations. This result may yet originate in undetected correlations induced by the TIA, or in some excess noise not properly accounted for, which leads to an overestimation of the available entropy and a reduction in the statistical distance to a uniform distribution. Additionally, the abnormal runs of ones can originate in the relatively small number of unique 4-bit sequences output by the generator. In the meantime, this problem may be mitigated by restricting the use of the output of this QNRG implementation as a seed to a cryptographically secure PRNG.

![Figure 9](image_url)

**Figure 9.** Histogram representing the distribution of $p$-values for 500 test runs with the (a) SHA-512 data variant and (b) the Toeplitz-hashed sequences.

In this way, the presence of some bias, namely the yielding of an abnormal frequency of 9-bit sequences of ones (and consequently of zeros), is detected. Given these results, we are forced to reject the hypothesis that the QRNG yields an output arbitrarily close to a uniform distribution, although this does not imply the absence of useful randomness or that the output is periodic. In fact, the implementation successfully passes a significant majority of the evaluations, including the other randomness test suites, which highlights its viability as a randomness source.

As a complementary analysis, we calculated the correlation coefficients from all data variants, including the raw unprocessed variant where only the binning process was applied. As can be seen in Figure 10, the coefficients are significantly lower for the hashed variants, which
shows that the randomness extraction process is effective at removing correlation between different samples. This result clearly supports the quality of this QRNG implementation.

5. Conclusions

In conclusion, a low-cost and high-speed QRNG based on homodyne measurements of vacuum fluctuations has been demonstrated and characterized. Detailed analysis of the main limiting factors to the implementation performance was made, and, in particular, a method for estimating the entropy contribution from the excess LO noise was presented. Results show that, when the total impinging power is constant, the entropy from classical contributions does not depend on the detection unbalancing, and, thus, the extractable randomness is constant. Through the proposed method, for an asymmetry of 50.75%, we find that only approximately 33.7% of the measured entropy can reliably be attributed to quantum fluctuations. Assuming that an eavesdropper has complete knowledge of electronic noise, an extraction rate of 0.5 true random bits per sample was achieved, which allows a theoretical throughput up to 19.53 Mbit/s. A randomness extraction operation is used to eliminate security loopholes introduced by electronic noise. This yields 192 kbit/s by applying a Toeplitz-hashing extractor, and 1.68 Mbit/s with an SHA-512 extractor. The resultant true RNs pass a proportion of 98.1% of the applied statistical tests, including the standard Dieharder and TestU01’s SmallCrush tests as well as most of NIST suite, corroborating the presence of high-quality randomness.

Author Contributions: Conceptualization, M.J.F., N.J.M., N.A.S. and A.N.P.; methodology, M.J.F., N.J.M. and N.A.S.; software, M.J.F.; validation, M.J.F.; formal analysis, M.J.F.; investigation, M.J.F., N.J.M. and N.A.S.; resources, N.J.M. and N.A.S.; writing—original draft preparation, M.J.F.; writing—review and editing, M.J.F., N.J.M., N.A.S. and A.N.P.; visualization, M.J.F.; supervision, N.J.M. and N.A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by Fundação para a Ciência e a Tecnologia (FCT) through national funds, by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020) of the Portugal 2020 framework, under 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). The authors also acknowledge support from the Programme New Talents in Quantum Technologies of the Gulbenkian Foundation (Portugal).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.
Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Randomness Test Results

The appendix summarizes the randomness test results for the TestU01’s SmallCrush library, Dieharder test battery, and NIST SP 800-22 statistical suite [48], respectively, represented in Tables A1–A3.

Table A1. TestU01’s SmallCrush results. For tests with multiple variants the worst case is reported.

| Statistical Test                   | Toeplitz-Hashing | SHA-512 |
|------------------------------------|------------------|---------|
|                                    | p-Value | Result | p-Value | Result |
| Birthday Spacings                  | 0.38     | PASSED | 0.75    | PASSED |
| Collision                          | 0.02     | PASSED | 0.11    | PASSED |
| Gap Chi-square                     | 0.92     | PASSED | 0.53    | PASSED |
| SimpPoker Chi-square               | 0.40     | PASSED | 0.32    | PASSED |
| Coupon Collector Chi-square        | 0.01     | PASSED | 0.68    | PASSED |
| MaxOft Chi-square                  | 0.40     | PASSED | 0.07    | PASSED |
| MaxOft Anderson-Darling            | 0.85     | PASSED | 0.39    | PASSED |
| WeightDistrib Chi-square           | 0.17     | PASSED | 0.98    | PASSED |
| Matrix Rank Chi-square statistic   | 0.40     | PASSED | 0.58    | PASSED |
| HammingIndep Chi-square            | 0.33     | PASSED | 0.09    | PASSED |
| RandomWalk1 H Chi-square           | 0.98     | PASSED | 0.91    | PASSED |
| RandomWalk1 M Chi-square           | 0.88     | PASSED | 0.66    | PASSED |
| RandomWalk1 J Chi-square           | 0.76     | PASSED | 0.83    | PASSED |
| RandomWalk1 R Chi-square           | 0.44     | PASSED | 0.72    | PASSED |
| RandomWalk1 C Chi-square           | 0.12     | PASSED | 0.16    | PASSED |

Table A2. Dieharder test suite with the default significance level $\alpha = 0.000001$. A certain test run is successful if the $p$-value satisfies $0.000001 \leq p$-value $\leq 0.999999$. For tests with multiple variants the worst case is reported.

| Statistical Test                   | Toeplitz-Hashing | SHA-512 |
|------------------------------------|------------------|---------|
|                                    | p-Value | Result | p-Value | Result |
| Diehard Birthdays                  | 0.40675035      | PASSED | 0.81784655| PASSED |
| Diehard 32x32 Binary Rank          | 0.02168705      | PASSED | 0.46240278| PASSED |
| Diehard 6x8 Binary Rank            | 0.98421063      | PASSED | 0.67581951| PASSED |
| Diehard Bitstream                  | 0.66303940      | PASSED | 0.93744997| PASSED |
| Diehard OPSO                       | 0.42701312      | PASSED | 0.93807686| PASSED |
| Diehard OQSO                       | 0.74489236      | PASSED | 0.94218224| PASSED |
| Diehard DNA                        | 0.87945687      | PASSED | 0.77400353| PASSED |
| Diehard Count the 1s (stream)      | 0.30986065      | PASSED | 0.65195156| PASSED |
| Diehard Count the 1s (byte)        | 0.99239469      | PASSED | 0.70164035| PASSED |
| Diehard Parking Lot                | 0.56185317      | PASSED | 0.72169377| PASSED |
| Diehard Minimum Distance           | 0.16836407      | PASSED | 0.53282829| PASSED |
| Diehard 3d Sphere                  | 0.92122584      | PASSED | 0.09348519| PASSED |
| Diehard Squeeze                    | 0.68478371      | PASSED | 0.23210050| PASSED |
| Diehard Runs                       | 0.95289230      | PASSED | 0.17701485| PASSED |
| Diehard Craps                      | 0.18203675      | PASSED | 0.99248414| PASSED |
| Marsaglia and Tsang GCD            | 0.01817631      | PASSED | 0.00951490| PASSED |
| STS Monobit                        | 0.43252666      | PASSED | 0.51032516| PASSED |
| STS Runs                           | 0.24917333      | PASSED | 0.77819504| PASSED |
| STS Serial                         | 0.97590450      | PASSED | 0.03058377| PASSED |
| RGB Bit Distribution               | 0.08876097      | PASSED | 0.99123444| PASSED |
| RGB Generalized Minimum Distance   | 0.18986042      | PASSED | 0.02234684| PASSED |
| RGB Permutations                   | 0.01963750      | PASSED | 0.29229770| PASSED |
| RGB Lagged Sum                     | 0.00849654      | PASSED | 0.75151327| PASSED |
| RGB Kolmogorov-Smirnov Test        | 0.38746113      | PASSED | 0.48506319| PASSED |
Table A3. NIST test suite with the default $\alpha = 0.01$ and a bit stream length of 13,525,308 bit. The minimum pass rate is 488/500 with the exception of the random excursion where it is 429/440 for the Toeplitz-hashing extractor. For tests with multiple $p$-values the smallest case is represented.

| Statistical Test             | Toeplitz-Hashing |                          |                          | SHA-512   |                          |                          |
|------------------------------|------------------|--------------------------|--------------------------|-----------|--------------------------|--------------------------|
|                              | $p$-Value        | Proportion               | Result                   | $p$-Value | Proportion               | Result                   |
| Frequency                    | 0.526105         | 498/500                  | PASSED                   | 0.870856  | 498/500                  | PASSED                   |
| BlockFrequency               | 0.459717         | 494/500                  | PASSED                   | 0.531812  | 496/500                  | PASSED                   |
| CumulativeSums               | 0.168112         | 496/500                  | PASSED                   | 0.090936  | 497/500                  | PASSED                   |
| Runs                         | 0.307077         | 496/500                  | PASSED                   | 0.562591  | 494/500                  | PASSED                   |
| LongestRun                   | 0.844641         | 494/500                  | PASSED                   | 0.595549  | 496/500                  | PASSED                   |
| Rank                         | 0.550347         | 495/500                  | PASSED                   | 0.486588  | 497/500                  | PASSED                   |
| FFT                          | 0.820143         | 496/500                  | PASSED                   | 0.916599  | 500/500                  | PASSED                   |
| NonOverlappingTemplate       | 0.010834         | 496/500                  | PASSED                   | 0.012474  | 497/500                  | PASSED                   |
| OverlappingTemplate          | 0.000000         | 487/500                  | FAILED                   | 0.000000  | 484/500                  | FAILED                   |
| Universal                    | 0.047478         | 495/500                  | PASSED                   | 0.662091  | 494/500                  | PASSED                   |
| Approximate entropy          | 0.921624         | 493/500                  | PASSED                   | 0.691081  | 496/500                  | PASSED                   |
| Random excursions            | 0.039635         | 437/440                  | PASSED                   | 0.159545  | 440/443                  | PASSED                   |
| Random-excursions variant    | 0.041438         | 437/440                  | PASSED                   | 0.110705  | 437/443                  | PASSED                   |
| Serial                       | 0.063615         | 499/500                  | PASSED                   | 0.307077  | 499/500                  | PASSED                   |
| LinearComplexity             | 0.401199         | 492/500                  | PASSED                   | 0.603841  | 497/500                  | PASSED                   |

References

1. Herrero-Collantes, M.; Garcia-Escartin, J.C. Quantum random number generators. Rev. Mod. Phys. 2017, 89, 015004. [CrossRef]
2. Knuth, D.E. The Art of Computer Programming, Volume 2: Seminumerical Algorithms, 3rd ed.; Addison-Wesley: Boston, MA, USA, 1998.
3. Kelsey, J.; Schneier, B.; Wagner, D.; Hall, C. Cryptanalytic attacks on pseudorandom number generators. In Fast Software Encryption; Vaudenay, S., Ed.; Springer: Berlin/Heidelberg, Germany, 1998; pp. 168–188.
4. Bouda, J.; Pivoluska, M.; Plesch, M.; Wilmott, C. Weak randomness seriously limits the security of quantum key distribution. Phys. Rev. A 2012, 86, 062308. [CrossRef]
5. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. Rev. Mod. Phys. 2002, 74, 145–195. [CrossRef]
6. Maranon, D.G.; Vallone, G.; Villoresi, P. Random bits, true and unbiased, from atmospheric turbulence. Sci. Rep. 2014, 4, 5490. [CrossRef]
7. Gong, L.; Zhang, J.; Liu, H.; Sang, L.; Wang, Y. True Random Number Generators Using Electrical Noise. IEEE Access 2019, 7, 125796–125805. [CrossRef]
8. Bayon, P.; Bossuet, L.; Aubert, A.; Fischer, V.; Pouchere, F.; Robisson, B.; Maurin, P. Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator. In Constructive Side-Channel Analysis and Secure Design; Schindler, W., Huss, S.A., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 151–166.
9. Gude, M. Concept for a High Performance Random Number Generator Based on Physical Random Phenomena. Frequenz 1985, 39, 187–190. [CrossRef]
10. Alkassar, A.; Nicolay, T.; Rothe, M. Obtaining True-Random Binary Numbers from a Weak Radioactive Source. In Computational Science and Its Applications—ICCSA 2005; Gervasi, O., Gavrilova, M.L., Kumar, V., Laganà, A., Lee, H.P., Mun, Y., Taniar, D., Tan, C.J.K., Eds.; Springer: Berlin/Heidelberg, Germany, 2005; pp. 634–646.
11. Fiorentino, M.; Santori, C.; Spillane, S.M.; Beausoleil, R.G.; Munro, W.J. Secure self-calibrating quantum random-bit generator. Phys. Rev. A 2007, 75, 032334. [CrossRef]
12. Williams, C.R.S.; Salevan, J.C.; Li, X.; Roy, R.; Murphy, T.E. Fast physical random number generator using amplified spontaneous emission. Opt. Express 2010, 18, 23584–23597. [CrossRef]
13. Wei, W.; Xie, G.; Dang, A.; Guo, H. High-Speed and Bias-Free Optical Random Number Generator. IEEE Photonics Technol. Lett. 2012, 24, 437–439. [CrossRef]
14. Martin, A.; Sanguinetti, B.; Lim, C.C.W.; Houlmann, R.; Zbinden, H. Quantum Random Number Generation for 1.25-GHz Quantum Key Distribution Systems. J. Light. Technol. 2015, 33, 2855–2859. [CrossRef]
15. Ma, H.Q.; Xie, Y.; Wu, L.A. Random number generation based on the time of arrival of single photons. Appl. Opt. 2005, 44, 7760–7763. [CrossRef]
16. Nie, Y.Q.; Zhang, H.F.; Zhang, Z.; Wang, J.; Ma, X.; Zhang, J.; Pan, J.W. Practical and fast quantum random number generation based on photon arrival time relative to external reference. Appl. Phys. Lett. 2014, 104, 051110. [CrossRef]
17. Wahl, M.; Leifgen, M.; Berlin, M.; Röhlicke, T.; Rahn, H.J.; Benson, O. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. Appl. Phys. Lett. 2011, 98, 171105. [CrossRef]
18. Wayne, M.A.; Jeffrey, E.R.; Akselrod, G.M.; Kwiat, P.G. Photon arrival time quantum random number generation. J. Mod. Opt. 2009, 56, 516–522. [CrossRef]
19. Nie, Y.Q.; Huang, L.; Liu, Y.; Payne, F.; Zhang, J.; Pan, J.W. The generation of 68 Gbps quantum random number by measuring laser phase fluctuations. *Rev. Sci. Instrum.* 2015, 86, 063105. [CrossRef]

20. Avesani, M.; Marangon, D.G.; Vallone, G.; Valloresi, P. Secure heterodyne-based quantum random number generator at 17 Gbps. *Nat. Commun.* 2018, 9, 1–8. [CrossRef]

21. Abellan, C.; Amaya, W.; Domenech, D.; Muñoz, P.M.; Capmany, J.; Longhi, S.; Mitchell, M.W.; Pruneri, V. Quantum entropy source on an InP photonic integrated circuit for random number generation. *Optica* 2016, 3, 989–994. [CrossRef]

22. Raffaelli, F.; Ferranti, G.; Mahler, D.H.; Sibson, P.; Kennard, J.E.; Santamato, A.; Sinclair, G.; Bonneau, D.; Thompson, M.G.; Matthews, J.C.F. A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers. *Quantum Sci. Technol.* 2018, 3, 035003. [CrossRef]

23. Leone, N.; Rusca, D.; Azzini, S.; Fontana, G.; Acerbi, F.; Gola, A.; Tontini, A.; Massari, N.; Zbinden, H.; Pavesi, L. An optical chip for self-testing quantum random number generator. *Appl. Phys. Lett.* 2021, 118, 264001. [CrossRef]

24. Gras, G.; Martin, A.; Choi, J.W.; Bussières, F. Quantum Entropy Model of an Integrated Quantum-Random-Number-Generator Chip. *Phys. Rev. Appl.* 2021, 15, 054048. [CrossRef]

25. Bai, B.; Huang, J.; Qiao, G.R.; Nie, Y.Q.; Tang, W.; Chu, T.; Zhang, J.; Pan, J.W. 18.8 Gbps real-time quantum random number generator with a photonic integrated chip. *Phys. Lett. Appl.* 2021, 118, 264001. [CrossRef]

26. Huang, L.; Zhou, H. Integrated 9 Gbps quantum random number generator with real-time extraction based on homodyne detection. *J. Opt. Soc. Am. B* 2019, 36, 130–136. [CrossRef]

27. Gabriel, C.; Wittmann, C.; Sych, D.; Dong, R.; Mauerer, W.; Andersen, U.L.; Marquardt, C.; Leuchs, G. A generator for unique quantum random numbers based on vacuum states. *Nat. Photonics* 2010, 4, 711–715. [CrossRef]

28. Symul, T.; Assad, S.M.; Lam, P.K. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Appl. Phys. Lett.* 2011, 98, 231103. [CrossRef]

29. Zheng, Z.; Zhang, Y.; Huang, W.; Yu, S.; Guo, H. 6 Gbps real-time optical quantum random number generator based on vacuum fluctuation. *Rev. Sci. Instrum.* 2019, 90, 043105. [PubMed][CrossRef]

30. Guo, X.; Cheng, C.; Wu, M.; Gao, Q.; Li, P.; Guo, Y. Parallel real-time quantum random number generator. *Opt. Lett.* 2019, 44, 5566–5569. [CrossRef]

31. Gehring, T.; Lupò, C.; Kordts, A.; Solar Nikolic, D.; Jain, N.; Rydberg, T.; Pedersen, T.; Pirandola, S.; Andersen, U. Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information. *Nat. Commun.* 2012, 11. [CrossRef]

32. Huang, W.; Zhang, Y.; Zheng, Z.; Li, Y.; Xu, B.; Yu, S. Practical security analysis of a continuous-variable quantum random-number generator with a noisy local oscillator. *Phys. Rev. A* 2020, 102, 012422. [CrossRef]

33. Loudon, R. The Quantum Theory of Light, 3rd ed.; Oxford University Press: Oxford, UK, 2000; pp. 88–94, 233–283.

34. Garry, C.; Knight, P. *Introductory Quantum Optics*; Cambridge University Press: Cambridge, UK, 2004; pp. 137–143.

35. Agrawal, G.P. *Laserwave Technology*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2005; pp. 151–156.

36. Almeida, M.; Pereira, D.; Facão, M.; Pinto, A.; Silva, N. Impact of imperfect homodyne detection on measurements of vacuum states shot noise. *Opt. Quantum Electron.* 2020, 52. [CrossRef]

37. Bennett, W.R. Spectra of quantized signals. *Bell Syst. Tech. J.* 1948, 27, 446–472. [CrossRef]

38. Bottacchi, S. *Noise and Signal Interference in Optical Fiber Transmission Systems*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2008; pp. 1–10.

39. Glauber, R.J. Coherent and Incoherent States of the Radiation Field. *Phys. Rev.* 1963, 131, 2766–2788. [CrossRef]

40. Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* 1948, 27, 379–423. [CrossRef]

41. Ferreira, M.J.; Silva, N.A.; Pinto, A.N.; Muga, N.J. Homodyne Noise Characterization in Quantum Random Number Generators. In Proceedings of the 2021 Telecoms Conference (ConfTELE), Leiria, Portugal, 11–12 February 2021; pp. 1–6.

42. Chi, Y.M.; Qi, B.; Zhu, W.; Qian, L.; Lo, H.K.; Youn, S.H.; Lvovsky, A.I.; Tian, L. A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution. *New J. Phys.* 2011, 13, 013003. [CrossRef]

43. Haw, J.Y.; Assad, S.M.; Lance, A.M.; Ng, N.H.; Sharma, V.; Lam, P.K.; Symul, T. Maximization of Extractable Randomness in a Quantum Random-Number Generator. *Phys. Rev. Appl.* 2015, 3, 1–12. [CrossRef]

44. Zhang, X.; Nie, Y.Q.; Liang, H.; Zhang, J. FPGA implementation of Toeplitz hashing extractor for real time post-processing of raw random numbers. In Proceedings of the 2016 IEEE-NPSS Real Time Conference, RT 2016, Padua, Italy, 6–10 June 2016.

45. Ma, X.; Xu, F.; Xu, H.; Tan, X.; Qi, B.; Lo, H.K. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Phys. Rev. A* 2013, 87. [CrossRef]

46. L’Ecuyer, P.; Simard, R. A Software Library in ANSI C for Empirical Testing of Random Number Generators. 2013. Available online: http://simul.io.umontreal.ca/testsuite01/guideshortestsuite01.pdf (accessed on 1 September 2020).

47. Brown, R.G.; Dirk Eddelbuettel, D.B. *Dieharder: A Random Number Test Suite*; Duke University Physics Department: Durham, NC, USA, 2020.

48. Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E.; Leigh, S.; Levenson, M.; Vangel, M.; Banks, D.; Heckert, A.; 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.