applied sciences

IMPACT FACTOR 2.7

CITESCORE 4.5

Article

Statistical Validation of a Physical Prime Random Number Generator Based on Quantum Noise

Maurício J. Ferreira, Nuno A. Silva, Armando N. Pinto and Nelson J. Muga

MDPI

https://doi.org/10.3390/app132312619

applied sciences

MDPI

Article

Statistical Validation of a Physical Prime Random Number Generator Based on Quantum Noise †

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

[1] Instituto de Telecomunicações, Campus Universitário de Santiago, University of Aveiro, 3810-193 Aveiro, Portugal; mauricioferreira@ua.pt (M.J.F.); anp@ua.pt (A.N.P.); muga@ua.pt (N.J.M.)
[2] Department of Electronics, Telecommunications and Informatics, University of Aveiro, 3810-193 Aveiro, Portugal
* Correspondence: nasilva@ua.pt
† This paper is an extended version of our paper published in Ferreira, M.J.; Carvalho, A.; Silva, N.A.; Pinto, A.N.; Muga, N.J. Probable Prime Generation from a Quantum Randomness 442 Source. In Proceedings of the 2023 23rd International Conference on Transparent Optical Networks (ICTON), Bucharest, Romania, 2–6 July 2023; pp. 1–4.

Abstract: Random prime numbers are an essential resource for many asymmetric cryptographic protocols. However, despite the emerging popularity of quantum random number generators (QRNGs) as sources of secure randomness, physical prime number generators have not yet been explored. In this work, we experimentally implement and characterize a vacuum-based probabilistic prime number generation scheme with an error probability of 3.5×10^{-15}. By removing the quantum source (QS), an additional scheme based on electronic noise is derived, and a comparative analysis for increasing prime lengths is made. We observed that the QS significantly outperforms the classical scheme for small prime generation, where increases up to 585.0% in the diversity of unique primes obtained are seen. Moreover, we propose a length-agnostic statistical test for prime number sequences and apply it to the output of the uniformized randomness source, which was successful in revealing underlying biases in the output prime distributions. The resultant sequences were subsequently submitted to the NIST statistical test suite, where the quantum and classical sources passed, respectively, 86.96% and 45.34% of the total test set applied.

Keywords: random number generation; probable prime numbers; vacuum fluctuations; electronic noise; Miller–Rabin probability test

Citation: Ferreira, M.J.; Silva, N.A.; Pinto, A.N.; Muga, N.J. Statistical Validation of a Physical Prime Random Number Generator Based on Quantum Noise. *Appl. Sci.* **2023**, *13*, 12619. https://doi.org/10.3390/app132312619

Academic Editor: David Petrosyan

Received: 27 October 2023
Revised: 17 November 2023
Accepted: 20 November 2023
Published: 23 November 2023

1. Introduction

Random Numbers (RNs) are currently an indispensable component of most cryptographic systems since their security fundamentally relies on using unpredictable keys, nonces, or seeds [1,2]. For example, random prime number generation has been particularly important given its role in choosing key pairs for public-key cryptographic protocols such as RSA or ECC [3]. The security of the former, for instance, relies on the difficulty of factoring a given public modulus n, which is obtained from the product of two large prime integers, $n = pq$. The public key, which is used for encryption, consists of the pair (n, e), where e is an additional public exponent. In turn, this factor e is related to the private exponent d, which is part of the private key (n, d) used for decryption. The first step to generate these key pairs is thus randomly selecting the two large prime factors. These should remain secret and be unpredictable since recovering them would allow an adversary to compute the private exponent from the public key [4]. Although often overlooked, choosing an adequate Random Number Generator (RNG) is thus critically important [5]. If an adversary can predict any future or past outputs with better accuracy than randomly guessing, security loopholes are introduced even if the cryptographic protocol itself remains secure [6]. As a result, the traditional approach of employing high throughput deterministic RNGs, the so-called Pseudorandom Number Generators (PRNGs), for security-critical applications

seems increasingly unsound [7,8]. Despite the best algorithmic implementations being able to output uniformly distributed numbers that pass multiple statistical tests, their output is inherently periodic and thus can be predicted by adversaries with enough computational resources [9]. In fact, the applicability of cryptanalytic attacks against PRNGs has progressively been made easier by the increasing computational power and novel techniques such as Machine Learning (ML), which are capable of independently recognizing the correlations in the RNG output [10,11]. More worryingly, they are particularly susceptible to the insertion of backdoors [12], and weak cryptographic keys have already been found to still be widely in use due to poorly implemented PRNGs [13]. Although there are alternative physical implementations that extract randomness from measuring noisy phenomena, most of these still rely on classical processes such as atmospheric noise [14–16]. Consequently, they still simply ground their unpredictability on an incomplete description of the physical system and can potentially present highly correlated outputs [2]. Indeed, recently, a ML model was found to be successful in increasing the probability of guessing the outcome of such a RNG whenever the electronic noise source was prominent [11].

These problems are slowly being addressed by the emergence of Quantum Random Number Generators (QRNGs), which extract randomness from the probabilistic properties of quantum measurements [2,17]. Unlike the approaches based on classical noise, their randomness source is fundamentally unpredictable to any adversary, thus allowing them to yield information-theoretically provable randomness [18]. In fact, several different schemes have already been thoroughly explored, such as measuring amplified spontaneous emission [19,20], phase laser noise [21,22], photon arrival times [23,24], or the quadrature fluctuations of the optical vacuum state [25–27]. The latter is particularly promising since it can deliver the high throughput rates of potentially several hundred Gbps seen for more complex implementations while requiring a simpler homodyne measurement scheme that can be implemented with off-the-shelf optical devices [28]. Moreover, obtaining the optical vacuum state can be done, within a reasonable approximation, by simply blocking the impinging optical signal, which makes it a source more resilient against environmental perturbations [29]. Due to the lower number of optical components required, these schemes are also more easily integrated. Despite often sacrificing the achievable throughput due to challenges such as the presence of dark currents, these compact schemes are essential to achieve commercially viable implementations [28,30]. This thus lowers their adoption threshold and allows them to compete against the traditional pseudorandom solutions. Nonetheless, the output statistical quality of these schemes should not be assumed by default but corroborated by extensive characterization. In fact, challenges such as guaranteeing a properly balanced detection or fluctuations in the classical noise floor can lower the available entropy and introduce security loopholes [31]. Although fully device-independent solutions exist, these rely on observing loophole-free Bell inequality violations and thus are tendentiously extremely slow and difficult to implement [32]. This makes them unfeasible for any practical realization, and thus, implementations at least partially based on trusted devices are widely used. Therefore, most schemes are still prone to manipulation by an adversary with even partial access to the entropy source, and their statistical properties can deviate if the expected environmental conditions change [33].

Given this, surprisingly, few assessments of the applicability of these generation schemes for random prime number generation have been made [34]. Random prime numbers are typically distilled from the output of a deterministic RNG using provable prime number generation algorithms such as the Shawe–Taylor random prime routine described in the Digital Signature Standard (FIPS 186-5) [3]. Alternatively, one can sequentially test different RNs with either primality-proving algorithms, such as the Pocklington and AKS tests, or probabilistic approaches such as the Miller–Rabin primality test [4,35]. In either case, the statistical quality of the retrieved prime number sequence is non-trivially impacted by the chosen RNG. Despite these routines acting as an additional postprocessing layer and thus masking some input biases, a highly correlated output can still be present when a compromised randomness source is used [34].

In this work, we extend the preliminary analysis made in [34] and proceed with the statistical validation of a probable quantum prime number generator based on raw homodyne measurements of vacuum quadrature fluctuations. To evaluate the extent to which the additional classical entropy impacts the statistical quality of the gathered prime sequences, we additionally perform a comparative analysis with a purely classical entropy source derived from the proposed vacuum-based QRNG and present the key merit figures such as the variation in the diversity of prime numbers obtained and the search times for different prime lengths. Moreover, a length-agnostic statistical validation approach based on measuring the frequency of observations in an equiprobable binning of the prime output distribution is proposed, and the resulting sequences are submitted to the NIST statistical test suite.

This paper is organized into 4 sections. In Section 2, we describe the experimental QRNG implementation and the additional probabilistic prime-searching algorithm implemented. In Section 3, the output noise from the quantum source is characterized in comparison with measurements from the classical scheme, and the prime sequences are statistically validated. Moreover, the key figures of merit for prime number generation are compared. Finally, in Section 4, a brief conclusion is presented.

2. Materials and Methods

In this study, to assess the impact of classical entropy contributions in the prime number generation, we have comparatively analyzed two randomness sources exploring distinct physical phenomena. The first is the proposed quantum scheme, which performs quadrature measurements of the vacuum state by employing a homodyne detection scheme. Here, these normally distributed noise contributions are amplified by a Local Oscillator (LO) that interacts with the vacuum state in a balanced Beam Splitter (BS) [29]. In practice, the input port of this BS can simply be blocked to obtain a reasonable approximation of this optical state. Subsequently, the output beams are detected, and their photocurrents are subtracted. Thus, ideally, only the shot noise remains, whose variance, σ_Q^2, is proportional to the impinging optical power, P_{LO}:

$$\sigma_Q^2 \propto q\mathcal{R}(\lambda)P_{LO}\Delta f, \tag{1}$$

where q is the electron's charge, $\mathcal{R}(\lambda)$ the wavelength-dependent responsivity of the photodetector and Δf its bandwidth [31]. Additional classical noise contributions will also be inevitably present due to factors such as excess relative intensity noise from an unbalanced detection or the electronic components in the experimental setup. The latter component was also separately recorded to obtain a second Classical Source (CS) from the device's electronic noise. Since the output of the vacuum-based QRNG contains a mixture of quantum entropy and potentially correlated classical noise contributions, a Randomness Extractor (RE) layer is typically required. This stage sacrifices a portion of the biased output sequence, allowing the scheme to achieve information-theoretically secure and bias-free RNs [18]. Nonetheless, since our goal is to assess the impact that a predominance of classical noise has on the prime number output, this stage was not implemented. Instead, we have simply considered the unprocessed output of the quantum scheme. Consequently, any correlations presented by the classical RNG will also be displayed by the QRNG implementation, thus allowing us to quantify the impact of the quantum noise source on the statistical quality of the prime output. We refer to [31] for a complete theoretical description of the implemented vacuum-based QRNG and derivation of the expected variances for all the noise sources considered.

2.1. QRNG Implementation

Figure 1 shows a schematic diagram of the implemented experimental vacuum-based randomness generation scheme. Here, a 1550.92 nm continuous-wave laser tuned at approximately 11 dBm is used as the LO, while a Variable Optical Attenuator (VOA) (VOA1) allows the accurate control of its output power. Moreover, a 80/20 BS (BS1) and an Optical

Power Meter (OPM) are introduced to monitor the input power at the 50/50 BS (BS2), which was registered at 5.5 mW. A second VOA (VOA2) was additionally used to obtain a fine-tuned balanced detection scheme. A balanced receiver (WL-BPD1GA) with an output bandwidth ranging from 300 kHz to 1 GHz was subsequently introduced to detect and subtract the output optical signals. It contains a Transimpedance Amplifier (TIA) with a gain of 3500 V/W that amplifies the resultant electronic signal. Finally, the output measurements are sampled at 983.04 MSa/s by the Texas Instruments ADS54J60EVM Analog-to-digital Converter (ADC) module, which has an acquisition range, R, of ± 0.95 V and a resolution, n, of 16 bits.

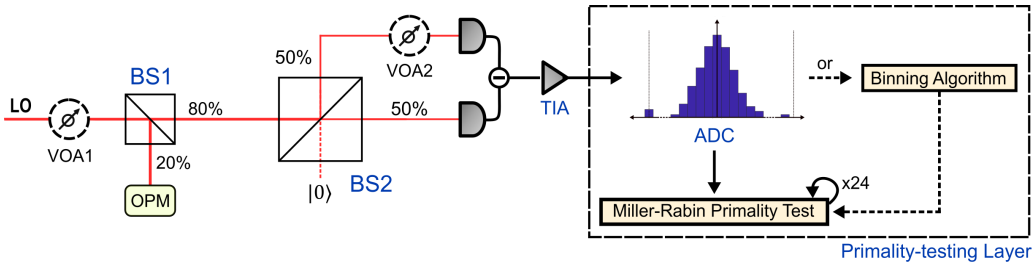


Figure 1. Experimental setup of the proposed vacuum-based QRNG. The LO interacts with the vacuum state in a BS (BS2) with its second input port blocked. Its output signals are subsequently detected in a balanced homodyne detection scheme and amplified by a high-gain TIA. The resulting signal is then either directly submitted to the prime-searching algorithm or mapped into a uniform distribution before a set of 24 Miller–Rabin primality tests is applied.

The digitization of the noise signal also introduces an additional quantization noise variance that can be determined as $\frac{\delta^2}{12}$, where $\delta = \frac{R}{2^{(n-1)}}$ is the bin width of the ADC [27]. Given these experimental conditions, an additional noise variance of $7 \times 10^{-5}\,\mathrm{mV}^2$ can be expected. Moreover, as specified by the Nyquist sampling theorem, the noise signal will not be accurately recovered when its bandwidth is larger than half the sampling frequency. Despite this, here, this condition should not be obeyed since, given a finite signal bandwidth, any samples taken would necessarily be highly correlated. In fact, under an ideal TIA response, maximally uncorrelated measurements are only obtained when the sampling frequency, f_s follows [36]:

$$f_s = \frac{2\Delta f}{j}, \quad \forall j \in \mathbb{N}, \tag{2}$$

where Δf is the cut-off frequency of the detector's TIA. Although an optimal sampling rate was not considered in this implementation, a value lower than 2 GSa/s must nevertheless be adopted to avoid introducing additional temporal correlations in the homodyne output signal [34].

To derive the classical randomness source based on the electronic noise measurements, the LO was simply removed from the experimental setup described, and measurements of the detector's electronic noise were recorded. This process also allows us to estimate the contribution of the classical noise floor to the discretized homodyne signal distribution, M, and thus quantify the fraction of randomness that can be extracted without compromising the implementation. A conservative approach is to consider the worst-case conditional min-entropy, $H_{\min}(M|E)$, as a lower bound. It quantifies the maximum probability of an eavesdropper predicting a QRNG outcome, given that the classical noise distribution E is known with arbitrary precision. Assuming that M and E are independent and follow identically distributed null-mean Gaussian distributions: [21,37]:

$$H_{\min}(M|E) = -\log_2\left[\max\left\{\frac{1}{2}\left[1+\mathrm{erf}\left(\frac{e_{\max}-R+\frac{3\delta}{2}}{\sigma_Q\sqrt{2}}\right)\right], \mathrm{erf}\left(\frac{\delta}{2\sigma_Q\sqrt{2}}\right)\right\}\right], \tag{3}$$

where R and δ are, respectively, the acquisition range and bin width of the previously considered ADC module, σ_Q is the experimentally measured standard deviation of the quantum noise distribution, and $e_{\max}$ is the maximum excursion considered for the classical noise signal. Here, this parameter was taken as $5\sigma_E$ so that, for any given classical noise sample, only a low probability, approximately 5.73×10^{-7} , of it falling outside the considered interval $[-e_{\max}, e_{\max}]$ was observed.

2.2. Prime-Searching Algorithm

Finally, the measurements were submitted to the prime-testing layer, which maps the output distribution of both schemes into a set of random prime numbers with a given bit length n_{prime}. Since both randomness sources measure Gaussian-distributed phenomena, their output distribution will be biased if no further postprocessing is applied. This could reflect itself on the generation of prime numbers, and thus, their output signals were also mapped into uniform distributions in an effort to increase their measured entropy. With that aim, the measurement distributions were divided by an equiprobable binning algorithm, and 16-bit Gray sequences were attributed to all outcomes falling on a certain bin [29]. Consequently, uniformly distributed 16-bit RNs are obtained. This step is also necessary to do a proper comparative analysis of the two sources since the electronic noise distribution will naturally have a lower variance than the overall homodyne signal, which includes additional contributions. The CS thus occupies a smaller proportion of the ADC range and outputs fewer unique codes, which further increases its bias when compared with the Quantum Source (QS). Nonetheless, to allow an assessment of the impact that this stage has on the statistical quality of the obtained prime RNs, the scenario where the biased distributions were directly used has also been considered.

To distill the prime numbers, the 16-bit random output is first converted to its binary representation. The algorithm then gathers a n_{prime}-bit prime number candidates by parsing the binary input bitwise until both the Most Significant Bit (MSB) and Least Significant Bit (LSB) are equal to one [34]. This guarantees that the candidate number is odd and has the expected bit-length. Naturally, in a practical application, where the generation rate is a major concern, the MSB and LSB can simply be forced to be unitary while gathering $(n_{\text{prime}} - 2)$-bit binary sequences from the QRNG output. This would greatly increase the fraction of the output submitted to the primality test and thus decrease the number of candidate numbers tested until a prime is found.

A sequence of 24 standard Miller–Rabin primality tests is then applied to the candidate number as defined by the Digital Signature Standard [3]. Given that a RE layer was not implemented, the random basis required for each test iteration was obtained from a Mersenne Twister PRNG. This avoids having to further limit the number of candidate numbers submitted and guarantees the statistical significance of the primality test even if correlations exist in the QRNG output. Given the sequence of probabilistic primality tests applied, the expected probability of false positives for this prime generator can be calculated as 4^{-24}, thus standing at 3.55×10^{-15} For this work, in order to balance between accuracy and algorithmic speed, a compromise was made in selecting this value. Nevertheless, a longer sequence of primality tests should be included to meet the security standards set for cryptographic applications such as RSA key generation [3].

In this work, we have chosen this approach of probabilistic primality testing due to, despite introducing the possibility of false positives, being much faster than deterministic algorithms, thus making the generation of large prime numbers feasible. Disregarding the test algorithmic complexity, a lower bound for the theoretically possible prime generation rate of this scheme, N, can be given by taking the asymptotic approximation for the prime-counting function, $\pi(x) \approx \frac{x}{\log x}$ [4], yielding:

$$N(\text{in primes/s}) \approx \frac{G}{2} \frac{n_{\text{prime}} - 2}{n_{\text{prime}}(n_{\text{prime}} - 1)\log 2} \tag{4}$$

where G is the maximum throughput of the implementation in bit/s. This yields a reasonable approximation for $G \gg n_{\text{prime}}$. The real performance is naturally much lower since it depends on the computational power available and decreases with the $O(24 \log^3 n_{\text{prime}})$ algorithmic complexity of the primality test [4].

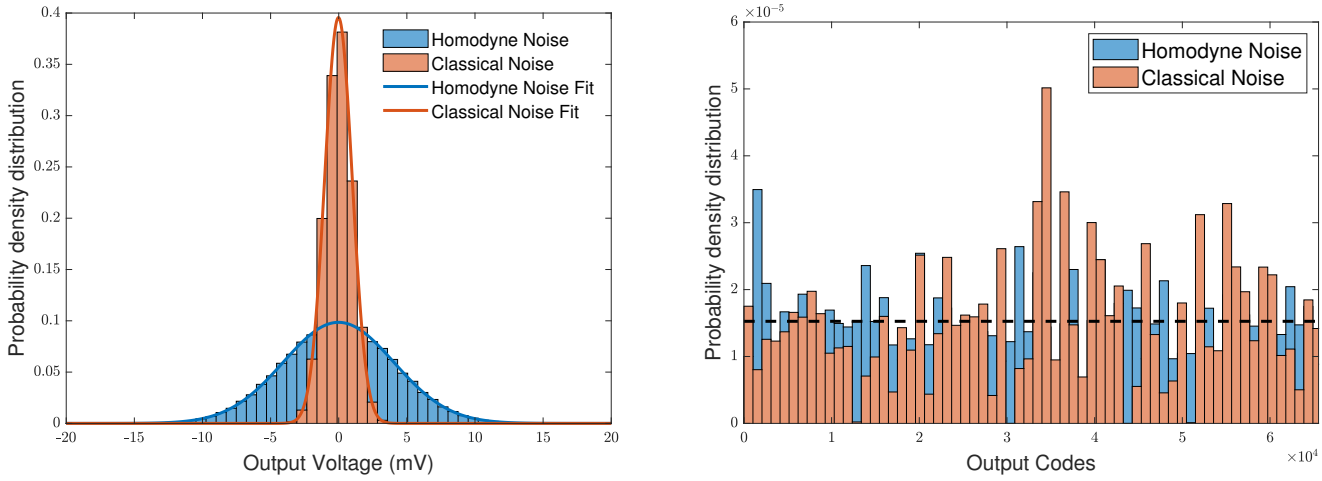
3. Results and Discussion

A sequence of 1 G noise samples was acquired for each of the randomness sources considered and used in the noise characterization presented in Section 3.1. As previously mentioned, each of these datasets was then considered in two different scenarios: directly in its biased form or after mapping them into a uniform distribution. By taking them in their binary representation, four distinct sequences of random bits were obtained. For each case, only the first 1 GB was submitted to the prime-searching algorithm. Consequently, in all cases, the segment of binary data used in prime number generation directly results from the first 500 M acquired samples from the respective noise source. All the described postprocessing was implemented on an Intel i9-10900k Central Processing Unit (CPU) for increasingly large prime numbers. To assess the performance variation of the scheme, the algorithm was implemented for prime lengths of 32, 64, 128, 256, and 512 bits. Given the fixed size of its binary input, the total amount of prime numbers yielded by the algorithm will decrease with the prime length. Consequently, when directly comparing the figures of merit obtained for different prime lengths, only the first 10 M prime numbers of each case were considered.

3.1. Noise Characterization

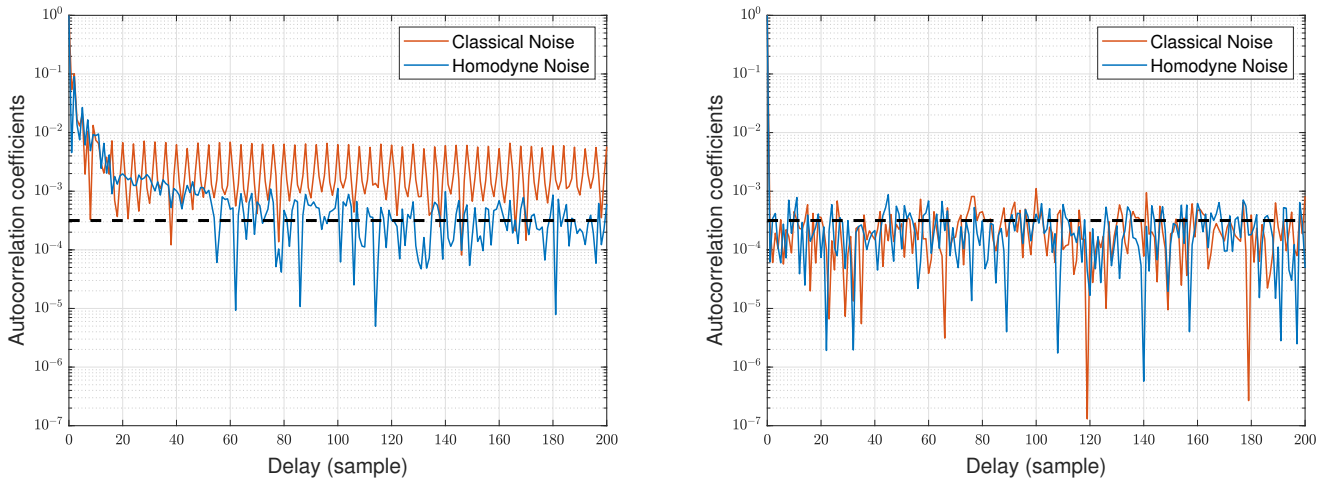
In the conditions previously described, a Quantum-to-classical Noise Ratio (QCNR) of at least 11.7 dB was always observed, which highlights the high noise clearance obtained. Over 1×10^9 samples, a classical noise floor of $1.04 \times 10^{-6}\,\text{V}^2$ was evaluated, while an average variance of $1.64 \times 10^{-5}\,\text{V}^2$ was seen for the homodyne signal. As can be seen in Figure 2a, both noise sources follow the expected null-mean Gaussian distribution. After applying the binning algorithm, as can be seen in Figure 2b, these output signals appear to be successfully mapped to the same set of output codes. Nonetheless, both sets seem to significantly deviate from the theoretically expected uniform distribution, whose probability density function is represented by the dashed line. This is additionally corroborated by the fact that both datasets conclusively fail a Chi-square goodness-of-fit test with null p-values, thus rejecting the null hypothesis that the measurements observed arise from a uniform distribution. Consequently, we verify that the simple binning algorithm is not completely successful in suppressing all the underlying biases of the raw RNG output. This illustrates the importance of implementing the RE layer in a fully fledged practical application. Despite this, the CS seems to present a greater deviation than the raw QRNG output, which may be a consequence of the increased entropy introduced by the QS.

In Figure 3a,b, the normalized autocorrelation coefficients for 10 M measurements calculated over a delay of 200 samples can be seen, respectively, for the raw and uniformized dataset. For a sequence of this size, these values should be normally distributed around a null average value with a standard deviation of 3.16×10^{-4}, which is here represented by a black-dashed line. Although the coefficients for the uniformized output stay within the expected standard deviation in both scenarios, this clearly contrasts with the case seen for the raw sequences presented in Figure 3a. Here, the QS clearly shows significant correlations for delays up to 60 samples, which can be mostly attributed to the TIA [36]. Meanwhile, we confirm the highly correlated nature of the CS output, which clearly shows the unreliability of using electronic noise for randomness generation. Consequently, we expect the raw CS to perform significantly worse at prime number generation.



(**a**) (**b**)

Figure 2. Distribution of 100 M samples of homodyne noise and classical noise taken (**a**) before and (**b**) after the binning algorithm was applied. This equiprobable binning maps both Gaussian distributions to the same output space. The black-dashed line represents the theoretical expected probability density function.



(**a**) (**b**)

Figure 3. Autocorrelation coefficients for 10 M classical and homodyne noise samples, calculated before (**a**) and after (**b**) the binning algorithm was applied. The black-dashed line represents the theoretical standard deviation expected.

Although the RE layer was not implemented, a quantum min-entropy of 8.39 bit was calculated for the QRNG implementation through the evaluation of Equation (3). At the chosen sampling rate, an information-theoretically secure implementation would support a maximum output rate of approximately 8.25 Gbps. This high throughput allows the implementation of a fast prime generation scheme. For example, as can be assessed through Equation (4), a theoretical prime generation rate of 180.0 M primes per second could be expected for 32-bit primes. Naturally, this does not consider the algorithmic complexity of the prime-testing layer, and significantly lower rates would be seen in a real-time implementation. Moreover, as expected, this rate decreases for prime numbers with longer bit-lengths since, according to the prime number theorem, the density of primes for any given value x is asymptotically $\frac{1}{log(x)}$ [4]. Consequently, the probability of the RNG outputting a prime number decreases for larger bit sizes. For example, for a length of 512 bit, the expected output rate is 11.6 M primes per second.

3.2. Figures of Merit

Given the input noise previously characterized, the total number of primes found over the entire 1 GB dataset for each of the scenarios considered is represented in Figure 4a. Here, the solid line represents a lower bound for the total number of primes found estimated through Equation (4). Here, it should be noted that the total number of primes found should asymptotically approximate this bound for increasing bit-lengths in agreement with the approximation taken for the prime-counting function in Section 2.2. As theoretically expected, this figure consistently decreases for larger prime lengths but remains relatively constant across the four scenarios for each prime length. A notable exception can be seen for the 32-bit prime output. Here, the normally distributed sources yield significantly fewer numbers than the uniformized scenarios. In fact, for the raw CS and QS cases, a total of 187.9 M and 191.7 M numbers were, respectively, obtained, representing decreases of 3.89% and 1.94% when compared with the average of 195.5 M seen across the uniformized scenarios. This reduction can naturally be explained by the biased input distribution of the raw randomness sources and is consistent with the smaller variance of the CS, which implies a smaller probability of yielding extreme candidate numbers.

Despite this, this performance difference is not seen in the time that it takes to find each prime, which stays consistent across the four datasets considered. Instead, the search time exponentially increases with the prime length as described by the decreasing generation rate, expressed in Equation (4), and the algorithmic complexity of the Miller–Rabin primality test. Figure 4b clearly illustrates this. For instance, although finding each prime took an average of 108.8 µs across all cases considered, 1019.2 µs were necessary for a length of 512 bit, highlighting the challenge of achieving physical RNG schemes able to deliver prime lengths suitable for cryptographic applications.

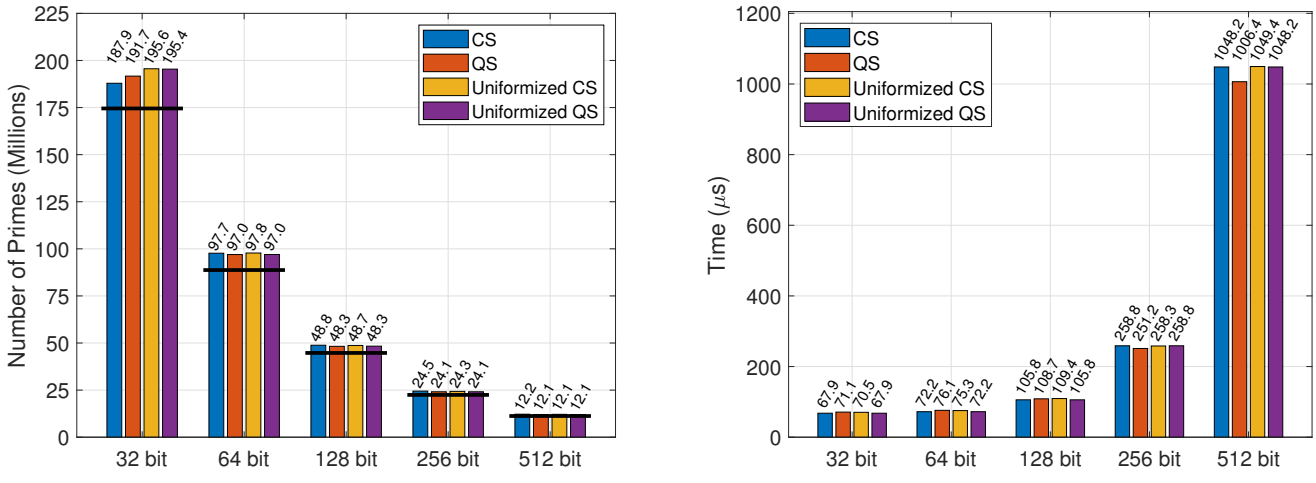


Figure 4. (**a**) Total number of primes found, and (**b**) the respective average search time required, with increasing prime sizes for each of the randomness sources considered. In the former, the solid line represents the estimated lower bound for the total number of prime numbers generated. All the values obtained are additionally represented for each case.

A more relevant figure of merit than the overall number of primes obtained is the diversity of the prime output sequences since it allows the identification of a prevalence of repeated outputs. Here, to allow a comparison between all sources and prime lengths considered, we have taken 10 M prime numbers from each case and compared the number of unique values. In fact, while for larger primes, every output is unique across all cases considered, this is not true for the 32 and 64-bit lengths. As seen in Figure 5a, the diversity of primes is particularly low for the 32-bit case, where the number of unique values is only a small fraction of the total. As with what was seen in the overall number of primes, for the unprocessed randomness sources, this observation can be expected since, due to the

normally distributed input noise, certain ADC codes have a higher probability of being observed. For smaller primes, which are constituted from fewer samples, this significantly reduces the diversity of candidate numbers seen, and thus, the probability of observing repeated prime numbers increases. This is obviously more easily observed in the 32-bit case, where every candidate number is only obtained from 2 ADC samples. However, the same phenomena can be seen for the 64-bit prime sequence represented in Figure 5b.

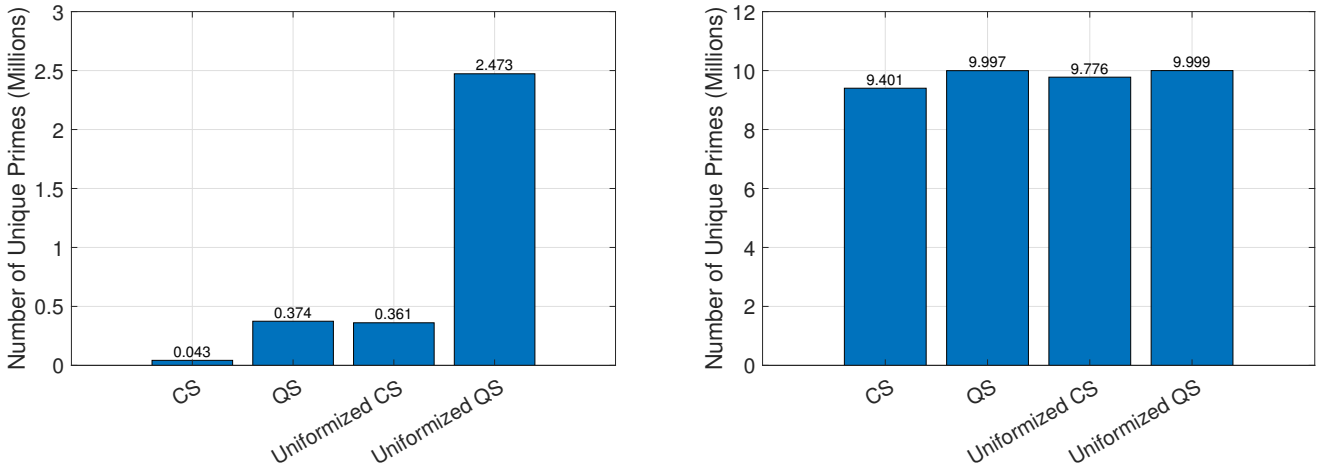


Figure 5. Number of unique primes observed for each of the randomness sources considered. Values were evaluated for 10 M primes with lengths of (**a**) 32 bits and (**b**) 64 bits. Additionally, all the values obtained are represented for each case.

The uncorrelated nature of the QS shows here an immediate advantage, yielding approximately 827.5% more unique RNs than the classical case. In fact, this difference cannot be explained by the higher noise variance of the homodyne signal. Although uniformizing the input noise clearly increases the diversity of primes for the classical scheme, the uniformized QS still outperforms it by an order of magnitude. Indeed, we observe an additional gain of 585.0% that cannot be solely attributed to the biased distribution of the unprocessed randomness sources. Nevertheless, at least for the 32-bit case, the diversity of primes remains low even for the uniformized QS, confirming the underlying bias revealed in Section 3.1 for both sources considered. Given that, in reality, the QS is a mixture of quantum noise and classical contributions, these can also be attributed to the CS. Despite this, it would be important to assess this figure of merit after implementing an adequate RE layer.

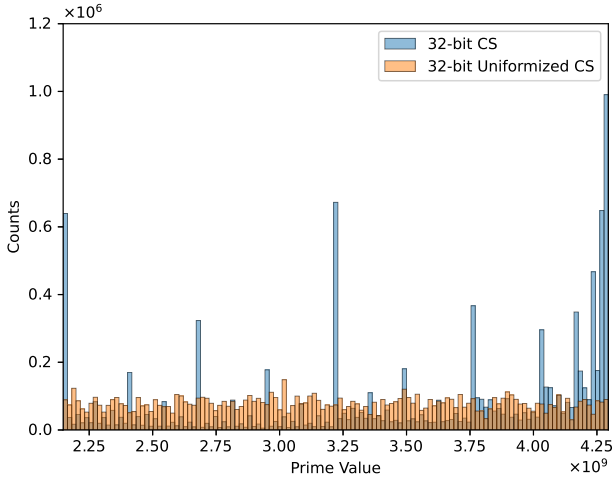
For completeness, in Table 1, we also present the variation in the diversity of prime numbers taken for the entire 1 GB total number of primes generated across different noise sources, which are also reflected in the values calculated. Here, the behavior previously described can still be observed, and, notably, the diversity variation for the 64-bit case is much more pronounced than in the first 10 M values. Finally, it should be noted that, in total, the raw CS yielded only 0.056% of the entire set of 32-bit prime numbers. On the other hand, both the QS and the uniformized CS were much more successful, generating approximately 0.53% of all possible outcomes. Meanwhile, the uniformized QS showed an even greater performance increase, outputting nearly 5% of all 32-bit prime numbers, which clearly illustrates its superiority.

Table 1. Difference (expressed in %) in the diversity of prime numbers found, when compared with the CS and uniformized CS cases, for the QS, uniformized CS, and uniformized QS schemes. In each case, all the prime numbers found in the entire 1 GB dataset were considered. Data from [34].

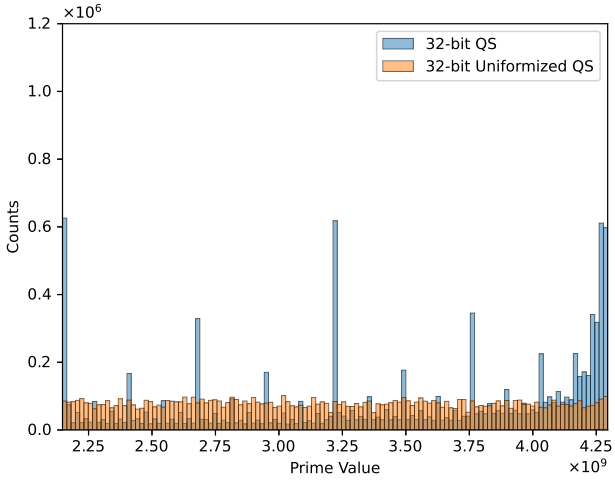
Prime Length (Bit)	QS (CS)	Uniformized CS (CS)	Uniformized QS (CS)	Uniformized QS (Uniformized CS)
32	890.7	837.1	8749.0	844.3
64	53.7	33.4	54.0	15.5

3.3. Statistical Validation

As a simple assessment of the statistical quality of the prime number sequences obtained, the distribution of 10 M samples was plotted for increasing lengths in each of the four cases considered. To illustrate these results, the 32-bit prime output is represented for the CS and QS cases, respectively, in Figure 6a,b. The distributions seen for all other lengths evaluated can be found in Figure A1 from Appendix A. As can be seen, the distribution significantly improves after applying the binning algorithm and uniformizing the input noise. In fact, both the raw CS and QS distributions appear to be clustered around certain values in the domain of possible outcomes, presenting prominent peaks in the number of counts. Meanwhile, the uniformized sources approach the desired uniform distribution among all possible outcomes. As seen in Figure A1, this behavior remains remarkably consistent across all prime lengths, with the outcome distribution following the same recognizable pattern. Given this, the raw noise sources appear to not be suitable for safe prime number generation and will be excluded from the following analysis. Additionally, as is exemplified in Figure 6c, we see an additional improvement of the prime distribution when the QS is considered .

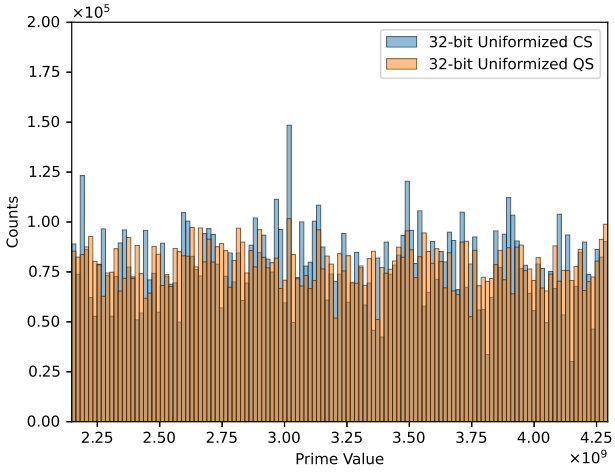


(**a**)



(**b**)

Figure 6. *Cont.*



(**c**)

Figure 6. Representative output distribution of 10 M 32-bit prime numbers for the (**a**) CS and (**b**) implemented vacuum-based QS both in the raw and uniformized scenarios. In (**c**), the 32-bit prime distributions for the uniformized sources are highlighted.

3.4. Length-Agnostic Statistical Validation

In this section, we present a length-agnostic approach to assess the statistical quality of the prime RNG output based on observing the probability of measurements falling below a given threshold. Since prime numbers are not uniformly distributed in the set of natural numbers $\mathbb{N}$, searching for the presence of patterns in the RNG output is not a trivial task. Statistical test suits, such as the one from NIST [1], typically certify randomness by expecting uniformly distributed sequences and simply test for deviations from this assumption. Moreover, for larger prime lengths, collecting and testing a sufficiently representative sequence can quickly become unfeasible due to the vast number of possible outcomes and the computational precision required to represent these values. Most statistical evaluations will be increasingly complex for larger prime lengths, making their implementation unfeasible.

Nonetheless, it should be possible to establish a threshold, p_{th}, such that any given n-bit prime distribution can be mapped into two equiprobable bins, each containing half of all possible outcomes. An unbiased prime RNG should then yield a uniformly distributed binary sequence that can be tested by a randomness test suite. Unfortunately, it is not feasible to calculate the exact value of the prime-counting function, $\pi(x)$, for any arbitrary x. Instead, lower and upper bounds, $\pi_{\text{min, max}}(x)$, must be established [38]:

$$\begin{aligned} \pi(x) &\geq \frac{x}{\log x}\left(1+\frac{1}{\log(x)}+\frac{1.8}{\log^2(x)}\right) \quad \text{for } x \geq 32299 \\ \pi(x) &\leq \frac{x}{\log x}\left(1+\frac{1}{\log(x)}+\frac{2.51}{\log^2(x)}\right) \quad \text{for } x \geq 355991. \end{aligned} \tag{5}$$

Since $\pi(x)$ is not a bijective function, p_{th} will also have to be estimated and thus presents associated uncertainty bounds, $p_{\text{th}}^{\text{min, max}}$. For any $k = \pi(x)$ [39]:

$$\begin{aligned} p_k &< k\left(\log(k)+\log\log(k)-1+\frac{\log\log(k)-2}{\log(k)}-\frac{(\log\log(k))^2-6\log\log(k)+10.667}{2\log^2(k)}\right) \quad \text{for } x \geq 46254381 \\ p_k &> k\left(\log(k)+\log\log(k)-1+\frac{\log\log(k)-2}{\log(k)}-\frac{(\log\log(k))^2-6\log\log(k)+11.321}{2\log^2(k)}\right) \quad \text{for } x \geq 2. \end{aligned} \tag{6}$$

Consequently, given a certain probability r that a n-bit prime number is below p_{th}, the expected interval for the number of measurements below the threshold, $I_{\text{min, max}}$, can be estimated through Equation (5):

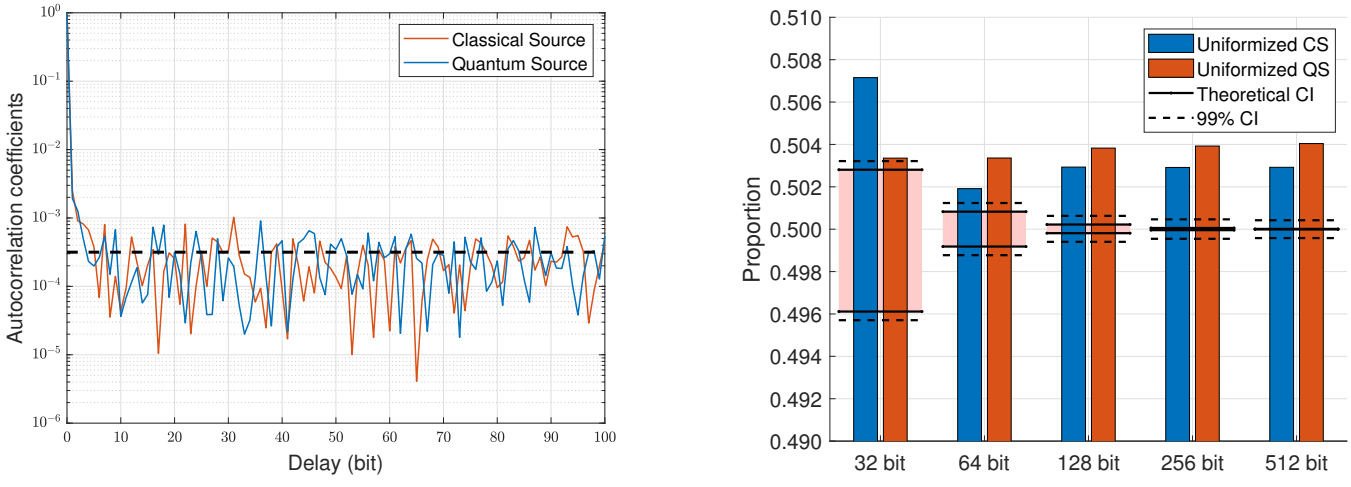
$$I_{\min,\,\max} = (1-r)\pi_{\min,\,\max}(2^{n-1}) + r\pi_{\min,\,\max}(2^n - 1). \tag{7}$$

Since there is uncertainty in determining p_{th}, there is also a maximum expected interval for the proportion of measurements below the threshold, $r_{\min,\,\max}$, which can be numerically calculated using the bounds in Equation (6):

$$r_{\min,\,\max} = \frac{\pi_{\min,\,\max}(p^{\min,\,\max}_{I_{\min,\,\max}}) - \pi_{\max,\,\min}(2^{n-1})}{\pi_{\max,\,\min}(2^n - 1) - \pi_{\max,\,\min}(2^{n-1})}. \tag{8}$$

After dividing the distribution of number primes, finding a proportion of outcomes outside the calculated probability interval, $r_{\min,\,\max}$, is a strong indicator that the sequence under test is biased. Moreover, since the output measurements are mapped into binary sequences, this approach has the advantage of not increasing in complexity for larger prime lengths, which allows the statistical validation of all prime lengths considered.

Here, we have applied this mapping, with a threshold probability of 0.5 , to the output of the uniformized CS and QS. In Figure 7a, the normalized autocorrelation coefficients for the binary threshold values of 10 M 32-bit prime numbers are shown. As can be seen, no persisting correlations were found for either source. The same is seen in the correlation analyses for all other lengths, which can be found in Figure A2 from Appendix A. Additionally, the proportion of measurements that fall below the equiprobable threshold was calculated for increasing lengths, as shown in Figure 7b. Here, the theoretically expected Confidence Interval (CI), given by Equation (8), are represented by full lines. Nonetheless, since only 10 M samples were evaluated, its 99% binomial CI was also calculated for each of the probability bounds. As can be seen, all the obtained values appear outside the acceptable interval. Consequently, we are forced to conclude that the prime RNG fails this particular statistical test for all the cases that were considered. Given that a single assessment was made, additional test runs are necessary to assess the statistical significance of this result. Nonetheless, this indicates an unbalanced dataset where the proportions of 0's and 1's in the binary sequences are significantly different. In practice, this means that the prime generation of the implemented RNG is slightly unbalanced, with more values being consistently outputted below the calculated threshold even for the larger prime lengths.



(**a**) (**b**)

Figure 7. (**a**) Normalized autocorrelation coefficients for 10 M threshold values for the 32-bit uniformized sources. The black-dashed line represents the theoretical standard deviation expected. (**b**) Proportion of the 10 M samples that fall below the equiprobable threshold. Full lines represent the theoretical maximum expected interval, while black-dashed lines represent its 99% CI.

Finally, to conclusively determine the significance of this result, a 100 Mbit binary sequence obtained from the 32-bit prime output was submitted to NIST's statistical test

suite [1]. These results are represented in Table A1 from Appendix B, both for the uniformized CS and QS. Here, each binary sequence was subdivided into bitstreams of 1 Mbit and subsequently submitted to the statistical tests. As can be seen, the output conclusively fails most of the applied evaluations, which confirms our prior assessment. In fact, we verify that both sources decisively fail the *Frequency* test, which evaluates a very similar metric to the previous analysis. Notably, although it also yields a failure, the QS performed slightly better in the *OverlappingTemplate* and *NonoverlappingTemplate* tests. In fact, here, 83 and 73 sequences, respectively, successfully passed these tests, which is contrasted with the 57 and 31 sequences that yielded a positive result for the CS. As described in [1], these two tests assess the occurrence of predetermined bit patterns, which could indicate that the QS output has higher entropy. Moreover, although the QS ultimately fails some test runs and, consequently, is rejected by the overall test, it is relevant to highlight that the vacuum-based QRNG performed significantly better than the classical scheme when considering all test iterations applied. In fact, the QS successfully passed 140 tests of the 161 applied, yielding a success rate of 86.96%. Meanwhile, the CS only passed 45.34% of the tests considered by the statistical suite. Despite this, the failures observed are very significant since they highlight serious flaws in the prime RNG implemented. Although it is hard to give a conclusive reason for this result, a strong candidate is the aforementioned lack of RE layer. The temporal correlations introduced by the TIA and the classical noise floor clearly manifest themselves on the prime number sequences obtained since, as previously verified, the prime-searching algorithm is unable to suppress them. In this way, it would be important to reassess these figures after implementing this essential step. Moreover, additional data should be gathered to allow more extensive statistical validation. This would allow us to conclusively determine the viability of the implemented vacuum-based QRNG for prime number generation.

4. Conclusions

In conclusion, we have implemented a probabilistic prime quantum number generation scheme based on homodyne measurements of vacuum fluctuations passed through a set of 24 Miller–Rabin primality tests. For a prime length of 512 bits, we expect a theoretical maximum throughput of 11.6 M primes per second with a probability of outputting a composite number of only 3.55×10^{-15} . By removing the QS, a second classical generation scheme based on electronic noise was obtained, and the two schemes were compared. Although the overall number of primes does not depend on the noise source chosen, the quantum scheme clearly outperforms the CS at small prime generation. For the set of 32-bit primes, increases in the diversity of primes up to 585.0% are shown, which cannot be explained by the bias of the input distribution. In fact, the quantum source was shown to yield approximately 5% of all possible prime outcomes, outperforming the classical RNG by an order of magnitude. Moreover, we revealed that strong biases in the input distribution are clearly reflected in the prime output distribution, and although these differences are less prominent for larger lengths, the output distributions were also shown to consistently improve for the QS. Finally, a novel length-agnostic statistical test for prime number sequences based on establishing interval bounds for the expected frequency of measurements in an equiprobable binning of the prime distribution was proposed and applied to the output of the uniformized sources. Using the known bounds for the prime-counting function, the proportion of prime numbers below any given threshold can be bounded such that observations outside this range are witnesses of an unbalanced prime distribution. This approach allows the direct validation of a sequence of prime numbers with arbitrary length instead of relying on assessing the underlying RNG, which would not consider potential biases introduced by the prime-searching algorithm. This analysis was able to reveal the underlying correlations in the prime output of both sources, which remain present due to the lack of a RE layer. The resultant binary sequences thus conclusively fail the tests contained in the NIST statistical test suite, with only 86.96% and 45.34% of the evaluations being, respectively, passed by the QS and CS. In fact, out of the 161 evaluations applied, the

QS source passed 140 tests, whereas the CS had a pass rate of 73. This nevertheless shows a significant difference between the two cases. Finally, to improve the statistical significance of this analysis, it would be important to gather additional datasets for each of the cases considered. This would allow us to more precisely estimate the key merit figures by establishing their respective confidence intervals, as well as apply a more extensive statistical validation. Moreover, to conclusively validate the viability of the vacuum-based implementation, it is fundamental to reassess all these cases after implementing the required RE stage.

Author Contributions: Conceptualization, M.J.F., N.J.M. and N.A.S.; 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, M.J.F., N.J.M., N.A.S. and A.N.P. 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 project QuantumPrime (PTDC/EEI-TEL/8017/2020) and UIDB/50008/2020-UIDP/50008/2020. M. Ferreira also acknowledges the 2022.09584.BD PhD grant from FCT.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

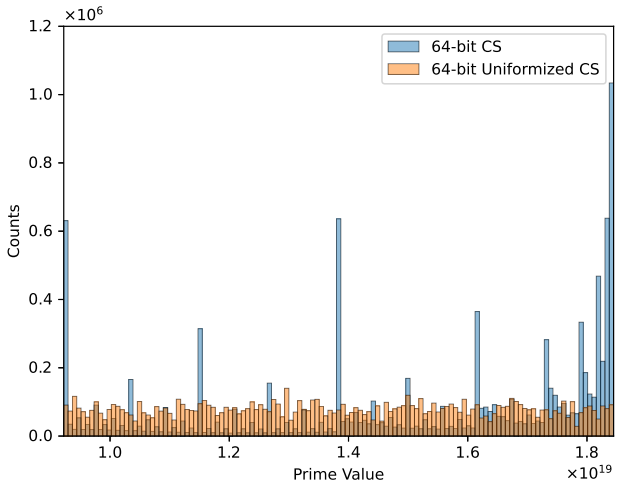
Data Availability Statement: The datasets presented in this study are available on request from the corresponding author. The data are not publicly available due to the privacy of follow-up studies.

Acknowledgments: The authors would like to thank André Carvalho for his assistance in the implementation of the software, and Mariano Lemus for his valuable comments and suggestions.

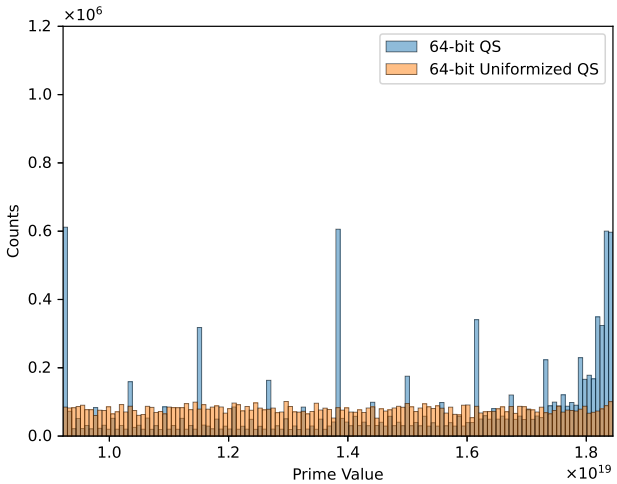
Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Statistical Validation

This appendix presents the output prime distributions and autocorrelation analyses for increasing prime lengths from the statistical validation discussed in Sections 3.3 and 3.4 that were not included in the main text. Figures A1 and A2 show the respective results.



(**a**)



(**b**)

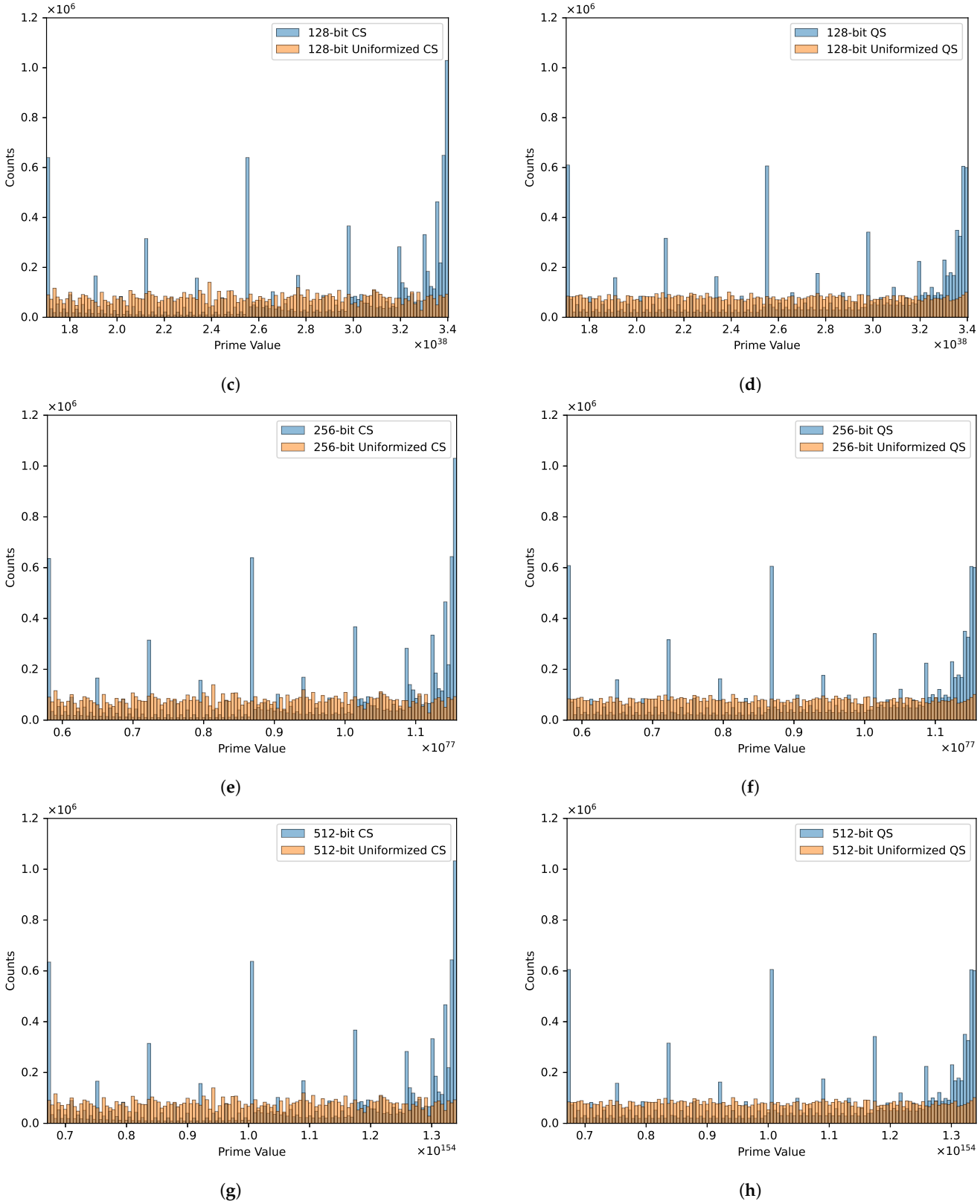


Figure A1. Output distribution of 10 M prime numbers for the (**a**) 64-bit CS, (**b**) 64-bit QS, (**c**) 128-bit CS, (**d**) 128-bit QS, (**e**) 256-bit CS, (**f**) 256-bit QS, (**g**) 512-bit CS, and (**h**) 512-bit QS. In each case, the uniformized source was also represented.

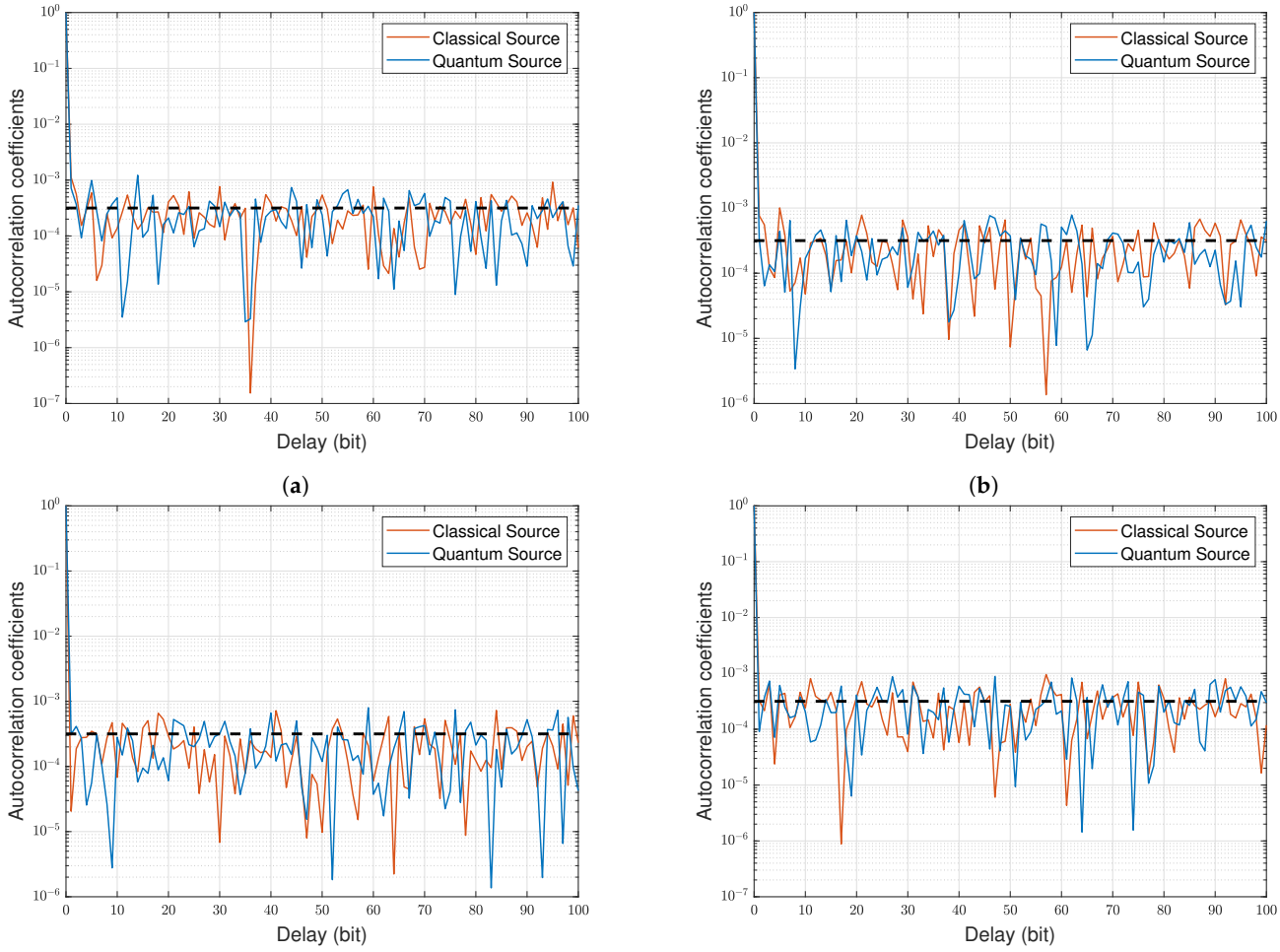


Figure A2. Autocorrelation coefficients for 10 M threshold values for the uniformized (**a**) 64-bit, (**b**) 128-bit, (**c**) 256-bit, and (**d**) 512-bit sources. For each case, both the CS and QS are represented and the dashed line represents the theoretically expected standard deviation.

Appendix B. Results from NIST's Statistical Test Suite

This appendix summarizes the results of the randomness tests from the NIST statistical test suite [1], which are represented in Table A1.

Table A1. NIST's statistical test suite results for the default $\alpha = 0.01$ and a data size of 100 Mbit (100 bit streams of 1 Mbit). The minimum pass rate is 96/100 and, when multiple values exist, the smallest is represented. For tests with multiple *p*-values, a Kolmogorov-Smirnov (KS) test was applied to obtain a representative value.

Statistical Test	Uniformized CS			Quantum QS		
	p-Value	Proportion	Result	*p*-Value	Proportion	Result
Frequency	0.000000	0/100	FAILED	0.000000	0/100	FAILED
BlockFrequency	0.000000	76/100	FAILED	0.000000	93/100	FAILED
CumulativeSums	0.000000	0/100	FAILED	0.000000	0/100	FAILED
Runs	0.000000	0/100	FAILED	0.000000	0/100	FAILED
LongestRun	0.010988	97/100	PASSED	0.000082	93/100	FAILED
Rank	0.304126	99/100	PASSED	0.262249	99/100	PASSED
FFT	0.262249	98/100	PASSED	0.028817	100/100	PASSED
NonOverlappingTemplate	0.000000	31/100	FAILED	0.000000	73/100	FAILED
OverlappingTemplate	0.000000	57/100	FAILED	0.000000	81/100	FAILED
Universal	0.319084	98/100	PASSED	0.304126	98/100	PASSED
Approximate entropy	0.000000	3/100	FAILED	0.000000	90/100	FAILED
Serial	0.500000	92/100	FAILED	0.704474	100/100	PASSED
LinearComplexity	0.319084	98/100	PASSED	0.319084	99/100	PASSED

References

1. 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. In *NIST Special Publication 800-22*; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2010. [CrossRef]
2. Herrero-Collantes, M.; Garcia-Escartin, J.C. Quantum random number generators. *Rev. Mod. Phys.* **2017**, *89*, 015004. [CrossRef]
3. Chen, L.; Moody, D.; Regenscheid, A.; Robinson, A. *Digital Signature Standard (DSS)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2023. [CrossRef]
4. Richard Crandall, C.B.P. *Prime Numbers: A Computational Perspective*, 2nd ed.; Springer: Berlin/Heidelberg, Germany, 2005.
5. Sonmez, M.; Barker, E.; Kelsey, J.; McKay, K.; Baish, M.; Boyle, M. *Recommendation for the Entropy Sources Used for Random Bit Generation*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018. [CrossRef]
6. Markowsky, G. The Sad History of Random Bits. *J. Cyber Secur. Mobil.* **2014**, *3*, 1–24. [CrossRef]
7. 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]
8. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **2020**, *12*, 1012–1236. [CrossRef]
9. Kelsey, J.; Schneier, B.; Wagner, D.; Hall, C. Cryptanalytic Attacks on Pseudorandom Number Generators. In Proceedings of the Fast Software Encryption, Paris, France, 23–25 March 1998; pp. 168–188.
10. Melià-Seguí, J.; Garcia-Alfaro, J.; Herrera-Joancomartí, J. A Practical Implementation Attack on Weak Pseudorandom Number Generator Designs for EPC Gen2 Tags. *Wirel. Pers. Commun.* **2011**, *59*, 27–42. [CrossRef]
11. Truong, N.D.; Haw, J.Y.; Assad, S.M.; Lam, P.K.; Kavehei, O. Machine Learning Cryptanalysis of a Quantum Random Number Generator. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 403–414. [CrossRef]
12. Bernstein, D.J.; Lange, T.; Niederhagen, R. Dual EC: A standardized back door. In *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 256–281.
13. Hastings, M.; Fried, J.; Heninger, N. Weak keys remain widespread in network devices. In Proceedings of the 2016 Internet Measurement Conference, Santa Monica, CA, USA, 14–16 November 2016; pp. 49–63.
14. Gong, L.; Zhang, J.; Liu, H.; Sang, L.; Wang, Y. True Random Number Generators Using Electrical Noise. *IEEE Access* **2019**, *7*, 125796–125805. [CrossRef]
15. Marangon, D.G.; Vallone, G.; Villoresi, P. Random bits, true and unbiased, from atmospheric turbulence. *Sci. Rep.* **2014**, *4*, 5490. [CrossRef]
16. Hsueh, J.C.; Chen, V.H.C. An ultra-low voltage chaos-based true random number generator for IoT applications. *Microelectron. J.* **2019**, *87*, 55–64. [CrossRef]
17. Kollmitzer, C.; Schauer, S.; Rass, S.; Rainer, B. (Eds.) *Quantum Random Number Generation Theory and Practice: Theory and Practice*; Springer International Publishing: Cham, Switzerland, 2020. [CrossRef]
18. 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*, 062327. [CrossRef]
19. Guo, Y.; Cai, Q.; Li, P.; Jia, Z.; Xu, B.; Zhang, Q.; Zhang, Y.; Zhang, R.; Gao, Z.; Shore, K.A.; et al. 40 Gb/s quantum random number generation based on optically sampled amplified spontaneous emission. *APL Photonics* **2021**, *6*, 066105. [CrossRef]
20. 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]
21. Huang, M.; Chen, Z.; Zhang, Y.; Guo, H. A Phase Fluctuation Based Practical Quantum Random Number Generator Scheme with Delay-Free Structure. *Appl. Sci.* **2020**, *10*, 2431. [CrossRef]
22. Avesani, M.; Marangon, D.G.; Vallone, G.; Villoresi, P. Secure heterodyne-based quantum random number generator at 17 Gbps. *Nat. Commun.* **2018**, *9*, 1–8. [CrossRef]
23. 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]
24. 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]
25. Gehring, T.; Lupo, 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.* **2021**, *12*, 605. [CrossRef] [PubMed]
26. 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]
27. 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]
28. Bruynsteen, C.; Gehring, T.; Lupo, C.; Bauwelinck, J.; Yin, X. 100-Gbit/s Integrated Quantum Random Number Generator Based on Vacuum Fluctuations. *PRX Quantum* **2023**, *4*, 010330. [CrossRef]
29. 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]

30. 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. *Appl. Phys. Lett.* **2021**, *118*, 264001. [CrossRef]
31. Ferreira, M.J.; Silva, N.A.; Pinto, A.N.; Muga, N.J. Characterization of a Quantum Random Number Generator Based on Vacuum Fluctuations. *Appl. Sci.* **2021**, *11*, 7413. [CrossRef]
32. Liu, Y.; Yuan, X.; Li, M.H.; Zhang, W.; Zhao, Q.; Zhong, J.; Cao, Y.; Li, Y.H.; Chen, L.K.; Li, H.; et al. High-Speed Device-Independent Quantum Random Number Generation without a Detection Loophole. *Phys. Rev. Lett.* **2018**, *120*, 010503. [CrossRef] [PubMed]
33. Li, Y.; Fei, Y.; Wang, W.; Meng, X.; Wang, H.; Duan, Q.; Ma, Z. Analysis of the effects of temperature increase on quantum random number generator. *Eur. Phys. J. D* **2021**, *75*, 69. [CrossRef]
34. Ferreira, M.J.; Carvalho, A.; Silva, N.A.; Pinto, A.N.; Muga, N.J. Probable Prime Generation from a Quantum Randomness Source. In Proceedings of the 2023 23rd International Conference on Transparent Optical Networks (ICTON), Bucharest, Romania, 2–6 July 2023; pp. 1–4. [CrossRef]
35. Clavier, C.; Feix, B.; Thierry, L.; Paillier, P. Generating Provable Primes Efficiently on Embedded Devices. In Proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, 21–23 May 2012; pp. 372–389.
36. Shen, Y.; Tian, L.; Zou, H. Practical quantum random number generator based on measuring the shot noise of vacuum states. *Phys. Rev. A* **2010**, *81*, 063814. [CrossRef]
37. Haw, J.Y.; Assad, S.M.; Lance, A.M.; Ng, N.H.Y.; Sharma, V.; Lam, P.K.; Symul, T. Maximization of Extractable Randomness in a Quantum Random-Number Generator. *Phys. Rev. Appl.* **2015**, *3*, 054004. [CrossRef]
38. Dusart, P. Autour de la Fonction qui Compte le Nombre de Nombres Premiers. Ph.D. Thesis, Université de Limoges, Limoges, France, 1998.
39. Axler, C. New Estimates for the nth Prime Number. *J. Integer Seq.* **2019**, *22*, 3.