eng

MDPI

Article

A High-Quality Random Number Generator Using Multistage Ring Oscillators and Fast Fourier Transform-Based Noise Extraction

Vatanpreet Singh [1,†], Md Sakib Hasan [2,*,†] and Syed Azeemuddin [1,2]

[1] CVEST—Center for VLSI and Embedded Systems Technologies, IIIT Hyderabad (India), Hyderabad 500032, India; vatanpreet.singh@research.iiit.ac.in (V.S.); asyed@olemiss.edu (S.A.)
[2] Department of Electrical and Computer Engineering, University of Mississippi, Oxford, MS 38677, USA
* Correspondence: mhasan5@olemiss.edu
† These authors contributed equally to this work.

Abstract: Random Numbers are widely employed in cryptography and security applications. This paper presents a novel approach to generate high-quality random bitstreams by harnessing the inherent noise properties of ring oscillators. We implemented ring oscillators with varying numbers of stages (3, 5, and 7), different geometries and different startup voltages in Cadence and recorded their total output power, which includes the cumulative noise effects. Subsequently, we exported these power measurements to MATLAB, where we applied a Fast Fourier Transform (FFT)-based technique to extract the total noise characteristics for each ring oscillator. Using the obtained noise data, we generated separate random bitstreams of 10 million bits for the 3-stage, 5-stage, and 7-stage ring oscillators. The final random bitstream, consisting of 10 million bits, was created by performing a bitwise XOR operation on the bitstreams generated by each ring oscillator. The degree of randomness of the generated bitstreams was assessed using the NIST 800-22 statistical test suite. Remarkably, the final random bitstream exhibited strong robustness and suitability for cryptographic applications. This innovative approach leverages the noise properties of ring oscillators to create reliable random bitstreams, offering potential applications in secure communications and cryptography. The results highlight the feasibility of using ring oscillators as noise sources for random bit generation and underscore their effectiveness in meeting stringent randomness criteria.

Keywords: random bitstreams; true random number generator; ring oscillators; noise properties; cryptography; security applications; NIST 800-22 statistical test suite

Citation: Singh, V.; Hasan, M.S.; Azeemuddin, S. A High-Quality Random Number Generator Using Multistage Ring Oscillators and Fast Fourier Transform-Based Noise Extraction. *Eng* **2024**, *5*, 433–446. https://doi.org/10.3390/eng5010023

Academic Editor: Antonio Gil Bravo

Received: 31 December 2023
Revised: 21 February 2024
Accepted: 29 February 2024
Published: 4 March 2024

1. Introduction

With the exponential growth of connected devices, from smart homes to industrial robots, information security is becoming paramount to safeguard our data and infrastructure [1,2]. The generation of high-quality random numbers plays a pivotal role in ensuring the security and effectiveness of cryptographic algorithms and protocols. Since the inception of secret- and public-key cryptosystems, the challenge of producing reliable random numbers has been a persistent concern. In contemporary times, with the escalating computational capabilities accessible to potential attackers, the importance of addressing this issue has become more pronounced. Since the inception of computers, they have served as valuable tools for generating such numbers, initially for statistical and scientific uses [3], and subsequently for cryptographic uses [4]. However, genuinely random numbers cannot be generated through programming alone. It is necessary to acquire entropy sources, initially from peripherals as outlined by Gutmann (1998) and later through the propositions of external hardware generators as suggested by Ni et al. (2022) [5,6]. Presently, computers utilize a combination of true random number generators (TRNGs) and deterministic random bit generators (DRBGs) integrated into external chips, such as Trusted Platform

Modules (TPMs) [7]. In the context of embedded systems deployed on reconfigurable logic platforms like FPGAs or systems-on-chips, a common approach involves combining a true random number generator (TRNG) with a pseudorandom number generator (PRNG) or a deterministic random bit generator (DRBG). This combination aims to achieve a favorable balance between randomness, area resources, and power consumption. In this context, numerous designs for TRNGs [8,9] and PRNGs [10,11] intended for implementation on FPGAs have been proposed. Additional avenues for TRNG development lie in exploiting the intrinsic randomness of quantum-mechanical phenomena such as radioactive decay and particle emissions. These represent compelling alternatives due to their inherent unpredictability and cost-effective potential [12]. Among the various proposals, those utilizing ring oscillators (ROs) as entropy sources combined with XOR gates for generating the final random bitstream appear to exhibit superior statistical properties, albeit with elevated area requirements [13–15]. Presently, in the research and advancement of true random number generators (TRNGs), entropy sources can be broadly categorized into three main groups: noise [16], chaos [17], and jitter. Notably, TRNGs based on jitter are often easier to integrate and are recognized for their portable implementations, as mentioned in the literature.

Ring oscillators (ROs) have emerged as a promising source of entropy for various cryptographic and security applications. ROs have garnered significant attention due to their inherent simplicity, low power consumption, and ease of integration into integrated circuits. While manufacturing variations induce inherent differences in RO frequencies between different devices, further randomness is introduced by a phenomenon known as jitter. Jitter refers to the short-term deviations in the period of the oscillation signal, arising from various noise sources which include thermal noise, power supply noise, and flicker noise.

This work's primary contributions include the following:

- A novel approach to generate true random numbers using a noise-based XOR combination of different multistage ring oscillators (MROs) with varying geometries and startup voltages (3, 5, and 7 stages). This approach helps mask potential periodicities or biases which existed in individual MRO outputs, leading to a more robust and unpredictable random number sequence.
- Evaluation and validation of the level of randomness in TRNG implementations using the guidelines outlined in the NIST 800-22 standard recommendation. This ensures that the generated random numbers are suitable for cryptographic applications by passing a battery of tests designed to detect non-randomness.
- Demonstrate that the combination of 3-, 5-, and 7-stage MROs with distinct geometries and startup voltages achieves the optimal balance between randomness and throughput. This finding provides valuable insights for designing MRO-based TRNGs for specific applications.

To guide the reading of this document, Section 2 outlines the proposed TRNG architecture, focusing on its design principles and implementation details. The key components of the TRNG, including the noise source, ring oscillators, and post-processing stages, are described in detail. Section 3 delves into the entropy analysis of the generated random numbers. The statistical randomness of the TRNG output is evaluated using NIST statistical tests, providing quantitative assessment of its compliance with randomness standards. It also discusses the key findings and insights gained from the experimental results. The impact of different TRNG configurations on entropy and randomness characteristics is thoroughly examined. Finally, Section 4 summarizes the main conclusions drawn from the study. The overall performance of the proposed TRNG is evaluated, highlighting its strengths and limitations. Future research directions and potential improvements are also outlined.

2. Multistage Ring Oscillator-Based TRNG Design and Implementation

Ring oscillators, with their simple architecture and inherent sensitivity to process variations, have become the de facto standard for monitoring gate delay and speed power

products of fabricated MOS inverters in silicon foundries. Composed of an odd number of identical CMOS inverters arranged in a closed loop, these negative feedback circuits exhibit unstable behavior, oscillating at a frequency directly proportional to the sum of individual gate delays. This ubiquitous application highlights the ring oscillator's unique ability to offer a fast, non-invasive, and highly accurate assessment of process integrity and device performance, making it an indispensable tool for ensuring the quality and efficiency of modern integrated circuits [18].

Ring oscillators comprise multiple delay cells, which can be either single-ended (conventional inverter) or of a differential type (differential pair). Oscillators utilizing differential delay cells demonstrate enhanced immunity to power supply and substrate noises, while single-ended counterparts can attain reduced phase noise for a given power dissipation. The optimal choice between differential and single-ended delay cells depends on the specific application and environment. For TRNGs demanding high randomness quality, the lower phase noise of single-ended cells may be preferred, even if it comes at the cost of increased noise sensitivity. This aligns with the decision in our proposed TRNG architecture to utilize single-ended delay cells. A single-ended ring oscillator is influenced by two primary noise sources: thermal noise and flicker noise. These noise sources exhibit distinct behaviors, and their impact on the oscillator's performance varies.

1. Thermal noise: Thermal fluctuations within the circuit elements contribute to random variations in their delays, leading to jitter. The channels of MOS transistors within the inverter exhibit resistive characteristics, leading to the generation of thermal noise, which is modeled as follows [19]:

$$\overline{i_n^2} = 4kTg_{ds0}\gamma \tag{1}$$

where i_n^2 is the average noise power in A^2/Hz; k represents the Boltzmann constant (1.38×10^{23} J/K); T is the absolute value of temperature; g_{ds0} is the drain source conductance with drain source voltage, V_{DS} = 0; and γ is the thermal drain noise coefficient (1 to 3 for short channel devices and 2/3 for long channel device [20]).

2. Flicker noise: This low-frequency noise arises from various phenomena within the transistors and manifests as long-term variations in the oscillation period. It constitutes the primary source of noise in MOS transistors at lower frequencies. The flicker noise can be modeled as follows:

$$v_n^2 = \frac{K}{WLC_{ox}f} \tag{2}$$

where K $\approx 10^2 4\ V^2F$ is a process-dependent constant; W is the gate width; L is the channel length; C_{ox} is the gate oxide capacitance per unit area; and f is the frequency of interest.

Figure 1 illustrates the three distinct entropy sources—three-stage, five-stage, and seven-stage ring oscillators—and their integration within the TRNG architecture. The figure also depicts the power spectrum analysis using Cadence, the FFT-based noise power extraction in MATLAB 2022a, and the bitwise XOR operation for generating the combined random bit sequence.

This study presents an innovative TRNG architecture that leverages a multistage ring oscillator to extract randomness from the inherent chaos of electronic circuits. While manufacturing variations induce inherent differences in RO frequencies between different devices, further randomness is introduced by a phenomenon known as jitter. Jitter refers to the short-term deviations in the period of the oscillation signal, arising from various noise sources [21] mentioned earlier.

The random nature of the jitter makes it a valuable source of entropy, which can be extracted by combining ROs with additional circuitry, and post-processing techniques can yield robust TRNGs that produce high-quality random numbers. The proposed design meticulously combines three distinct entropy sources—three-stage, five-stage, and seven-stage ring oscillators—to generate a symphony of random bits. To harness the individual characteristics of each entropy source, the total output power from the ring oscillators is

meticulously analyzed using Cadence, a leading electronic design automation platform. Subsequently, a judiciously applied FFT-based algorithm in MATLAB extracts the total noise power from this power spectrum, providing a rich source of randomness. Distinct bit sequences are then generated using a comparator, producing separate streams of 10 million bits for each ring oscillator. Remarkably, a new sequence of 10 million bits is ingeniously crafted through a bitwise XOR operation performed on the three independent 10 million bitstreams, effectively weaving the unique characteristics of each entropy source into a single, robust random sequence.

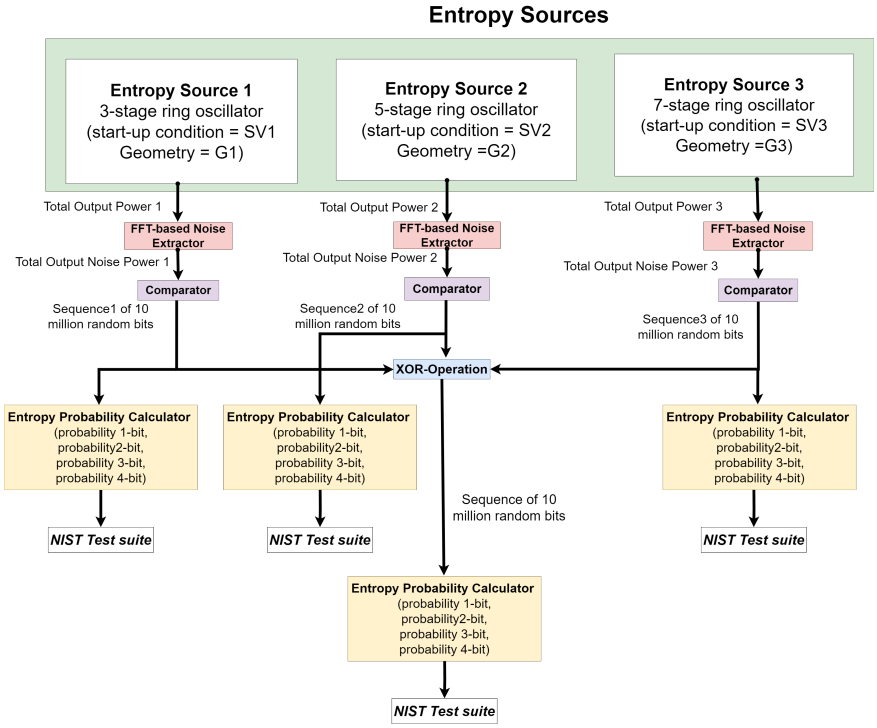

Figure 1. Architecture of the proposed TRNG employing a multistage ring oscillator.

The resultant bit sequences undergo rigorous scrutiny, subjected to comprehensive entropy calculations and NIST statistical randomness tests. This meticulous evaluation ensures that the generated random bits possess the requisite level of unpredictability and robustness, meeting the stringent standards of cryptographic applications. In essence, this TRNG design not only harnesses the distinct characteristics of multiple entropy sources, but also meticulously evaluates the generated random bits, ensuring their reliability and unpredictability. This innovative approach paves the way for the development of highly secure and reliable TRNGs, safeguarding the integrity of cryptographic systems and the confidentiality of sensitive data.

2.1. Three-Stage Ring Oscillator

Ring Oscillators, characterized by a feedback loop connecting an odd number of inverters, generate oscillations through a combination of phase shift (2π per stage) and gain in each stage, satisfying the Barkhausen criteria. While offering basic oscillation capabilities, their fixed phase shift per stage (π/N, where N is the number of stages) and reliance on DC inversion for the remaining phase shift limit their tuning range and noise sensitivity. These limitations also render conventional ring VCOs more susceptible to various noise sources, including phase noise, supply sensitivity, and common-mode rejection, compared to other VCO topologies [22].

Figure 2 presents the schematic of the three-stage ring oscillator used in the design [23]. Below are the design parameters considered for the three-stage ring oscillator:

$$(W/L)_1 = 240\ \text{nm}/180\ \text{nm} \tag{3}$$

$$V_{out}(t = 0) = 1.5\ \text{V} \tag{4}$$

$$V_{DD} = 1.8\ \text{V} \tag{5}$$

$$C_1 = 1\ \text{pF} \tag{6}$$

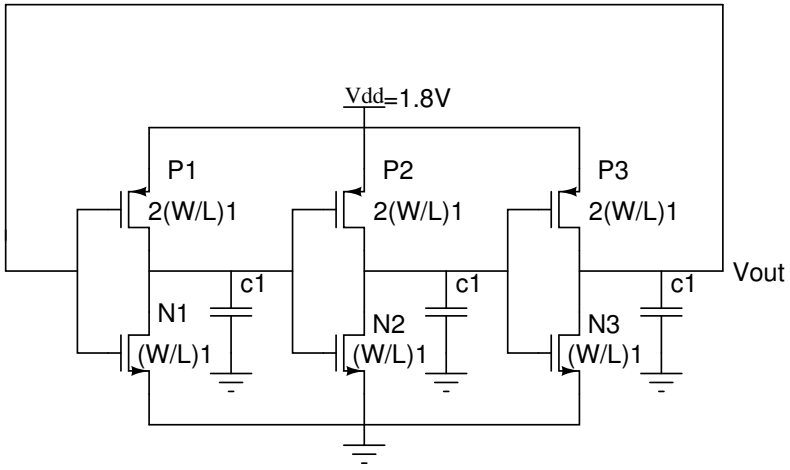

Figure 2. Schematic of three-stage ring oscillator.

Mathematically, static and dynamic power is expressed as

$$P_s = V_{cc} I_{cc} \tag{7}$$

$$P_d = C_{pd} V_{cc}^2 f_i N_{sw} + C_L V_{cc}^2 f_o N_{sw} \tag{8}$$

where V_{cc} represents the supply voltage, I_{cc} is the current flow into a device, C_{pd} denotes the dynamic power dissipation capacitance, f_i is the input signal frequency, f_o represents the output signal frequency, C_L is the external capacitance, and N_{sw} represents the number of bits switching.

By employing Equations (7) and (8), Figure 3 presents the total output power of the three-stage ring oscillator, with a peak value of 350 microwatts.

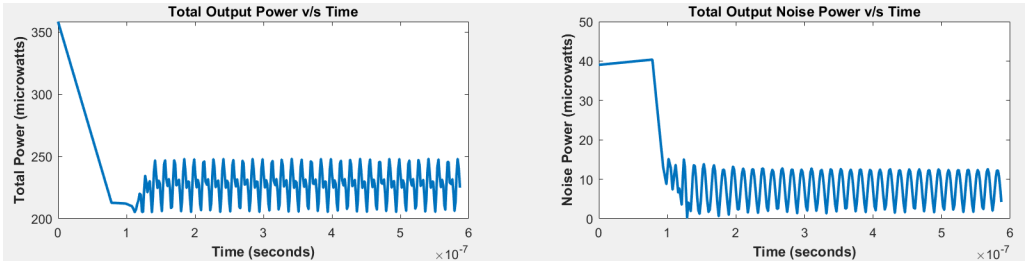

Figure 3. Total output power and noise power for a three-stage ring oscillator.

2.2. Five-Stage Ring Oscillator

Figure 4 presents the schematic of the five-stage ring oscillator used in the design. Below are the design parameters considered for the five-stage ring oscillator:

$$(W/L)_1 = 350\ \text{nm}/180\ \text{nm} \tag{9}$$

$$V_{out}(t = 0) = 0.8\ \text{V} \tag{10}$$

$$V_{DD} = 1.8 \text{ V} \tag{11}$$

$$C_1 = 1 \text{ pF} \tag{12}$$

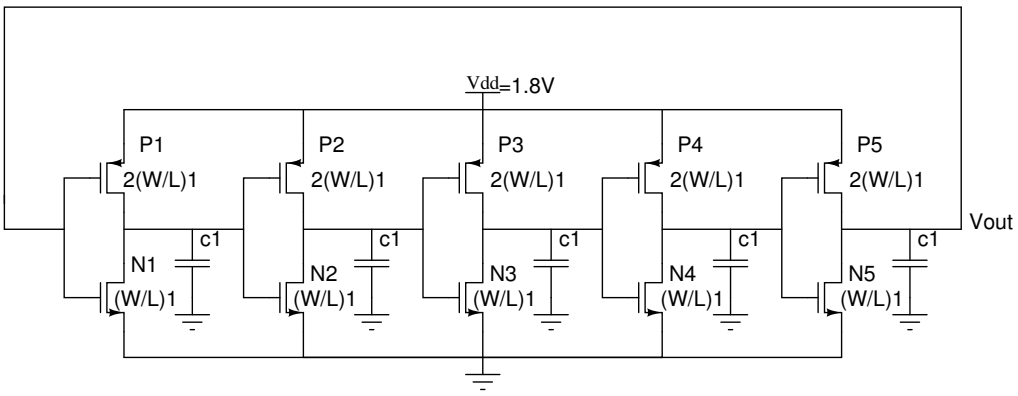

Figure 4. Schematic of five-stage ring oscillator.

Employing Equations (7) and (8), Figure 5 presents the total output power of the five-stage ring oscillator, with a peak value of 220.8 microwatts.

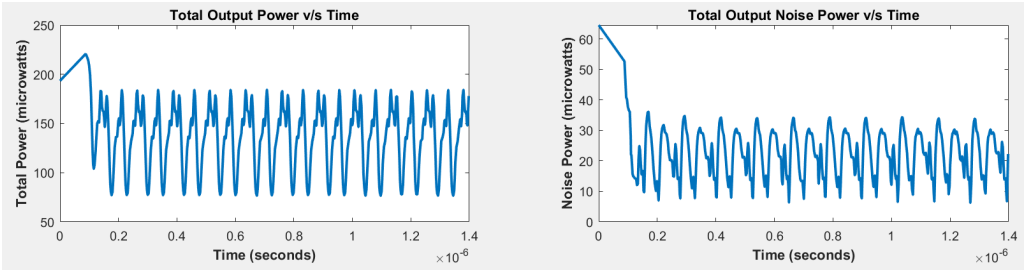

Figure 5. Total output power and noise power for a five-stage ring oscillator.

2.3. Seven-Stage Ring Oscillator

Figure 6 presents the schematic of the seven-stage ring oscillator used in the design. Below are the design parameters considered for the seven-stage ring oscillator:

$$(W/L)_1 = 460 \text{ nm}/180 \text{ nm} \tag{13}$$

$$V_{out}(t = 0) = 1.15 \text{ V} \tag{14}$$

$$V_{DD} = 1.8 \text{ V} \tag{15}$$

$$C_1 = 1 \text{ pF} \tag{16}$$

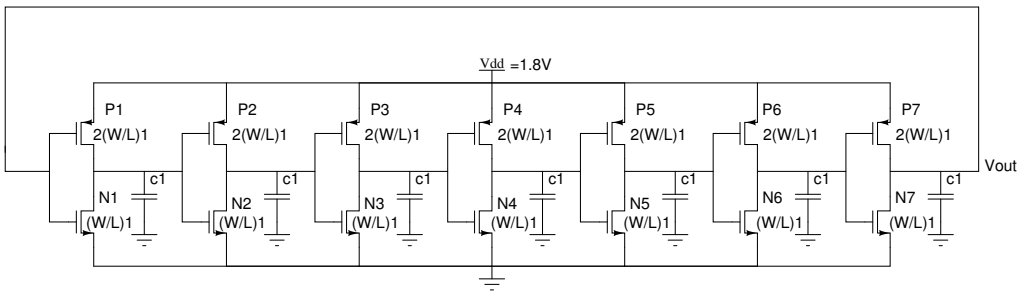

Figure 6. Schematic of seven-stage ring oscillator.

Employing Equations (7) and (8), Figure 7 presents the total output power of the seven-stage ring oscillator, with a peak value of 619 microwatts.

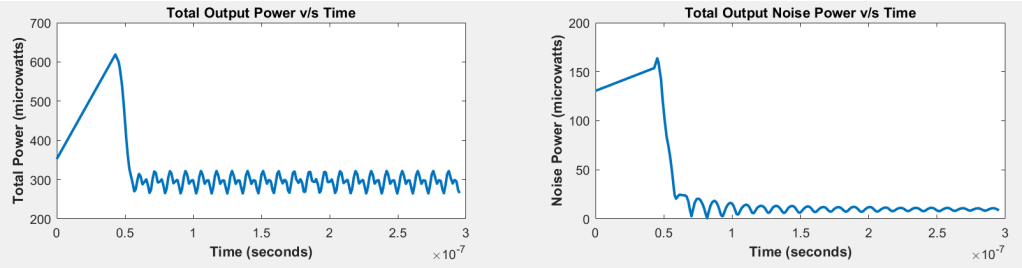

Figure 7. Total output power and noise power for a seven-stage ring oscillator.

2.4. FFT-Based Noise Extractor

The Fast Fourier Transform (FFT) is a powerful tool used for signal analysis in various fields like audio processing, image processing, and telecommunications. One of its significant applications is in extracting noise from signals [24]. The algorithm for FFT-based noise extraction is as below [25]:

1. Convert the signal from the time domain (amplitude vs. time) to the frequency domain (amplitude vs. frequency) using FFT. This provides a clear view of the signal's frequency content:

$$X[K] = \sum_{n=0}^{N-1} x[n] W_N^{nK} \tag{17}$$

where $x[n]$ is the discrete time domain output power signal, K is a frequency component, $W_N = e^{-i2\pi/N}$, and $N = 100 \times 10^6$.

2. Noise usually appears as high-frequency components in the frequency domain, while the desired signal occupies lower frequencies. Analyzing the power spectrum (distribution of power across frequencies) helps identify these noise frequencies. Mathematically, the noise spectrum is defined as

$$X_1[K] = 0 \text{ if } \mathrm{K} < K_1 \tag{18}$$

$$= \mathrm{X[K]} \text{ if } \mathrm{K} \geq K_1 \tag{19}$$

The value of K_1 is decided to be 70×10^6, 60×10^6, and 80×10^6 for three-, five-, and seven-stage ring oscillators, respectively, while keeping the maximum value of K as 100×10^6.

3. Then, perform an inverse Discrete Fourier Transform to convert the noise spectrum back to the time domain. This results in a noise signal in time domain:

$$x_1[n] = \frac{1}{N} \sum_{K=0}^{N-1} X_1[K] W_N^{-nK} \tag{20}$$

where $x_1[n]$ is the noise signal in time domain, K is a frequency component, $W_N = e^{-i2\pi/N}$, and $X_1[K]$ is a noise spectrum.

Figures 3, 5 and 7 show the noise power in time domain for three-, five-, and seven-stage ring oscillators, respectively. Maximum noise power for three-, five-, and seven-stage ring oscillators is reported to be 40, 64, and 163 microwatts, respectively.

2.5. Post-Processing

The proposed post-processing algorithm comprises three main stages:

Stage 1: Downsampling

The initial step involves downsampling the input sequence of 100 million analog values by a factor of 5. This reduces the data size to a manageable 20 million analog values, alleviating computational complexity and improving processing efficiency.

Stage 2: Comparator

The downsampled 20 million analog values are then divided into two groups of 10 million each. The first group represents the original analog values, while the second group comprises the analog values at even positions. A comparison is performed between each pair of corresponding values from the two groups. If the analog value at the first position exceeds the analog value at the second position, a '1' is output; otherwise, a '0' is output.

Stage 3: Random Bitstream Generation and XOR Operation

Separately, three random bitstreams of 10 million bits each are generated for three-, five-, and seven-stage ring oscillators. These bitstreams are then combined using an exclusive-OR (XOR) operation to produce a final random bitstream of 10 million bits.

The post-processing algorithm enhances the overall randomness of the final random bitstream, as evidenced by the results presented in Tables 1 and 2. It renders the generated random numbers more suitable for cryptographic applications.

Table 1. Entropy and probability calculations.

Parameter	3-Stage	5-Stage	7-Stage	XOR
P(0)	48.9800	50.0319	53.0404	49.9856
P(1)	51.0200	49.9681	46.9596	50.0144
H(A)	0.9997	1.0000	0.9973	1.0000
P(00)	17.0464	21.7931	28.8902	24.9983
P(01)	31.9336	28.2388	24.1502	24.9872
P(10)	31.9336	28.2388	24.1502	24.9872
P(11)	19.0864	21.7292	22.8094	25.0272
H(B)	1.9429	1.9879	1.9940	2.0000
P(000)	5.4355	6.9194	17.1509	12.4973
P(001)	11.6109	14.8737	11.7393	12.5011
P(010)	20.0756	15.9456	13.6319	12.4656
P(011)	11.8580	12.2932	10.5184	12.5217
P(100)	11.6109	14.8737	11.7393	12.5011
P(101)	20.3227	13.3651	12.4109	12.4861
P(110)	11.8580	12.2932	10.5184	12.5217
P(111)	7.2284	9.4360	12.2910	12.5055
H(C)	2.8855	2.9597	2.9826	3.0000
P(0000)	0.6112	1.3428	6.8250	6.1881
P(0001)	4.8243	5.5766	10.3258	6.3092
P(0010)	7.0283	6.8265	3.9519	6.1957
P(0011)	4.5826	8.0472	7.7874	6.3054
P(0100)	6.2776	7.4559	7.8502	6.1887
P(0101)	13.7981	8.4897	5.7816	6.2769
P(0110)	6.1326	5.4613	1.1004	6.2261
P(0111)	5.7253	6.8320	9.4180	6.2956
P(1000)	4.8243	5.5766	10.3258	6.3092
P(1001)	6.7866	9.2971	1.4135	6.1919
P(1010)	13.0473	9.1191	9.6800	6.2698
P(1011)	7.2753	4.2460	2.7310	6.2163
P(1100)	5.3334	7.4178	3.8891	6.3124
P(1101)	6.5246	4.8754	6.6293	6.2093
P(1110)	5.7253	6.8320	9.4180	6.2956
P(1111)	1.5031	2.6041	2.8730	6.2099
H(D)	3.7998	3.8994	3.7950	4.0000

Table 2. NIST-800 statistical test results for XOR of three-,five-, and seven-stage ring oscillators.

Test Name	*p*-Value	Pass Rate	Result
Frequency	0.066882	10/10	Passed
Block Frequency	0.350485	10/10	Passed

Table 2. *Cont.*

Test Name	*p*-Value	Pass Rate	Result
Cumulative Sums	0.066882	10/10	Passed
Runs	0.122325	9/10	Passed
Longest Run	0.534146	10/10	Passed
Binary Matrix Rank	0.350485	9/10	Passed
Non-Overlapping	0.739918	10/10	Passed
Overlapping	0.534146	9/10	Passed
Universal Statistical	0.534146	10/10	Passed
Approximate Entropy	0.350485	10/10	Passed
Random Excursions	0.911413	10/10	Passed
Random Excursions Variant	0.534146	10/10	Passed
Serial	0.122325	10/10	Passed
Linear Complexity	0.350485	10/10	Passed

2.6. Entropy and Probability Calculator

In the realm of information theory, entropy serves as a crucial metric, quantifying the average uncertainty associated with a random variable. When dealing with random bitstreams, the concept of entropy becomes particularly relevant, offering insights into the inherent information content within the data [26].

In essence, entropy measures the degree of randomness or unpredictability in a bitstream. It reflects the average amount of information per bit required to accurately predict the next bit in the sequence. The higher the entropy, the more unpredictable and information-rich the bitstream is, and vice versa [27,28]. One-bit probability numbers are calculated using the mathematical formula below:

$$P(A) = \frac{\text{number of pattern “A” in bitstream}}{\text{total number of bits}} \tag{21}$$

where A = 0, 1.

Two-bit probability numbers are calculated using the mathematical formula below:

$$P(B) = \frac{\text{number of pattern “B” in bitstream}}{\text{total number of bits}/2} \tag{22}$$

where B = 00, 01, 10, 11.

Three-bit probability numbers are calculated using the mathematical formula below:

$$P(C) = \frac{\text{number of pattern “C” in bitstream}}{\text{total number of bits}/3} \tag{23}$$

where C = 000, 001, 010, 011, 100, 101, 110, 111.

Four-bit probability numbers are calculated using the mathematical formula below:

$$P(D) = \frac{\text{number of pattern “D” in bitstream}}{\text{total number of bits}/4} \tag{24}$$

where D = 0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1111.

The entropy of a random bitstream refers to the average amount of information per bit contained within the stream. It is measured in bits per bit (bit/bit). For the good degree of randomness, generated random bitstreams should have a uniform distribution.

Entropy for one-bit distribution is defined as

$$H(A) = -\sum_{A=0}^{A=1} P(A) \log_{10} P(A) \tag{25}$$

For uniform distribution, $P(A)$ and $H(A)$ should be close to 0.5 and 1, respectively. Entropy for two-bit distribution is defined as

$$H(B) = -\sum_{B=00}^{B=11} P(B) \log_{10} P(B) \tag{26}$$

For uniform distribution, $P(B)$ and $H(B)$ should be close to 0.25 and 2, respectively. Entropy for three-bit distribution is defined as

$$H(C) = -\sum_{C=000}^{C=111} P(C) \log_{10} P(C) \tag{27}$$

For uniform distribution, $P(C)$ and $H(C)$ should be close to 0.125 and 3, respectively. Entropy for four-bit distribution is defined as

$$H(D) = -\sum_{D=0000}^{D=1111} P(D) \log_{10} P(D) \tag{28}$$

For uniform distribution, $P(D)$ and $H(D)$ should be close to 0.0625 and 4, respectively.

2.7. NIST-800 Statistical Randomness Tests

The NIST Test Suite comprises 15 statistical tests designed to evaluate the randomness of binary sequences produced by cryptographic random or pseudorandom number generators, whether they are hardware- or software-based [29,30]. These tests focus on various forms of non-randomness that may be present in a sequence and include decomposable subtests. The 15 tests are as follows:

1. Frequency (Monobit) Test;
2. Block Frequency;
3. Cumulative Sums;
4. Runs;
5. Longest Runs;
6. Binary Matrix Rank;
7. Non-Overlapping;
8. Overlapping;
9. Universal Statistical;
10. Approximate Entropy;
11. Random Excursions;
12. Random Excursions Variant;
13. Serial;
14. Linear Complexity;
15. Discrete Fourier Transform (Spectral) Test.

p-values play a pivotal role in interpreting the results of NIST-800 randomness tests. They provide a quantitative measure of how likely it is to observe a test statistic as extreme as the one obtained, assuming the null hypothesis (hypothesis of randomness) is true. Understanding the significance of *p*-values is crucial for drawing accurate conclusions about the randomness of a bit sequence.

1. A low *p*-value (generally less than 0.01) indicates that the observed deviation from randomness is unlikely to be due to chance alone. This suggests that the null hypothesis (randomness) should be rejected, and the bit sequence is likely non-random.

2. A high *p*-value (generally greater than 0.05) suggests that the observed deviation from randomness can be easily attributed to chance. This allows us to accept the null hypothesis and consider the bit sequence to be sufficiently random.

3. TRNG: Randomness Statistical Assessment and Entropy Source Validation

3.1. Comparitive Study of Entropy and Probability Numbers

Table 1 presents the probabilities of generating one, two, three, and four bits, as well as the entropy, for three different cases: three-, five-, and seven-stage ring oscillators, and the XOR of three bits using Equations (21)–(28). The entropy is a measure of the randomness of the system, and a higher entropy value indicates a more random system. The XOR of three bits also has a high entropy, which is due to the nonlinear nature of the XOR operation. The XOR operation can produce unpredictable outputs, even if the inputs are known. The following are the observations from the data in Table 1:

1. The entropy of the three-stage ring oscillator deviates significantly from the ideal values for two, three, and four bits. Therefore, three-stage ring oscillator alone is not an ideal candidate for the true random number generator. Therefore, there is no need to run NIST-800 tests for this case.
2. The five-stage ring oscillator exhibits a substantial difference from the ideal entropy for two, three, and four bits. Therefore, five-stage ring oscillator alone is not an ideal candidate for the true random number generator. Therefore, there is no need to run NIST-800 tests for this case.
3. The seven-stage ring oscillator, while closer to the ideal values, still falls short for three and four bits. Therefore, seven-stage ring oscillator alone is not an ideal candidate for the true random number generator. Therefore, there is no need to run NIST-800 tests for this case.
4. The XOR operation of the three-, five-, and seven-stage ring oscillators achieves the ideal entropy values for all four bits. Therefore, this combination is an ideal choice for the true random number generator (TRNG). Thus, NIST-800 tests will be run for this case.

The analysis of the three stages of ring oscillators (3-, 5-, and 7-stage) revealed that their individual entropy values deviated from ideal values for specific bit combinations. The 3-stage oscillator significantly diverged for 2, 3 and 4 bits, the 5-stage oscillator showed substantial deviations for 2, 3, and 4 bits, and the 7-stage oscillator, while closer to ideal, still exhibited a slight discrepancy for 3 and 4 bits. These deviations suggest that individual ring oscillators, despite their simplicity, lack sufficient randomness for secure TRNG applications.

However, a remarkable observation emerged when combining all the ring oscillators with an XOR operation. This combined setup achieved perfect entropy values for one, two, three, as well as four bits, significantly exceeding the performance of individual oscillators. This synergistic effect demonstrates that the XOR's nonlinear behavior effectively cancels out periodicities or biases present in the individual ring oscillator outputs, leading to a highly random bit sequence.

3.2. NIST-800 Statistical Randomness Tests

The results of the NIST-800 statistical randomness tests for the XOR of three-, five-, and seven-stage ring oscillators with a total number of bitstreams of 10 and the length of each bistream as 1 million bits, presented in Table 2, demonstrate the strong random properties of the generated bitstreams. With the exception of the Fast Fourier Transform (FFT) test, all fourteen test cases were successfully passed. This exceptional performance highlights the effectiveness of the XOR operation in enhancing the randomness of the bitstreams. The successful completion of these tests provides confidence in the suitability of these ring oscillators for applications requiring high-quality random number generation.

The inherent randomness of the ring oscillators stems from their chaotic nature, which arises from the nonlinear interactions between the individual stages. The XOR operation further enhances this randomness by introducing additional nonlinearities and eliminating any potential correlations between the bitstreams generated by the individual ring oscillators. The noise resulting from the simulation of the ring oscillator has a periodic oscillation, which leads to the failure of the FFT test. We think that the actual hardware chip will have

more stochastic and aperiodic noise, which will solve this problem. Future work needs to involve the hardware implementation to verify this hypothesis.

These findings have significant implications for the development of secure and reliable cryptographic systems. Random number generators are essential components of cryptographic algorithms, and their quality directly impacts the security of the overall system. The strong random properties of the XOR'd bitstreams generated by these ring oscillators make them well suited for use in cryptographic applications, where high-quality randomness is crucial for ensuring the confidentiality, integrity, and authenticity of sensitive information.

4. Conclusions

The results of this study demonstrated that ring oscillators, miniature circuits whose chaotic oscillations offer a promising source of unpredictable data, have emerged as potential candidates for true random number generators (TRNGs). However, individual ring oscillators often exhibit limitations in their randomness, making them unsuitable for critical security applications. This study has demonstrated the effectiveness of a novel approach that utilizes a combination of multiple-ring oscillators with diverse geometries and startup voltages. Individually, each oscillator exhibits a unique chaotic behavior due to its distinct physical layout and initial bias. Combining these diverse voices through an XOR operation unlocks a new level of randomness. We analyzed the probabilities of generating one, two, three, and four bits and calculated the entropy for each case. None of the three types of ring oscillators alone demonstrated ideal entropy values for all four bits, indicating their inadequacy as standalone TRNGs. However, the XOR operation of these three types of ring oscillators achieved ideal entropy values for all four bits, suggesting its potential as a robust TRNG. The NIST-800 statistical randomness tests have conclusively demonstrated the effectiveness of the XOR operation in enhancing the randomness of bitstreams generated by ring oscillators. With the successful completion of fourteen out of fifteen test cases, the XOR'd bitstreams exhibited strong random properties, highlighting the effectiveness of this approach. Future work needs to involve the hardware implementation of this TRNG approach. The future of multiple-ring oscillator TRNGs lies in enhancing their capabilities through integration with PUFs, exploring dynamic XOR configurations, extending to diverse platforms, developing advanced post-processing techniques, designing lightweight architectures, investigating novel topologies, utilizing machine learning for entropy estimation, seeking standardization, and continuously evaluating against emerging threats. Additionally, integrating them with quantum-resistant cryptography paves the way for future-proof secure systems.

Author Contributions: Conceptualization, V.S., M.S.H. and S.A.; Methodology, V.S. and M.S.H.; Software, V.S.; Validation, V.S.; Resources, S.A.; Writing—original draft, V.S.; Writing—review & editing, V.S. and M.S.H.; Visualization, M.S.H. and S.A.; Supervision, S.A.; Project administration, S.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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. The data are not publicly available due to security reasons.

Acknowledgments: We thank Madhav Pulipati from AMPICQ, Hyderabad, who gave the initial idea and support for this journal.

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

Abbreviations

The following abbreviations are used in this manuscript:

FPGA	Field Programmable Gate Arrays
VCO	Variable Controlled Oscillator
TRNG	True Random Number Generator
FFT	Fast Fourier Transform
NIST	National Institute of Standards and Technology
RO	Ring Oscillator
ROs	Ring Oscillators
MRO	Multistage Ring Oscillator
PUF	Physical Unclonable Function
SV1	Start Up Voltage 1
SV2	Start Up Voltage 2
SV3	Start Up Voltage 3
G1	Geometry 1
G2	Geometry 2
G3	Geometry 3

References

1. Rostami, M.; Koushanfar, F.; Karri, R. A primer on hardware security: Models, methods, and metrics. *Proc. IEEE* **2014**, *102*, 1283–1295. [CrossRef]
2. Nannipieri, P.; Di Matteo, S.; Baldanzi, L.; Crocetti, L.; Belli, J.; Fanucci, L.; Saponara, S. True random number generator based on Fibonacci-Galois ring oscillators for FPGA. *Appl. Sci.* **2021**, *11*, 3330. [CrossRef]
3. Parrilla, L.; García, A.; Castillo, E.; López-Villanueva, J.A.; Meyer-Baese, U. Revisiting Multiple Ring Oscillator-Based True Random Generators to Achieve Compact Implementations on FPGAs for Cryptographic Applications. *Cryptography* **2023**, *7*, 26. [CrossRef]
4. Şarkışla, M.A.; Ergün, S. An area efficient true random number generator based on modified ring oscillators. In Proceedings of the 2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Chengdu, China, 26–30 October 2018; IEEE: Piscataway Township, NJ, USA; pp. 274–278.
5. Gutmann, P. Software Generation of Practically Strong Random Numbers. In Proceedings of the Usenix Security Symposium, San Antonio, TX, USA, 26–29 January 1998.
6. Ni, T.; Peng, Q.; Bian, J.; Yao, L.; Huang, Z.; Yan, A.; Wen, X. MRCO: A Multi-ring Convergence Oscillator-based High-Efficiency True Random Number Generator. In Proceedings of the 2022 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Singapore, 14–16 December 2022; IEEE: Piscataway Township, NJ, USA; pp. 1–6.
7. Choi, S.; Shin, Y.; Yoo, H. Analysis of Ring-Oscillator-based True Random Number Generator on FPGAs. In Proceedings of the 2021 International Conference on Electronics, Information, and Communication (ICEIC), Jeju, Republic of Korea, 31 January–3 February 2021; IEEE: Piscataway Township, NJ, USA; pp. 1–3.
8. Sivaraman, R.; Rajagopalan, S.; Amirtharajan, R. FPGA based generic RO TRNG architecture for image confusion. *Multimed. Tools Appl.* **2020**, *79*, 13841–13868. [CrossRef]
9. Sivaraman, R.; Sridevi, A.; Rajagopalan, S.; Janakiraman, S.; Rengarajan, A. Design and analysis of ring oscillator influenced beat frequency detection for true random number generation on fpga. In Proceedings of the 2019 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 23–25 January 2019; IEEE: Piscataway Township, NJ, USA; pp. 1–6.
10. Bakiri, M.; Guyeux, C.; Couchot, J.F.; Oudjida, A.K. Survey on hardware implementation of random number generators on FPGA: Theory and experimental analyses. *Comput. Sci. Rev.* **2018**, *27*, 135–153. [CrossRef]
11. Syafalni, I.; Jonatan, G.; Sutisna, N.; Mulyawan, R.; Adiono, T. Efficient homomorphic encryption accelerator with integrated PRNG using low-cost FPGA. *IEEE Access* **2022**, *10*, 7753–7771. [CrossRef]
12. Park, S.; Gun Choi, B.; Kang, T.; Park, K.; Kwon, Y.; Kim, J. Efficient hardware implementation and analysis of true random-number generator based on beta source. *ETRI J.* **2020**, *42*, 518–526. [CrossRef]
13. Petura, O.; Mureddu, U.; Bochard, N.; Fischer, V.; Bossuet, L. A survey of AIS-20/31 compliant TRNG cores suitable for FPGA devices. In Proceedings of the 2016 26th international conference on field programmable logic and applications (FPL), Lausanne, Switzerland, 29 August–2 September 2016; IEEE: Piscataway Township, NJ, USA; pp. 1–10.
14. Cui, J.; Yi, M.; Cao, D.; Yao, L.; Wang, X.; Liang, H.; Huang, Z.; Qi, H.; Ni, T.; Lu, Y. Design of true random number generator based on multi-stage feedback ring oscillator. *IEEE Trans. Circuits Syst. Ii: Express Briefs* **2021**, *69*, 1752–1756. [CrossRef]
15. Cao, Y.; Zhao, X.; Zheng, W.; Zheng, Y.; Chang, C.H. A new energy-efficient and high throughput two-phase multi-bit per cycle ring oscillator-based true random number generator. *IEEE Trans. Circuits Syst. Regul. Pap.* **2021**, *69*, 272–283. [CrossRef]
16. Rojas-Muñoz, L.F.; Sánchez-Solano, S.; Martínez-Rodríguez, M.C.; Brox, P. True Random Number Generation Capability of a Ring Oscillator PUF for Reconfigurable Devices. *Electronics* **2022**, *11*, 4028. [CrossRef]

17. Sivaraman, R.; Rajagopalan, S.; Sridevi, A.; Rayappan, J.; Annamalai, M.P.V.; Rengarajan, A. Metastability-induced TRNG architecture on FPGA. *Iran. J. Sci. Technol. Trans. Electr. Eng.* **2020**, *44*, 47–57. [CrossRef]
18. Abidi, A.A. Phase noise and jitter in CMOS ring oscillators. *IEEE J. Solid State Circuits* **2006**, *41*, 1803–1816. [CrossRef]
19. Manku, T. Microwave CMOS-device physics and design. *IEEE J. Solid State Circuits* **1999**, *34*, 277–285. [CrossRef]
20. Razavi, B. CMOS technology characterization for analog and RF design. *IEEE J. Solid State Circuits* **1999**, *34*, 268–276. [CrossRef]
21. Zafarkhah, E.; Maymandi-Nejad, M.; Zare, M. Single-ended ring oscillators: Analysis and design. *IET Circuits Devices Syst.* **2020**, *14*, 869–875. [CrossRef]
22. Islam, R.; Suprotik, A.N.K.; Uddin, S.Z.; Amin, M.T. Design and analysis of 3 stage ring oscillator based on MOS capacitance for wireless applications. In Proceedings of the 2017 International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox's Bazar, Bangladesh, 16–18 February 2017; IEEE: Piscataway Township, NJ, USA; pp. 723–727.
23. Rezayee, A.; Martin, K. A three-stage coupled ring oscillator with quadrature outputs. In Proceedings of the ISCAS 2001. The 2001 IEEE International Symposium on Circuits and Systems (Cat. No. 01CH37196), Sydney, NSW, Australia, 6–9 May 2001; IEEE: Piscataway Township, NJ, USA; Volume 1, pp. 484–487.
24. Bounchaleun, A. An Elementary Introduction To Fast Fourier Transform Algorithms. 2019. Available online: https://math.uchicago.edu/~may/REU2019/REUPapers/Bounchaleun.pdf (accessed on 30 December 2023).
25. Yoshizawa, T.; Hirobayashi, S.; Misawa, T. Noise reduction for periodic signals using high-resolution frequency analysis. *EURASIP J. Audio Speech Music. Process.* **2011**, *2011*, 1–19. [CrossRef]
26. Bikos, A.; Nastou, P.E.; Petroudis, G.; Stamatiou, Y.C. Random Number Generators: Principles and Applications. *Cryptography* **2023**, *7*, 54. [CrossRef]
27. Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423. [CrossRef]
28. Cao, Y.; Liu, W.; Qin, L.; Liu, B.; Chen, S.; Ye, J.; Xia, X.; Wang, C. Entropy Sources Based on Silicon Chips: True Random Number Generator and Physical Unclonable Function. *Entropy* **2022**, *24*, 1566. [CrossRef] [PubMed]
29. Zhu, S.; Ma, Y.; Lin, J.; Zhuang, J.; Jing, J. More powerful and reliable second-level statistical randomness tests for NIST SP 800-22. In Proceedings of the Advances in Cryptology–ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, 4–8 December 2016; Proceedings, Part I 22. Springer: Berlin/Heidelberg, Germany, 2016; pp. 307–329.
30. Sulak, F.; Uğuz, M.; Kocak, O.; Doğanaksoy, A. On the independence of statistical randomness tests included in the NIST test suite. *Turk. J. Electr. Eng. Comput. Sci.* **2017**, *25*, 3673–3683. [CrossRef]