electronics

MDPI

Article

Entropy Model of Rosin Autonomous Boolean Network Digital True Random Number Generator

Yi Zong *,†, Lihua Dong † and Xiaoxin Lu

School of Telecommunications Engineering, Xidian University, Xi'an 710071, China; lih_dong@mail.xidian.edu.cn (L.D.); 20011210446@stu.xidian.edu.cn (X.L.)
* Correspondence: 22011210962@stu.xidian.edu.cn
† These authors contributed equally to this work.

Abstract: A True Random Number Generator (TRNG) is an important component in cryptographic algorithms and protocols. The Rosin Autonomous Boolean Network (ABN) digital TRNG has been widely studied due to its nice properties, such as low energy consumption, high speed, strong platform portability, and strong randomness. However, there is still a lack of suitable entropy models to deduce the requirement of design parameters to ensure true randomness. The current model to evaluate the entropy of oscillator-based TRNGs is not applicable for Rosin ABN TRNGs due to low-frequency noise. This work presents a new, suitable stochastic model to evaluate the entropy of Rosin ABN TRNGs. Theoretical analysis and simulation experiments verify the correctness and the effectiveness of the model, and, finally, the appropriate sampling parameters for Rosin ABN TRNGs are given for sufficient entropy per random bit to ensure true randomness.

Keywords: autonomous Boolean network; true random number generator; entropy models; Allan variance

Citation: Zong, Y.; Dong, L.; Lu, X. Entropy Model of Rosin Autonomous Boolean Network Digital True Random Number Generator. *Electronics* **2024**, *13*, 1140. https://doi.org/10.3390/electronics13061140

Academic Editor: Martin Reisslein

Received: 25 January 2024
Revised: 12 March 2024
Accepted: 19 March 2024
Published: 20 March 2024

1. Introduction

The unpredictability of true random numbers provides a fundamental security guarantee for cryptographic algorithms and security protocols, and a high-performance TRNG is also an important component to ensure network security [1]. Usually, there are two methods to evaluate the randomness of the output sequence of a TRNG: One is to detect whether it has obvious statistical deviation [2–6]. The other one is to establish a random entropy model, and from this model, it is feasible to derive the requirements for the design parameters of TRNGs, so as to guide the design of a TRNG in reverse.

The statistical tests cannot or have difficulties detecting the possible hidden weakness inside TRNGs. Therefore, most scholars focus on the study of the entropy model of TRNGs. The entropy model is a stochastic model used to evaluate the entropy of a specific TRNG, and an accurate entropy estimation for this specific random number generator structure in theory can be obtained by this stochastic model [7]. The entropy used in this article is Shannon entropy. To model oscillator-based TRNGs, Killmann and Schindler proposed a common stochastic model from the time domain [8]. However, only the lower bound of output entropy can be obtained through this analysis method. In 2014, Ma et al. [7] proposed a stochastic model to calculate the precise entropy for RO-based TRNGs, and put forward the quality factor Q to assist the structural design. In 2018, Zhu et al. discussed the calculation error between the standard variance in the counting results and approximate Q in the entropy model proposed by Ma et al., thus giving a more accurate estimate of jitter [9]. In 2019, Ma et al. proposed an entropy estimation method for TRNGs based on ADC sampling [10]. In 2021, Markku-Juhani O. Saarinen et al. put forward a new lower bound estimation formula for the entropy of ring vibration sources, which is more widely used than the previous formula [11]. However, there is no suitable common stochastic

model to calculate the precise entropy for common TRNGs, such as metastable state TRNGs, ABN TRNGs, TRNGs with complex feedback behavior, and so on.

Among them, ABN TRNGs can play a huge role in embedded and other scale-limited environments because they can be integrated on cheap and highly integrable electronic chips. And their speed of generating random numbers is also very fast, which can consistently meet the real-time requirements of modern communication and become an important kind of TRNG. In 2013, Rosin et al. used an ABN to construct a new type of physical TRNG which has a wide spectrum, a high frequency, and can achieve high-speed output through parallel approaches. However, when the number of the nodes is low, the oscillation of the Boolean Network is weakened and even degenerates [12]. In 2018, on the basis of Rosin TRNGs, Yang Hui changed the time delay between logic links by adding inverters, so that the structure can still output stable and available random numbers at low nodes [13]. In 2020, Gong et al. highlighted the factors affecting chaotic Boolean Networks, which provided a certain theoretical basis for the subsequent study of chaotic Boolean Networks [14].

In this paper, based on the entropy model used for RO-based TRNGs [7], we establish a random entropy model for the TRNG of a Rosin Autonomous Boolean Network. The proposed entropy model is verified on Rosin's TRNG with different numbers of nodes. The experimental results show that the proposed entropy model is correct and effective. Different parameters are provided for different entropy requirements.

The rest of this paper is organized as follows. In Section 2, we briefly introduce the TRNG based on Boolean Networks. Section 3 presents the proposed entropy model and analyzes the difference between TRNGs based on oscillators and those based on Autonomous Boolean Networks. In Section 4, the effectiveness and correctness of this entropy model is validated and the optimal sampling parameters for different requirements are given. In Section 5, we summarize this paper.

2. TRNGs Based on Autonomous Boolean Networks

A Boolean Network is a network composed of Boolean operations, such as AND, OR, and NOT, as well as Boolean nodes with two states: on state 1 and off state 0. In Boolean Networks, due to factors such as thermal noise, shot noise, and so on, the phase of the circuit will produce a certain amount of jitter. When this kind of jitter undergoes nonlinear walk within an Autonomous Boolean Network, its amplitude is amplified by about two orders of magnitude, which will cause the weak entropy source with originally small jitter to evolve into a strong entropy source with severe jitter. TRNGs of Autonomous Boolean Networks with this characteristic have been widely studied by cryptography scholars due to their nice properties of elegant structure and high speed [15–18].

A TRNG of a Rosin Autonomous Boolean Network with n nodes [12] is shown in Figure 1. The nodes in this network have only one exclusive NXOR gate (denoted as $\odot$), and the others are exclusive XOR gates (denoted as $\oplus$, around the circumference of the circle). Each node has three inputs, one output, and self-feedback. Adjacent nodes are inputs to each other and arrow represents wire. The true random number is obtained by sampling the XOR values (the red $\oplus$) of four network nodes through low-frequency clock signals. Whether this network generates chaotic oscillation depends on the initial conditions and the setting of delay, that is, ideally, there is no stagnation point.

Just as the author of [12] said, when we sample the proposed TRNG structure in Figure 1 with a frequency of 100 MHz, the collected data should pass the National Institute of Standards and Technology (NIST) SP800-22 [3]. However, when we verified this TRNG structure on Altera Cyclone IV EP4CE6F with a sampling frequency of 100 MHz, some groups of collected data were unable to pass the NIST test. This indicates that the Rosin's Autonomous Boolean Network TRNG differs on different FPGA models, and its platform portability is challenged. To obtain the the parameters for this structure on different FPGAs, we established an entropy model for this structure.

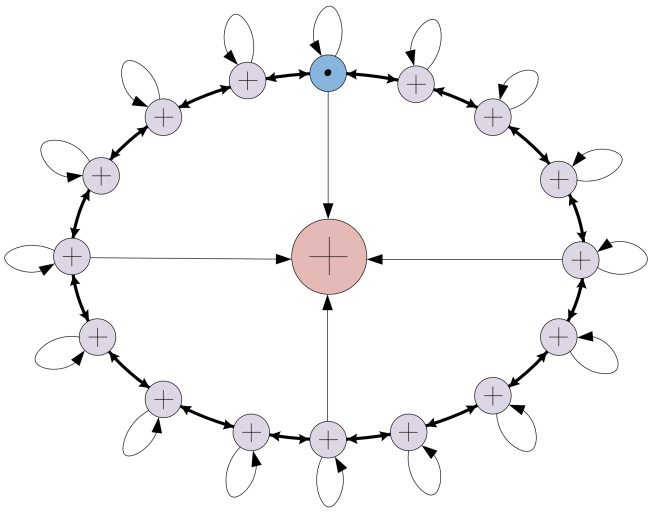

Figure 1. TRNG of Rosin Autonomous Boolean Network.

3. Entropy Model of Rosin Autonomous Boolean Network TRNG

To establish a suitable model for this structure, we noted that the Rosin Boolean Network TRNG and the oscillation-based TRNG have great similarity. Both of them use low-frequency clock signals to sample high-frequency jitter signals to generate random numbers and the source of their randomness is phase jitter. To this end, we first attempted to use the TRNG entropy model based on an oscillation ring to analyze the Rosin's Autonomous Boolean Network; based on the differences between the two, we obtained an entropy model that can be applicable to the TRNG based on Rosin's Autonomous Boolean Network.

3.1. The Entropy Model of Ma Is Not Applicable to TRNGs of the Rosin Autonomous Boolean Network

In traditional "low-frequency sampling of high-frequency" TRNGs, the sampling parameters can usually be adjusted according the average and variance in the rising edge jump transition number of the output sequence, so that the low-frequency sampling signal can just sample at the jump transitions of the fast oscillating signal and obtain the best random output sequence. In view of this, this section counts the number of jump transition rising edges of the output sequence of the Rosin Autonomous Boolean Network TRNG shown in Figure 1, and calculates the mean and variance of the counted values. The specific experimental steps are as follows:

1. Implement the structure shown in Figure 1 using FPGA, with n = 16, and sample the TRNG output with a 100 MHz system clock signal. The sampling method is as follows: when the rising edge of the sampled signal jumps, the counter begins to record the number of rising edges of the TRNG output signal; when the falling edge of the sampled signal jumps, the counter outputs the number of rising edges counted and performs a reset operation to obtain a total of 2^{16} count values;
2. The average value is 128.6207, and the variance is 73.9459^2.

This result is not consistent with the assumption $\frac{\mu}{\sigma} \ll 1$ in Ma et al.'s stochastic entropy model. The reason is described as follows.

In the frequency domain, let b be the output signal of the oscillation ring. If b is a zero-mean stationary random process, the standard variance in signal b can be expressed as [19]

$$Var(b) = \sum_{\alpha=-2}^{2} \frac{h_\alpha}{(\pi\tau)^2} \int_0^{f_h} f^{\alpha-2} \sin^2(\pi\tau f) df \quad (1)$$

where f_h is the cut-off frequency of the oscillation ring; α indicates the type of noise; the α value is +2, indicating white noise phase modulation, +1, indicating flicker noise phase modulation, 0, indicating white noise frequency modulation, -1, indicating flicker

noise (low-frequency noise) frequency modulation, and -2, indicating random walk (low-frequency noise) frequency modulation. According to reference [19], when $f \to 0$, the integrand function can be approximated as $\pi^2\tau^2 f^{\alpha}$. At this point, if $\alpha = -1$ or -2 is taken, the integrand function will not converge.

In the Autonomous Boolean Network TRNG, the signal generated will amplify the jitter to a hundred times its original amplitude, which means that the thermal noise and flicker noise in the noise source will be simultaneously amplified by a hundred times, at which point the flicker noise will be amplified ($\alpha = -1$). The impact of low-frequency noise cannot be ignored, as it accelerates the accumulation speed of jitter. The comparison between the cumulative changes (the red shadow) in signal jitter on ABN TRNGs and the cumulative changes in signal jitter based on traditional ring oscillators is shown in Figure 2.

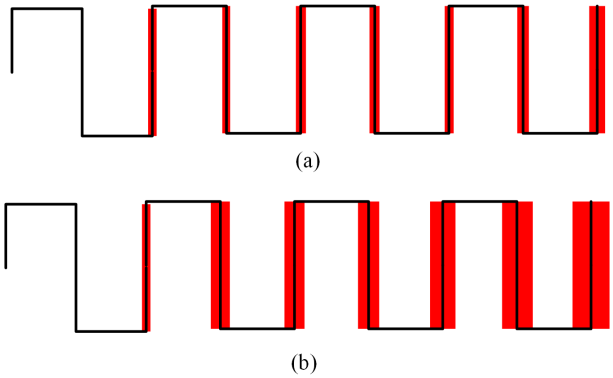

Figure 2. Jitter accumulation comparison chart: (**a**) traditional TRNG jitter accumulation. (**b**) Rosin Autonomous Boolean Network jitter accumulation.

The cumulative speed of jitter affects the oscillation speed of the output waveform, as shown in Figure 3, which is a comparison of the output waveforms of an ABN TRNG composed of 16 nodes and a single classical oscillation ring. The horizontal axis in the figure is 25 ns/M. It can be observed that for every jump in the output of the classical oscillation ring, the output of the Rosin Autonomous Boolean Network oscillation ring has already jumped dozens or even hundreds of times.

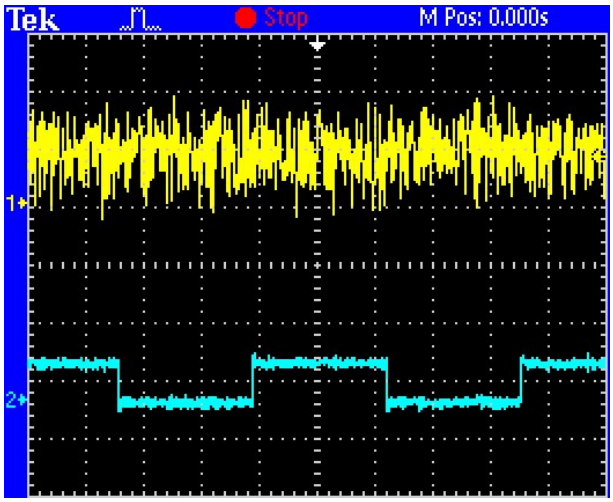

Figure 3. Comparison of output waveforms between a single Rosin Autonomous Boolean Network TRNG (sig 1) and a single oscillation loop TRNG (sig 2).

Therefore, the random entropy model proposed by Ma et al. cannot be used to evaluate the entropy of the Rosin Autonomous Boolean Network TRNG. It is necessary to improve

the model and find more suitable parameters to describe the jitter in the Rosin Autonomous Boolean Network.

3.2. Allan Variance Is More Suitable for Describing the Jitter of Rosin Autonomous Boolean Network TRNGs

Allan variance is a variance used to analyze the phase and frequency instability of oscillation loops [20]. Let b be the output signal of the oscillator loop and $\overline{b}_i$ be the mean value within the i-th interval of length τ. The Allan variance in the oscillator loop output signal b in a dataset consisting of M mean samples within intervals of length τ can be expressed as follows:

$$\mathrm{Avar}(b) = \sigma_b^2(\tau) = \frac{1}{2(M-1)} \sum_{i=1}^{M-1} (\overline{b}_{i+1} - \overline{b}_i)^2 \tag{2}$$

In the frequency domain, the Allan variance can be expressed as

$$\mathrm{Avar}(b) = \sigma_b^2(\tau) = \sum_{\alpha=-2}^{2} \frac{2h_\alpha}{(\pi\tau)^2} \int_0^{f_h} \sin^4(\pi\tau f) f^{\alpha-2} df \tag{3}$$

When $f \to 0$, the integrated function can be approximated as $\pi^4\tau^4 f^{\alpha+2}$. At this point, even if the signal b is affected by low-frequency noise (i.e., with α taking values of -1 and -2), the integrated function still converges. Therefore, in the subsequent analysis, the Allan variance, which is more friendly to low-frequency noise, is used to characterize the magnitude of jitter in the Rosin Autonomous Boolean Network TRNG.

3.3. Entropy Model of the Rosin Autonomous Boolean Network TRNG

Based on the above analysis, an entropy model is established for the Rosin Autonomous Boolean Network TRNG.

As shown in Figures 4 and 5, using the clock signal S_2 as the control signal for the counter, the counter counts the number of rising edges of the Rosin TRNG output signal S_1 when S_2 is at a high level. When S_2 is at a low level, the counter values are stored in a register, and the counter is reset. τ is chosen as the interval, where each τ counter value in the register forms a group. The mean μ is calculated for each group, and this mean is considered the half-period length of the high-frequency signal $S_1^{'}$.

The slow clock signal S_3 is used as a low-frequency signal to sample the transition signal $S_1^{'}$.

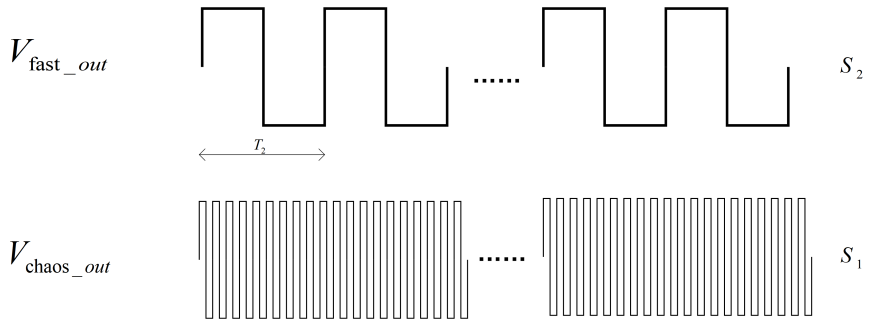

Figure 4. Sampling diagram of the output waveform of the Rosin Autonomous Boolean Network TRNG.

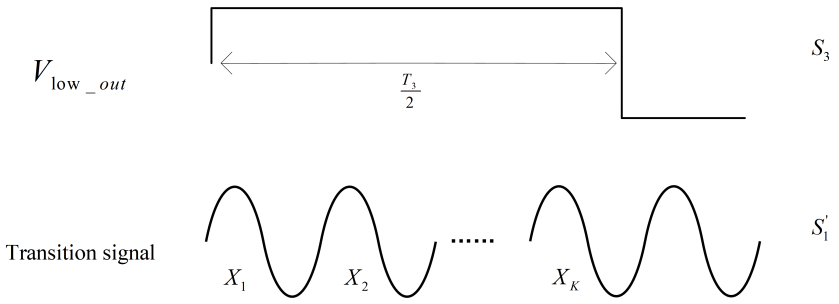

Figure 5. Equivalent model.

Assuming the half-periods of the transition signal $s_1^{'}$, obtained by counting, are denoted as X_k, where $k = 1, 2, \ldots$, and due to the presence of jitter, it can be assumed that X_k follows a normal distribution with mean μ and Allan variance σ_a^2, i.e., $X_k \sim N(\mu, \sigma_a^2)$. Let the signal S_3 have a period T_3, and let R_i be the number of rising edges of $S_1^{'}$ within half a period of S_3. The sampled data for the i-th bit, denoted as b_i, are given by $b_i = (b_{i-1} + R_i) \bmod 2$. The basic assumptions in our work are the same as those made in Ma's stochastic model, which was used to calculate the precise entropy for RO-based TRNGs [7]. Here, b_i is still the i-th sampled bit. Since the operation of adding R_i with b_{i-1} can be treated as a type of post-processing, this operation causes no impact on the information entropy. So, the equation $b_i = (b_{i-1} + R_i) \bmod 2$ can be further simplified to $b_i = R_i \bmod 2$. Let $L_k = X_1 + X_2 + \ldots + X_k$; thus,

$$Pr(R_i \leq k) = Pr(L_k \geq \frac{T_3}{2}) \tag{4}$$

where k is the minimum value that $L_k \geq \frac{T_3}{2}$. According to the Central Limit Theorem, the distribution function of L_k is given by $L_k \sim N(k\mu, k\sigma_a^2)$. Therefore, we can further derive

$$Pr(R_i \leq k) = \frac{1}{\sqrt{2k\pi}\sigma_a} \int_{\frac{T_3}{2}}^{+\infty} e^{-\frac{(t-k\mu)^2}{2k\sigma_a^2}} dt \tag{5}$$

Let $u = t - k\mu, x = u/\sqrt{2k}\sigma$. Then,

$$Pr(R_i \leq k) = \frac{\sqrt{2k}\sigma_a}{\sqrt{2k\pi}\sigma_a} \int_{\frac{\frac{T_3}{2}-k\mu}{\sqrt{2k}\sigma_a}}^{+\infty} e^{-x^2} dx = \frac{1}{2}(1 - erf(\frac{\frac{T_3}{2} - k\mu}{\sqrt{2k}\sigma_a})) \tag{6}$$

The probability of having k rising edges of signal within the duration of $T_3/2$ can be expressed as follows:

$$Pr(R_i = k) = Pr(R_i \leq k) - Pr(R_i \leq k-1) = \frac{1}{2}(erf(\frac{\frac{T_3}{2} - (k-1)\mu}{\sqrt{2(k-1)}\sigma_a}) - erf(\frac{\frac{T_3}{2} - k\mu}{\sqrt{2k}\sigma_a})) \tag{7}$$

Let p_1 be the probability of the i-th sampled bit b_i, equal to 1, and p_0 be the probability of the i-th sampled bit b_i, equal to 0. Then, we have

$$p_1 = Pr(b_i = 1) = Pr(R_i \bmod 2 = 1) = \sum_{k=0}^{k=+\infty} Pr(R_i = 2k+1) \tag{8}$$

$$p_0 = 1 - p_1 \tag{9}$$

Let X_n be the n-bit output and x_j be the j-th bit. Since the counter is reset at every period of S_3, then, using the property of the Markov process, we obtain the probability $p_{X_n} = Pr(b_1 = x_1, b_2 = x_2, \ldots, b_n = x_n)$ as follows:

$$p_{X_n} = Pr(B_n = X_n) = \prod_{j=0}^{n-1} {p_0}^{1-x_j} {p_1}^{x_j} = \prod_{j=0}^{n-1} (1-p_1)^{1-x_j} {p_1}^{x_j} \tag{10}$$

When the random process B_n is in the ideal condition, i.e., a stationary random process, the entropy rate for each bit of TRNG output is equal to

$$H = \lim_{n\to\infty} \frac{H_n}{n} \tag{11}$$

$$H_n = -\sum_{X_n\in\{0,1,\ldots,2^n-1\}} p_{X_n} \cdot \log_2 p_{X_n} \tag{12}$$

Due to the fact that the output signal S_1 of the Rosin Autonomous Boolean Network TRNG is a strong random source, its correlation approaches zero in a short period of time. Therefore, the correlation between each random number X_k is zero, indicating mutual independence. As a result, the entropy rate for each bit of the TRNG output is equal to

$$H = -p_b \log_2 p_b - (1-p_b)\log_2(1-p_b) \tag{13}$$

4. Model Verification

In this section, we validate the effectiveness and correctness of the entropy model.

4.1. Validation of the Effectiveness of the Entropy Model

In this subsection, we validate the effectiveness of the entropy model. The specific validated steps are as follows:

1. Implement the structure shown in Figure 1 using an FPGA, with n = 16. Let the output of this Rosin Autonomous Boolean Network TRNG be denoted as signal S_1. Count signal S_1 using a clock signal S_2 with a frequency of 100 MHz, resulting in a total of 2^{16} count values.
2. Calculate the mean of the count values, $\mu = 128.6207$.
3. Set τ = 4 and M = 8 in the formula for calculating the Allan variance. Utilizing 2^{16} count values, use Matlab R2019b to compute the Allan variance:

$$\mathrm{Avar}(b) = \sigma_b^2(\tau) = \frac{1}{2(M-1)} \sum_{i=1}^{M-1} (\bar{b}_{i+1} - \bar{b}_i)^2 \tag{14}$$

   The calculated Allan variance is 5.0978^2.
4. Given a lower bound on entropy, we can compute the corresponding value of the quality factor Q, according to the relationship between the output entropy and quality factor [21]:

$$H_{lower} = 1 - \frac{4}{\pi^2 \ln 2} e^{-4\pi^2 Q} \tag{15}$$

   and

$$Q = \rho^2 v, \rho = \sigma_b f_{high}, v = \frac{f_{high}}{f_{low}} \tag{16}$$

   where σ_b is the Allan variance. So,

$$Q = \frac{\sigma_b^2 f_{high}^3}{f_{low}} \tag{17}$$

   For example, if H_{lower} is set to 0.9999, then $Q = 0.2197$. Assuming that the low-frequency sampling clock signal S_3 is without jitter, let f_3 be the frequency of the low-frequency sampling signal and f_4 and σ_4 be the frequency and jitter of the transition signal $s_1^{'}$, respectively. The highest sampling frequency for the slow signal can be obtained by $f_3 = \frac{\sigma_4^2 f_4^3}{Q}$. The highest calculated sampling frequency under these conditions is 18.2 MHz when $Q = 0.2197$.
5. To evaluate the Rosin Autonomous Boolean Network TRNG (n = 16) as shown in Figure 1, collect 2^{16} data points for four cases, that is, the sample frequencies are

18.2 MHz, 15 MHz, 20 MHz, and 60 MHz, which correspond to the highest sampling frequency, a lower sampling frequency, a higher sampling frequency, and a significantly higher frequency. The corresponding entropy values are shown in Figure 6.

It is observed that the entropy value reaches the design standard 0.9999 at a sampling frequency of 18.2 MHz. Below this frequency, the entropy value gradually increases, while above this frequency, the entropy value gradually decreases, aligning with the actual scenario.

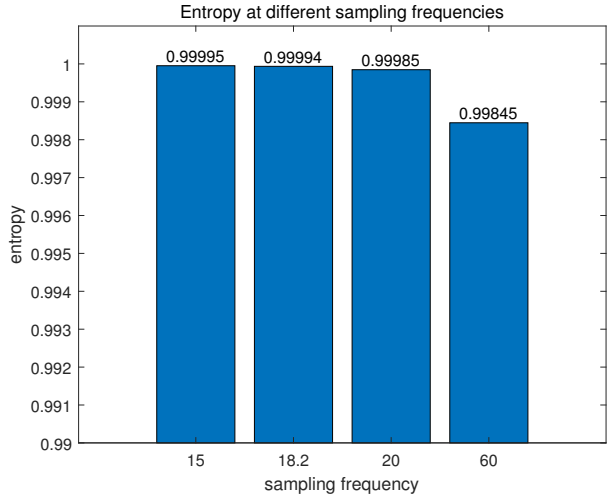

Figure 6. Entropy values at different sampling frequencies.

On the other hand, utilizing the 2^{16} count values obtained, the statistical variance is calculated to be 73.9459^2. Plugging this value into Equation (14), the theoretical calculation yields a maximum sampling frequency of 720 MHz for an entropy of 0.9999.

We collected data in three cases, that is, with a sample frequency of 100 MHz, the frequency obtained by Ma's model, and that by our improvement model. It was found that after our improvement, the PROPORTION in the NIST test was increased and subjected to an 800-22 NIST test, while, under the first two sample frequencies, there are cases that cannot pass the 800-22 NIST test, that is, the proportion is lower than 0.987 (as show in Table 1, marked with *). This indicates that the standard variance tends to overestimate the jitter in the Rosin Autonomous Boolean Network.

Table 1. NIST test.

	Proportion with a Sample Frequency of 100 MHz	**Proportion with the Sample Frequency Obtained from Ma's Model**	**Proportion with the Sample Frequency Obtained from Our Improved Model**
Frequency	0.971 *	0.830 *	0.993
Block Frequency	0.990	0.970 *	0.991
Cumulative Sums	0.938 *	0.851 *	0.995
Runs	0.989	0.972 *	0.991
LongestRun	0.982 *	0.970 *	0.993
Rank	0.985 *	0.978 *	0.996
FFT	0.991	0.971 *	0.996
NonOverlappingTemplate	0.983 *	0.934 *	0.988
OverlappingTemplate	0.927 *	0.788 *	0.987
ApproximateEntropy	0.970 *	0.930 *	0.990
RandomExcursions	0.989	0.954 *	0.989
RandomExcursionsVar	0.972 *	0.955 *	0.988
Serial	0.987	0.880 *	0.990
LinearComplexity	0.982 *	0.960 *	0.994

As we can see from Table 1, there were 8 and 15 stars, respectively, for the first two cases, while for our case, all the tests were passed successfully.

4.2. Validation of the Correctness of the Entropy Model

This section aims to validate the correctness of the entropy model in Section 3.3. Based on the actual sampling data, we know that the Allan variance is 5.0978^2. Using the relationship between the count values and Allan variance in the entropy model, we can obtain a theoretical value. If we can proof that the theoretical value of the Allan variance is still equal to 5.0978^2, then we have proved the correctness of the entropy model. The specific validation process is as follows:

1. Obtain 2^{16} count values.
2. Calculate the mean μ using the count values.
3. Similar to Section 4.1, calculate the sampling frequency f_3 using the count values.
4. Calculate the minimum value of k that satisfies $L_{\mathrm{k}} \geq \frac{T_3}{2}$.
5. Divide each k count value into a group, count the number of groups that satisfy $L_k \geq \frac{T_3}{2}$, and use the relationship $Pr(R_i \leq k) = Pr(L_k \geq \frac{T_3}{2})$ to approximate the probability value.
6. Substitute the statistical results of the above data into Formula (15) to calculate the Allan variance; the result is shown in Table 2.

$$\sigma_a = \frac{\frac{T_3}{2} - k\mu}{\sqrt{2k}erf^{-1}(1 - 2Pr(R_i \leq k))} \tag{18}$$

Table 2. Allan Variance σ_a^2 corresponding to different count values in theoretical model.

Counting Value	Number of Occurrences	Proportion	σ_a^2
496	1	0.00001	5.5366^2
497	27	0.0004	5.1859^2
498	750	0.0114	5.0907^2
499	7644	0.1166	5.0660^2
500	24,191	0.3691	0
501	24,275	0.3704	5.1576^2
502	7819	0.1193	5.1398^2
503	798	0.00122	5.2086^2
504	31	0.0005	0

Regarding the results shown in Table 2, the presence of two zeros in the Allan variance is due to the conditions $T_3/2 = k\mu$ and $erf^{-1}(1 - 2Pr(R_i \leq k)) = -\infty$. In these cases, the variance is indeed 0, and therefore, these two zero values need not be considered. From the table, it can be observed that the Allan variance obtained from the calculation model is close to the experimentally measured Allan variance of 5.0978^2. This indicates that our entropy model can be used to establish and analyze a random model for the Rosin Autonomous Boolean Network TRNG.

4.3. Comparison of Results and Recommended Parameters

In order to achieve the optimal parameters for Rosin's Boolean Network TRNG on different FPGA models, it is necessary to analyze the impact of the frequency of the slow clock control signal S_3 on the output.

Firstly, let $r = (T_3/2) \bmod \mu$. If $r = 0$, the period value T_3 of the control signal S_3 is exactly a multiple of the period value of the transition signal $S_1^{'}$. In this case, the edges of the two signals coincide at any moment, meaning that the sampling point is precisely located at the 0–1 transition edge of the $S_1^{'}$ periodic signal.

If $r = (s/2) \bmod \mu = 0.5\mu$, the period value of the control signal S_3 is half a period value more than a multiple of the $S_1^{'}$ periodic value. In this scenario, the sampling point is precisely located between two adjacent 0–1 transition edges of the $S_1^{'}$ periodic signal, resulting in the maximum deviation in the sampled random number effect.

Based on the above analysis, let $r = (s/2) \bmod \mu = 0$; by substituting parameters $\mu = 128.6207$, we could obtain $T_3 = 4\mu = 514.4528$. This result indicates that, ideally, when sampling the transition signal $S_1^{'}$ with a slow signal S_3 of 515 half periods, the output entropy of the TRNG can be maximized. When using different FPGAs to port this structure, the corresponding half-cycle length T_3 and Allan variance σ_a^2 can be calculated based on different count values, and then the entropy model can be used to obtain the highest sampling frequency required to achieve entropy on different structures, in order to achieve the fastest output speed.

Then, we utilize the proposed entropy estimation method to configure the structural parameters of Rosin's Boolean Network under the weakened and even degenerate case, that is, where the number of the nodes are as low as nodes 5, 6, 7, and 8, and calculate the entropy values. Using the model to determine sampling parameters at low nodes will result in greater entropy and better improvement.

The mean, Allan variance, and the required half-period length for an entropy greater than 0.9999 for the structure proposed by Rosin under nodes 5, 6, 7, and 8, obtained through the experimental steps described in Section 4.1, are shown in the Table 3.

Table 3. Mean, Allan variance, and recommended half-cycle length under low-node Rosin structure.

	5 Nodes	**6 Nodes**	**7 Nodes**	**8 Nodes**
Mean	129.1118	129.0564	130.1705	128.5994
Allan variance	5.117^2	5.137^2	5.114^2	5.103^2
Recommended half-cycle length	12,136.5092	7488.4844	6508.525	3343.5844
Sample frequency	1.055 MHz	1.71 MHz	1.967 MHz	3.829 MHz

Because Rosin ABN TRNGs may experience insufficient entropy or even degradation at low nodes, we investigated the applicability of our model at low nodes. Under the same structure, the entropy values obtained by directly sampling and those obtained after using the recommended parameters are shown in Table 4. Through the comparison of the entropy values, it can be observed that the entropy values of the Rosin structure significantly increased under low-node conditions after using the recommended parameters. This also validates the feasibility and correctness of our entropy model.

Table 4. Comparison of entropy values before and after using the recommended parameters between the structure of this article and the Rosin structure.

	5 Nodes	**6 Nodes**	**7 Nodes**	**8 Nodes**
Directly output entropy value	0.933503	0.941833	0.943939	0.974506
Entropy value under recommended parameters	0.99996	0.99994	0.99991	0.99997

5. Conclusions

This paper established a theoretical entropy model to evaluate the entropy and presented entropy calculation method for Rosin ABN TRNGs. The model replaces standard variance with Allan variance, which is more suitable for estimating jitter in the Rosin ABN. The correctness and effectiveness of this model was validated in Altera Cyclone IV

EP4CE6F and Altera Cyclone IV EP4CE10F FPGA, and recommended sampling parameters were provided to enhance the quality of the generated true random numbers. Future work will focus on entropy modeling and analysis for broader Boolean chaos TRNGs.

Author Contributions: Conceptualization, Y.Z. and L.D.; Data curation, X.L.; Investigation, L.D.; Software, Y.Z. and X.L.; Supervision, L.D.; Validation, Y.Z. and L.D.; Writing—original draft, Y.Z. and L.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

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

References

1. Crocetti, L.; Matteo, S.D.; Nannipieri, P.; Fanucci, L.; Saponara, S. Design and Test of an Integrated Random Number Generator with All-Digital Entropy Source. *Entropy* **2022**, *24*, 139. [CrossRef] [PubMed]
2. Killmann, W. *A Proposal for: Functionality Classes and Evaluation Methodology for True (Physical) Random Number Generators*; Bundesmat fur Sicherheir in der Information technik (BSI): Bon, Germany, 2001.
3. Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E.; Leigh, S.; Levenson, M.; Vangel, M.; Banks, D.; Heckert, A. *Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Revision 1A*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2010.
4. Barker, E.B.; Feldman, L.; Witte, G. *ITL Bulletin: Recommendation for Random Number Generation Using Deterministic Random Bit Generators (August 2015)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2015.
5. *GM/T 0005-2012*; Randomness Testing Specifications. National Standardization Administration of China: Beijing, China, 2012.
6. Saponara, S. Review of Methodologies and Metrics for Assessing the Quality of Random Number Generators. *Electronics* **2023**, *12*, 723.
7. Ma, Y.; Lin, J.; Chen, T.; Xu, C.; Liu, Z.; Jing, J. Entropy Evaluation for Oscillator-Based True Random Number Generators. In Proceedings of the Cryptographic Hardware and Embedded Systems, Busan, Republic of Korea, 23–26 September 2014.
8. Killmann, W.; Schindler, W. A Design for a Physical RNG with Robust Entropy Estimators. In Proceedings of the Cryptographic Hardware and Embedded Systems—CHES 2008, 10th International Workshop, Washington, DC, USA, 10–13 August 2008.
9. Zhu, S.; Chen, H.; Fan, L.; Chen, M.; Xi, W.; Feng, D. Jitter estimation with high accuracy for oscillator-based TRNGs. In Proceedings of the Smart Card Research and Advanced Applications: 17th International Conference, CARDIS 2018, Montpellier, France, 12–14 November 2018; Revised Selected Papers 17; Springer: Berlin/Heidelberg, Germany, 2019; pp. 125–139.
10. Ma, Y.; Chen, T.; Lin, J.; Yang, J.; Jing, J. Entropy estimation for ADC sampling-based true random number generators. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2887–2900. [CrossRef]
11. Saarinen, M.J.O. On entropy and bit patterns of ring oscillator jitter. In Proceedings of the 2021 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Shanghai, China, 16–18 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.
12. Rosin, D.P.; Rosin, D.P. Ultra-fast physical generation of random numbers using hybrid boolean networks. In *Dynamics of Complex Autonomous Boolean Networks*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 57–79.
13. Hui, Y. Design and Analysis of Digital True Random Number Generator. Master's Thesis, Xidian University, Xi'an, China, 2018.
14. Gong, L.; Zhang, J.; Sang, L.; Liu, H.; Wang, Y. The unpredictability analysis of Boolean chaos. *IEEE Trans. Circuits Syst. II Express Briefs* **2019**, *67*, 1854–1858. [CrossRef]
15. Braccini, M.; Roli, A.; Barbieri, E.; Kauffman, S.A. On the criticality of adaptive Boolean network robots. *Entropy* **2022**, *24*, 1368. [CrossRef] [PubMed]
16. Charlot, N.; Canaday, D.; Pomerance, A.; Gauthier, D.J. Hybrid boolean networks as physically unclonable functions. *IEEE Access* **2021**, *9*, 44855–44867. [CrossRef]
17. Gao, S.; Wu, R.; Wang, X.; Liu, J.; Li, Q.; Wang, C.; Tang, X. Asynchronous updating Boolean network encryption algorithm. *IEEE Trans. Circuits Syst. Video Technol.* **2023**, *33*, 4388–4400. [CrossRef]
18. Yan, P.F.; Zhang, H.; Zhang, C.; Chang, R.Y.; Sun, Y.J. Synchronization of Boolean networks with chaos-driving and its application in image cryptosystem. *IET Image Process.* **2023**, *17*, 4176–4189. [CrossRef]
19. Allini, E.N.; Skórski, M.; Petura, O.; Bernard, F.; Laban, M.; Fischer, V. Evaluation and monitoring of free running oscillators serving as source of randomness. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2018**, *2018*, 214–242. [CrossRef]

20. Allan, D.W. A Modified "Allan Variance" with Increased Oscillator Characterization Ability. In Proceedings of the Annual Frequency Control Symposium, Philadelphia, PA, USA, 27–29 May 1981.
21. *GM/T 0078-2020*; Design Guide for Password Random Number Generation Module. National Standardization Administration of China: Beijing, China, 2020.