electronics

MDPI

Article

Design of True Random Number Circuit with Controllable Frequency

Xinsheng Wang * and Xiyue Wang

School of Information Science and Engineering, Harbin Institute of Technology, Weihai 264209, China; 19B905055@stu.hit.edu.cn

* Correspondence: xswang@hit.edu.cn

Abstract: True random number generators (TRNGs) have been a research hotspot due to secure encryption algorithm requirements. Therefore, such circuits are necessary building blocks in state-of-the-art security controllers. In this paper, a TRNG based on random telegraph noise (RTN) with a controllable rate is proposed. A novel method of noise array circuits is presented, which consists of digital decoder circuits and RTN noise circuits. The frequency of generating random numbers is controlled by the speed of selecting different gating signals. The results of simulation show that the array circuits consist of 64 noise source circuits that can generate random numbers by a frequency from 1 kHz to 16 kHz.

Keywords: random telegraph noise; true random numbers; information security; controllable frequency

Citation: Wang, X.; Wang, X. Design of True Random Number Circuit with Controllable Frequency. *Electronics* **2021**, *10*, 1517. https://doi.org/10.3390/electronics10131517

Academic Editor: Fabian Khateb

Received: 6 June 2021
Accepted: 21 June 2021
Published: 23 June 2021

1. Introduction

With the development of information technology, information security technology has become a significant research hotspot. The application of random numbers is the basis of the entire encryption process in the field of information security. Therefore, it is useful for information security to generate high-quality and high-throughput-rate random numbers.

True random numbers (TRNs) are generally based on a real physical random phenomenon and has a true source of random entropy. This includes metastable phenomena of digital circuits, thermal noise, jitter, and other random physical phenomena. TRN has unpredictable characteristics, which means that no attacker can observe and manipulate it [1].

The method of using the physical noise of the circuit as the source of entropy has better randomness and higher operability at the level of the circuits. Several mode TRNGs based on RTN have been studied to obtain hardware devices with better randomness [2–5]. Most TRNGs based on RTN are focused on generating random numbers with low power or better randomness. In addition, the frequency of random numbers generation is an important performance indicator. Previous research on the frequency of random number generation has focused on increasing fixed frequency. In fact, the controllable frequency of random number generation has great significance in circuit applications.

We designed a TRNG by the combination of digital and analog circuits. The analog circuits consist of noise array circuits for generating RTN, a low-noise operational amplifier circuit for acquiring noise signals, a high-pass filter circuit for filtering noise signals, and a comparator circuit for comparing random signals. The digital circuits include a digital decoder circuit for gating noise array circuits and a memory circuit for storing random signals.

2. Materials and Methods

2.1. Noise Source Circuits

2.1.1. Principle of RTN Generation

RTN is one of the important dynamic sources of change in metal-oxide semiconductor field effect transistors (MOSFETs). The drain current of MOSFETs will fluctuate randomly between several discrete numbers over a wide time range if the MOSFET channel has a defect or trap [6].

RTN is a type of charge migration disturbance caused by trap trapping and releasing charge in single or multiple traps, which causes macrocurrent fluctuation. The probability of a single trap appearing in the oxide layer on the surface of the channel is high in short channel MOSFETs. Therefore, this paper focuses on the RTN caused by a single trap in short-channel MOSFETs.

$$\frac{\Delta I_D}{I_D} = \alpha \frac{g_m}{I_D} \frac{q}{WLC_{OX}} \left(1 - \frac{x_t}{t_{OX}}\right) \quad (1)$$

The physical characteristics of random telegraph noise are mainly determined by three parameters: the average capture time τ_c, the average emission time τ_e, and the difference in current between the two states ΔI_D. The normalized amplitude of current fluctuation between trap capture and emission electrons is described by Equation (1) [7,8].

2.1.2. RTN Source Circuit

The fluctuation current is difficult to accurately collect by the signal processing circuit since the macroperformance of the RTN is a small fluctuation of the drain current. Therefore, a method of converting the fluctuating current into a large-voltage fluctuation was adopted, as shown in Figure 1. The voltage fluctuations can be adjusted to a greater order of magnitude by selecting an appropriate circuit structure. Therefore, the input noise requirement for the subsequent signal-processing circuit is much lower since the amplitude of the output voltage is large.

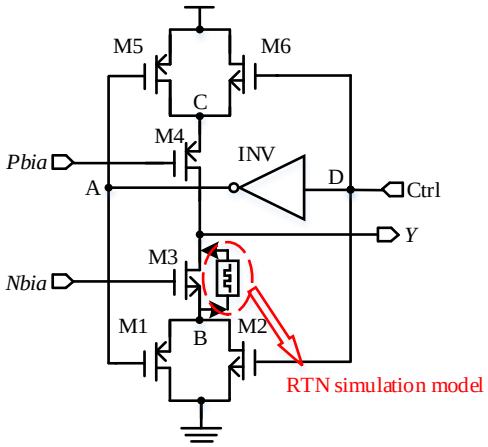

Figure 1. Random telegraph noise (RTN) source circuit structure.

Considering that the RTN appears when the MOSFET oxide layer has a defect or trap, the occurrence of the trap is a probabilistic event in the production process of the integrated circuits. Therefore, the redundancy design of the noise source unit circuit is required. A strobe circuit is added to control different noise source units, as shown in Figure 1, where Ctrl is the strobe control signal. M3 is an N-type MOSFET that generates RTN. M4 is a load to convert the drain current into a voltage signal.

Simulation analysis was performed using the simulation tool MMSIM under Cadence's integrated environment IC617. The input of the circuit is *Nbia* = 650 mV for the

bias voltage input of the N-type MOSFET and *Pbia* = 400 mV for the bias voltage input of the P-type MOSFET. The transient simulation time is 50 ms.

The results are shown in Figure 2. It can be seen from the simulation waveform that the fluctuation of the drain current caused by the RTN phenomenon produces a voltage fluctuation. Furthermore, the RTN simulation model can precisely describe the RTN phenomenon in the transistor.

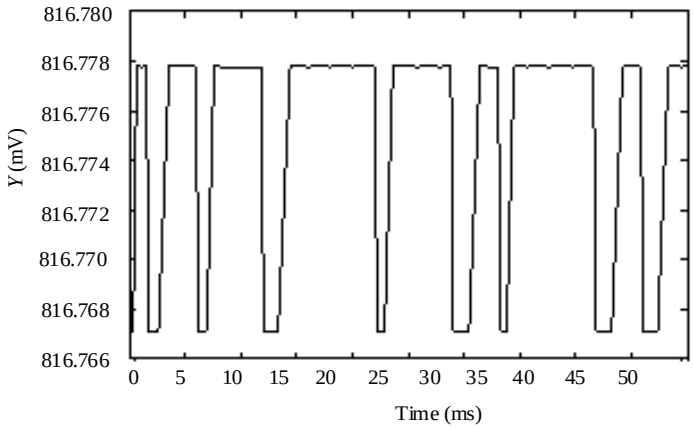

Figure 2. Noise source circuit transient simulation waveform.

2.2. Noise Signal Processing Circuits

The structure of processing noise signals includes analog and digital circuits, as shown in Figure 3. The main function of the digital circuit is to gate the noise source circuits and store the random numbers. The main function of the analog circuit is to amplify, filter, and compare the noise source signals. The decoder strobes the noise source circuits, the operational amplifier (OA) amplifies the RTN signals, and the amplified signals are filtered by the filter to remove the DC offset and the low-frequency other $1/f$ noise. The output of the filter is compared to a reference voltage by comparators, which ultimately produces a random bit stream. Finally, the memory circuits store the random bit stream.

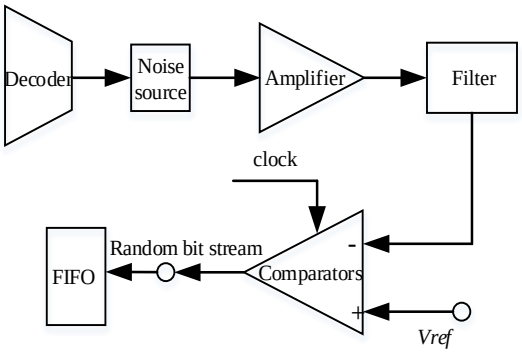

Figure 3. Schematic diagram of noise signal processing circuit.

2.2.1. Operational Amplifier

The OA uses a two-stage amplification structure, as shown in Figure 4. The cascode devices of M4 and M5 can effectively increase the gain of the first stage, which can increase the small-signal transconductance and reduce the thermal noise of the circuit. The differential stage inputs, M2 and M3, are P-type MOSFETs because P-type MOSFETs have lower frequency flicker noise than N-type MOSFETs. M1 and M0 provide mirror current. M6 and M7 are used as loads. It should be noted that the gate length of the load transistor is larger than that of the input transistor, which is more helpful in reducing flicker noise [9].

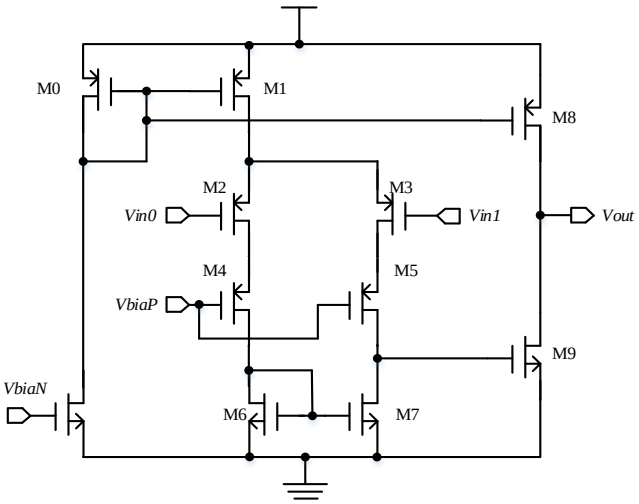

Figure 4. Operational amplifier circuit.

2.2.2. High-Pass Filter

The RTN signals need to be filtered to remove the DC component and other low-frequency flicker noise after amplifying. The high-pass filter can implement the function of filtering. The high-pass filter structure is shown in Figure 5. It uses a MOSFET instead of a capacitor and a resistor since the gate of the MOSFET can be regarded as a pole of the capacitor, while the remaining source, drain, and substrate are terminated together as the other pole of the capacitor. In addition, two MOSFETs are connected in series instead of resistors. A high-pass filter of the desired cutoff frequency can be achieved by appropriately selecting the ratio of the channel width to length of the MOSFET.

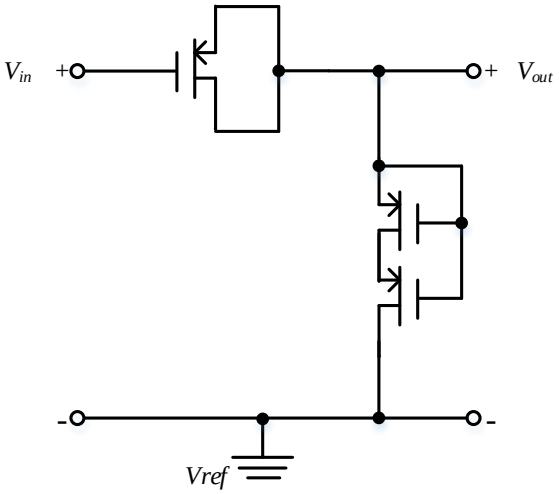

Figure 5. Filter circuit.

2.2.3. Latch Comparator

The structure of the comparator has been optimized, while the traditional dynamic latched comparator structure has defects. The dynamic comparator structure is shown in Figure 6. The bias currents of the input and latch stages are provided by M1 and M2. This also reduces the stack of transistors between the power supply and ground compared to a conventional dynamic latched comparator structure. Therefore, it is suitable for operation at low-supply voltages.

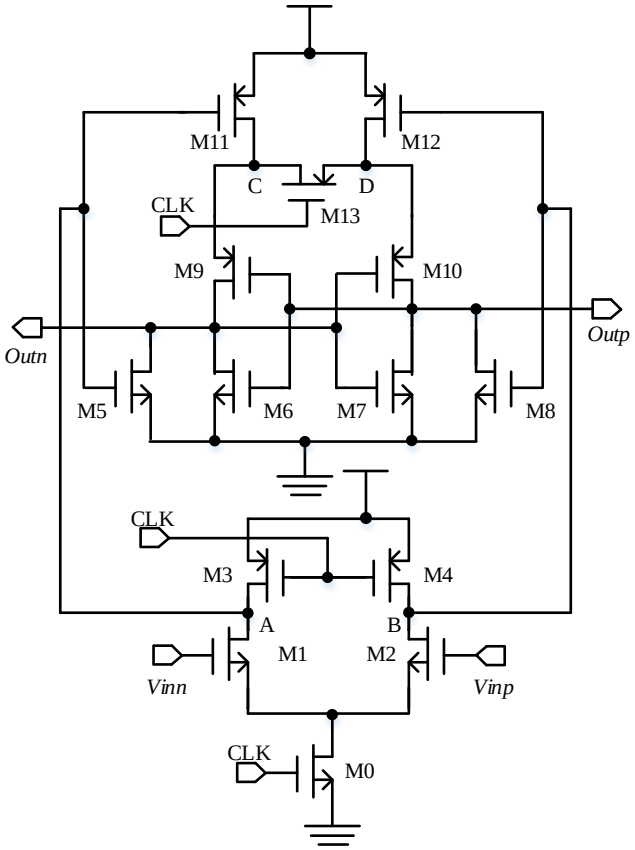

Figure 6. Latch comparator circuit.

The working process of the high-speed dynamic latched circuit is divided into two phases, a reset phase and a comparison phase. In the reset phase, CLK is in a logic-low state, M0 is turned off, M3 and M4 are turned on, node A and node B are pulled to voltage VDD, M11 and M12 are turned off, M5 and M8 are turned on, and *Outn* and *Outp* are pulled to zero potential. The latch consisting of M6, M9, M7, and M10 is in the hold state; the output of the comparator is kept at zero potential.

In the comparison phase, CLK is in a logic-high state, M0 is turned on, M3 and M4 are turned off, node A and node B discharge at different rates depending on the input voltages, *Vinn* and *Vinp*. When the voltages of node A and node B are successively placed on VDD-|VTH|, which is the turn-on voltage of the P-type MOSFET, M11 and M12 start to conduct and operate in the saturation region. Node C and node D then begin to charge until M9 and M10 are turned on. Then, *Outn* and *Outp* are charged until M6 and M7 are turned on. There must be a voltage difference between nodes A and B at the same time since the discharge rates of node A and node B are different at the beginning. Therefore, the *Outn* and *Outp* have a voltage difference. This differential voltage is rapidly amplified to the supply voltage and zero potential as the initial differential of the latch. The *Outn* will output a logic 1, and the *Outp* will output a logic 0, if the voltage value of *Vinn* is greater than *Vinp*. Similarly, *Outn* will output a logic 0, and *Outp* will output a logic 1, if the voltage value of *Vinn* is less than *Vinp*.

2.2.4. Asynchronous FIFO

The asynchronous first input first utput (FIFO) is connected after the comparator output. The aim of the asynchronous design is to deal with the problem that the read clock of the digital circuits is not synchronized with the write clock of the analog circuits.

The asynchronous FIFO is generally composed of a write controller, a read controller, a synchronization unit, and a storage array, as shown in Figure 7. The write controller is responsible for receiving the write enable signal in the write clock domain, providing the

write address and generating a full signal. In Figure 7, *full* is the write FIFO full signal, *wr_en* is the write enable signal, *wr_clk* is the write clock, and *wr_addr* is the write address. The read controller is responsible for receiving the read enable signal, providing the read address and generating a null signal in the read clock domain. Additionally, empty is the read FIFO empty signal, *rd_en* is the read enable signal, *rd_clk* is the read clock, and *rd_addr* is the read address. The storage array is responsible for writing and reading data. The *din* is the data input, *dout* is the data output, and *rst_n* is the asynchronous reset signal. The synchronization unit is responsible for synchronizing the read address signal of the read clock domain to the write clock domain and synchronizing the write address of the write clock domain to the read clock domain. The *syn_rd_addr* is a read address signal synchronized to the write clock domain, and *syn_wr_addr* is a write address signal synchronized to the read clock domain. The purpose of the synchronization process is to compare the read address with the write address to generate a full or empty signal.

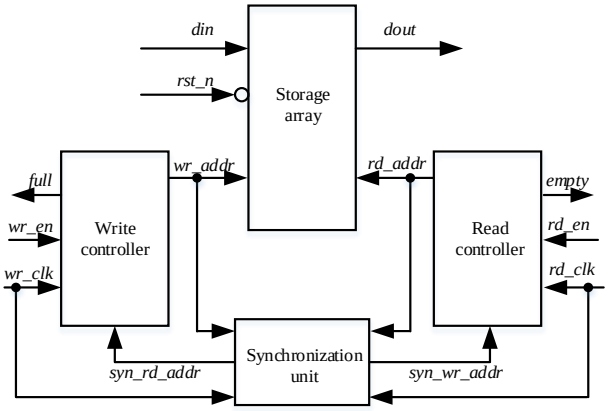

Figure 7. Asynchronous first input first utput (FIFO) circuit.

3. Results

The analog system of the designed noise source circuit, operational amplifier circuit, high-pass filter circuit, and latched comparator circuit is verified by post-simulation. The simulation results are shown in Figure 8.

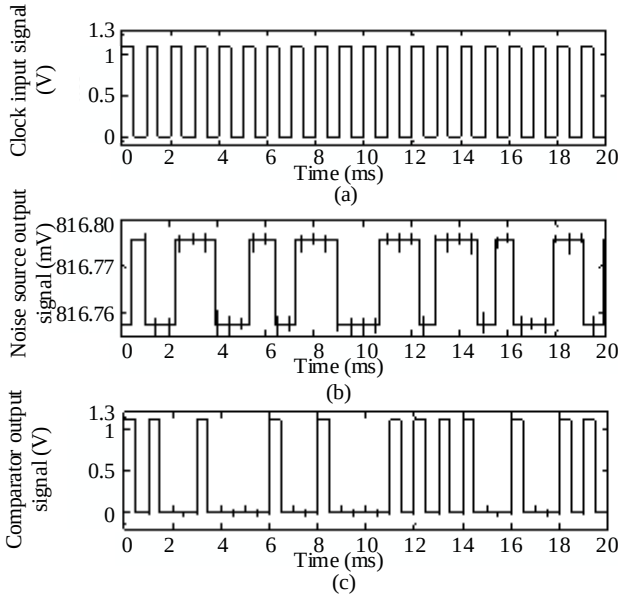

Figure 8. Analog system post-simulation waveform.

In Figure 8, (a) is the clock input signal of the dynamic latched comparator, (b) is the output voltage signals of the RTN source circuit, and (c) is the output voltage signals of the dynamic latched comparator. It can be concluded that the comparator will output logic 1 if the output voltage fluctuation value of the RTN source circuit is high by analyzing the post-simulation waveform. Similarly, the comparator will output logic 0 if the output voltage fluctuation value of the RTN source circuit is at a lower value. The output of the comparator produces a random sequence after a period of simulation. In summary, the entire true random number analog circuit system implements the process from the random signals of the RTN source to the random sequence output.

The design contains digital and analog circuits, so it is necessary to perform mixed post-simulation to verify system functions. Figure 9 shows a schematic of the top-level circuit for digital-analog mixed simulation. The digital-to-analog interface part needs to convert the digital signal into a corresponding analog signal, the digital logic 1 is converted into a power voltage of the noise source part by 1.1 V, and the digital logic 0 is converted into a ground voltage value of 0 V.

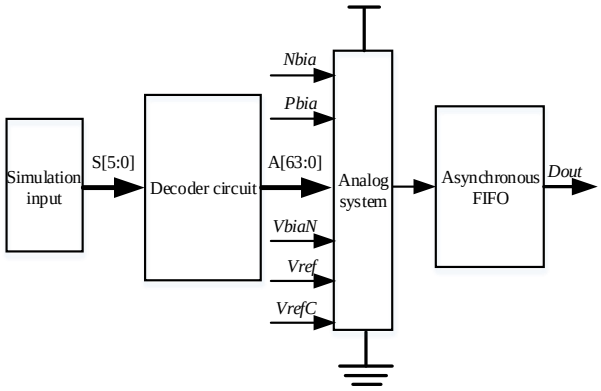

Figure 9. Schematic of digital-analog mixed post-simulation.

In Figure 10, (a) shows the input of the digital decoder, and the number represents the logical value of the input; (b) is the input clock signal of the dynamic latch comparator in the analog system circuit; (c) is the output signal of the RTN source unit; and (d) is the output comparison result of the dynamic latched comparator. It can be confirmed that there is a trap in the MOSFET oxide layer of the noise source circuit when the input logic value of the decoder is one or three, which can generate RTN and a random sequence. On the contrary, there is no trap in the MOSFET oxide layer of the noise source circuit when the input logic value of the decoder is zero or four. Therefore, the output value of the comparator is always zero. It can be seen from the mixed simulation that the digital circuits can match the analog circuits to achieve the expected function.

Figure 11 shows the waveform of random bit streams generated by TRNGs with different frequencies of selecting noise array circuits in 20 ms. It can be found that the frequency of random bit streams remains steady when the frequency of selecting noise circuits is lower than 1 kHz. This is the frequency of the RTN noise. The frequency of random bit streams will increase significantly when the frequency of selecting noise circuits increases. Additionally, within a certain range, the frequency of random bit streams is equal to the frequency of selecting noise circuits, where (a) is the random bit streams generated by selecting one noise circuit; (b) is the random bit streams generated by selecting noise circuits with a frequency of 1 kHz; (c) is the random bit streams generated by selecting noise circuits with the frequency of 4 kHz; and (d) is the random bit streams generated by selecting noise circuits with a frequency of 16 kHz.

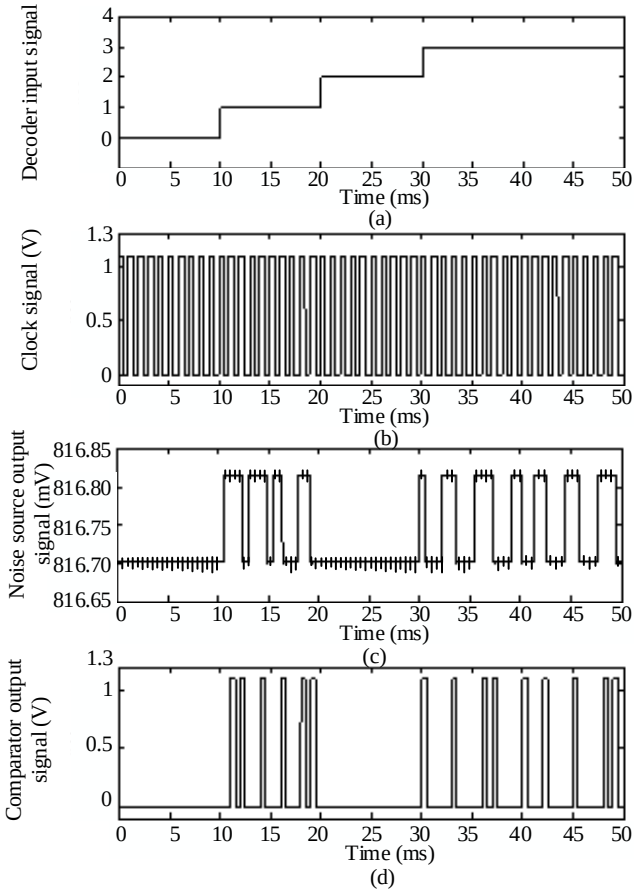

Figure 10. Digital-analog mixed post-simulation waveform.

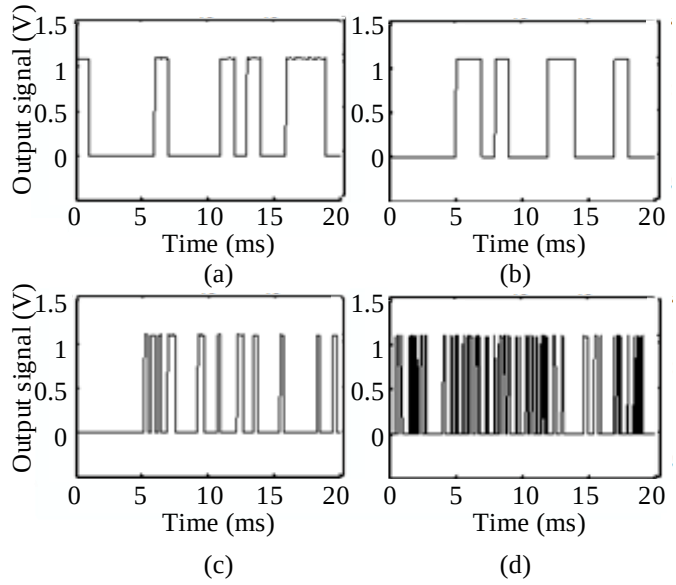

Figure 11. Digital-analog mixed post-simulation waveform.

4. Discussion

The method of probability and statistics was used to detect random numbers. The test procedure issued by the National Institute of Standards and Technology (NIST) is one of the standards for randomness testing [10]. The random numbers of 100 Mbit generated by the TRNG were tested. The results of the randomness testing are shown in Table 1.

Table 1. National Institute of Standards and Technology (NIST) randomness testing results.

Random Detection	*p*-Value	Random Detection	*p*-Value
Frequency Test	0.4372	Maurer Test	0.6787
Frequency Test within a Block	0.1909	Lempel-Ziv Compression Test	0.2023
Runs Test	0.6329	Linear Complexity Test	0.7792
Test for the Longest Run of Ones in a Binary Matrix Rank Test	0.9114	Serial Test	0.4001
Binary Matrix Rank Test	0.4373	Approximate Entropy Test	0.4453
Discrete Fourier Transform Test Matching Test	0.1025	Cumulative Sums Test	0.8141
Non-overlapping Template Matching Test	0.9879	Random Excursions Test	0.5955
Overlapping Template Matching Test	0.1816	Random Excursions Variant Test	0.7981

The NIST algorithm includes 16 detection items which describe the randomness of the sequence from different aspects. The final judgment of each detection item usually uses the *p*-value method. It can be confirmed that a detection item passes the randomness testing if its *p*-value is larger than the value of α. The significance level of α is 0.1 [10].

The results showed that the random numbers generated by the TRNG which was been designed in this paper passed the randomness testing. The quality of random numbers is higher.

The processes of collecting, processing, converting, and storing RTN signals are focused on in this paper. The design and implementation of low-noise budget amplifiers, high-pass filters, and dynamic latch comparators were studied. There is also an asynchronous FIFO module which stores the random number sequence. The method of controllable frequency for the final random number sequence was proposed by using noise source arrays and switch gating. The conformity between the RTN signal in the actual circuits and the adopted model and the randomness of the RTN signals are not the focus of this paper.

5. Conclusions

The proposed TRNG designed by combining digital and analog circuits achieved controllable frequency by generating random numbers. The simulation showed that the frequency can be controlled by the speed of selecting noise array circuits. It was verified that more noise circuits can be used in the array circuits to increase the throughput rate. The randomness testing of the random numbers generated by the TRNG indicates that they are true random numbers.

Author Contributions: X.W. (Xinsheng Wang) was in charge of the implementation and circuit structure; X.W. (Xiyue Wang) was in charge of implementing the simulation and testing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: We would like to thank the Harbin Institute of Technology (HIT), China.

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

References

1. Tehranipoor, F.; Yan, W.; Chandy, J.A. Robust hardware true random number generators using DRAM remanence effects. In Proceedings of the 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, USA, 3–5 May 2016; pp. 79–84.
2. Brederlow, R.; Prakash, R.; Paulus, C.; Thewes, R. A low-power true random number generator using random telegraph noise of single oxide-traps. In Proceedings of the 2006 IEEE International Solid State Circuits Conference—Digest of Technical Papers, San Francisco, CA, USA, 6–9 February 2006; pp. 1666–1675.
3. Chen, X.; Wang, L.; Li, B.; Wang, Y.; Li, X.; Liu, Y.; Yang, H. Modeling Random Telegraph Noise as a Randomness Source and its Application in True Random Number Generation. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* **2016**, *35*, 1435–1448. [CrossRef]
4. Figliolia, T.; Julian, P.; Tognetti, G.; Andreou, A.G. A true random number generator using RTN noise and a sigma delta converter. In Proceedings of the 2016 IEEE International Symposium on Circuits and Systems (ISCAS), Montreal, QC, Canada, 22–25 May 2016; pp. 17–20.
5. Brown, J.; Gao, R.; Ji, Z.; Chen, J.; Wu, J.; Zhang, J.; Zhou, B.; Shi, Q.; Crowford, J.; Zhang, W. A low-power and high-speed True Random Number Generator using generated RTN. In Proceedings of the IEEE Symposium on VLSI Technology, Honolulu, HI, USA, 18–22 June 2018; pp. 95–96.
6. Luo, M.; Wang, R.; Guo, S.; Wang, J.; Zou, J.; Huang, R. Impacts of random telegraph noise (RTN) on digital circuits. *IEEE Trans. Electron. Devices* **2015**, *62*, 1725–1732.
7. Buisson, O.R.D.; Ghibaudo, G.; Brini, J. Model for drain current RTS amplitude in small-area MOS transistors. *Solid-State Electron.* **1992**, *35*, 1273–1276. [CrossRef]
8. Simoen, E.; Dierickx, B.; Claeys, C. Hot-Carrier degradation of the Random Telegraph Signal amplitude in submicrometer Si MOSTs. *Appl. Phys. A* **1993**, *57*, 283–289. [CrossRef]
9. Jolly, R.D.; Mccharles, R.H. A low-noise amplifier for switched capacitor filters. *IEEE J. Solid-State Circuits* **1983**, *17*, 1192–1194. [CrossRef]
10. Paul, R.; Dey, H.; Chakrabarti, A.; Ghosh, R. NIST Statistical Test Suite. *arXiv* **2016**, 1–4. Available online: https://arxiv.org/pdf/1609.01389v1.pdf (accessed on 17 October 2019).