electronics

Article

Behavioral Analysis and Immunity Design of the RO-Based TRNG under Electromagnetic Interference

Zhiwen Zhang and Tao Su *

School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou 510006, China; zhangzhw25@mail2.sysu.edu.cn
* Correspondence: sutao@mail.sysu.edu.cn

Abstract: True random-number generators based on ring oscillators (RO-based TRNG) are widely used in the field of information encryption because of their simple structure and compatibility with CMOS technology. However, radiated or conducted electromagnetic interference can dramatically deteriorate the randomness of the output bitstream of the RO-based TRNG, which poses a great threat to security. Traditional research focuses on the innovation of the means of attack and the detection of circuit states. There is a lack of research on the interference mechanism and anti-interference countermeasures. In this paper, the response of the RO array to electromagnetic interference was analyzed, and the concept of synchronous locking was proposed to describe the locking scene of multiple ROs. On the basis of synchronous locking, the RF immunity of the RO-based TRNG was modeled, which can explain the degradation mechanism of bitstream randomness under RFI. Moreover, the design method of gate-delay differentiation is presented to improve the RF immunity of the RO-based TRNG at a low cost. Both transistor-level simulation and board-level measurement proved the rationality of this scheme.

Keywords: electromagnetic interference; ring oscillator; true random-number generator; injection locking

Citation: Zhang, Z.; Su, T. Behavioral Analysis and Immunity Design of the RO-Based TRNG under Electromagnetic Interference. *Electronics* **2021**, *10*, 1347. https://doi.org/10.3390/electronics10111347

Academic Editor: Flavio Canavero

Received: 28 April 2021
Accepted: 1 June 2021
Published: 4 June 2021

1. Introduction

Integrated circuits under electromagnetic interference (EMI) are widely studied. The subject can be divided into the propagation of electromagnetic-interference waves and the interaction between electromagnetic interference and integrated circuits. The mechanism of the response of an integrated circuit to EMI can inspire the design of anti-interference circuits, which prevent interference damage. As a typical integrated circuit, true random-number generators based on a ring oscillator (RO-based TRNG) are widely used to generate secret keys in the field of security encryption because of their simple circuit structure and compatibility with CMOS technology.

RO-based TRNGs were first proposed by Sunar et al. [1]. Their randomness is generated by sampling the RO oscillating signal with random jitter, which is caused by physical noise. First, multiple oscillating signals are generated by an RO array. An exclusive OR (XOR) operation is performed between every two oscillating signals, and operations are repeated until there is only one output. Then, a D flip-flop is used to sample the XOR operation output, as shown in Figure 1a. Because jitter accumulates with time, sampling signal f_s should be of a lower frequency. Wold et al. [2] proposed an improved RO-based TRNG. Compared with the original structure, only a D flip-flop was added at the output end of each RO, as shown in Figure 1b. The output bitstream of the TRNG directly met the randomness test [3] and did not need to be optimized by the post-processing program. Therefore, the improved structure was adopted in this paper to study electromagnetic interference.

Published studies show that RO-based TRNGs are quite vulnerable to EMI. The randomness of its output bitstream is severely damaged when ROs are locked and jitter is suppressed. Markettos and Moore [4] first injected a continuous wave into the power wire of an RO-based TRNG and reduced the keyspace of a secure microcontroller containing an RO-based TRNG from 264 to 3300. Bayon et al. [5,6] implemented a contactless electromagnetic-wave attack on RO-based TRNG. Compared with the conducted injection-attack method in [4], it was not limited to the low-pass filtering effect of the power-supply pin, and the interference-frequency range was greatly enhanced. The RO-based TRNG in [6] was implemented on a FPGA chip, which contained up to 50 ROs, so it was more universal and persuasive. Osuka et al. [7] coupled a sinusoidal EMI wave to a power cable through a current probe, where the power cable transmitted the interference into the chip. This could implement a long-distance interference injection, destroy the randomness of an RO-based TRNG, and leave no invasion evidence. These conducted and radiated interference methods could lock ROs and destroy the entropy source. However, the injection-locking conditions and the mechanism of randomness degradation are not clear. Some anti-interference methods based on the algorithm level were proposed [8,9], but there is still a lack of countermeasures based on the circuit-design level.

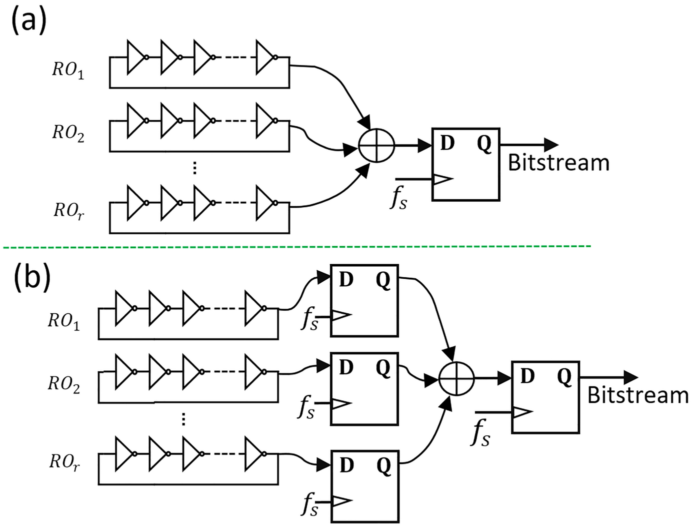

Figure 1. RO-based TRNG. (**a**) Original circuit in [1]; (**b**) improved circuit in [2].

The degradation of bitstream randomness is highly relevant to the status of ROs. A ring oscillator (RO) is composed of an odd number of inverters that are the minimal delay unit in the digital circuit. It is widely used in noise-waveform detection [10] and on-chip process sensing [11] because of its high sensitivity. Studies on the injection locking of ROs under EMI already exist. The authors in [12–15] injected interference from the signal port or the tail-current port of an RO, which differed from the interference-injection scene of the RO-based TRNG. ROs in the above papers also were not composed of complementary metal–oxide semiconductors (CMOS). Mureddu et al. [16] built RO circuits on an FPGA board and injected interference coupled from a delay line. Detailed experiments were carried out on different series of FPGAs. Tao Su et al. [17,18] directly injected interference from the power-supply port of CMOS inverter-based ROs and discovered and explained the injection-pulling and -locking phenomenon. In the above studies, the power-side-injecting method was closest to the real interference situation. The RO-based TRNG contains an array of ring oscillators, in which RO stages may be the same or different. This requires that we focus on the locking behavior of the whole RO array.

This paper supplemented and discussed aspects that were not considered in existing research, and it is arranged as follows: Section 2 introduces the experimental locking conclusion of an RO with EMI on the power supply and puts forward the concept of the locking region. The theory of synchronous locking for the situation of a locked RO array was proposed to explain the overall behavior. In Section 3, the degradation mechanism of the TRNG bitstream is analyzed and verified by simulation. To improve electromagnetic immunity, the electromagnetic immunity of the RO-based TRNG was modeled. A design scheme, gate-delay differentiation, was proposed to improve immunity. Section 4 contains the PCB measurement where the gate-delay-differentiation scheme was verified to be effective. Section 5 is the conclusion.

2. Injection Locking of Ring Oscillators

2.1. Conical Locking Region

According to our previous research, there are two behaviors of the RO with EMI on the supply, as shown in Figure 2a: injection pulling [17] and injection locking [18]. In Figure 2b, injection pulling means that the oscillating frequency of RO f_{RO} shifts towards a higher or lower frequency with the increase in sinusoidal interference amplitude A_{RFI}. A shift towards a higher or lower frequency depends on the f_{RFI} value. In Figure 2c, injection locking means that the RO is out of a frequency-shifting state, and f_{RO} is locked to a constant value. Changing A_{RFI} does not affect f_{RO}. f_{RO_free} and f_{RO_locked} represent the free-oscillating frequency and locked frequency of the RO, respectively.

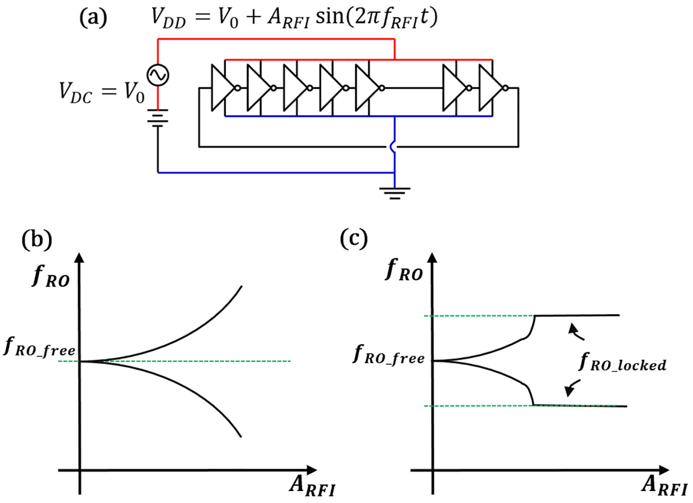

Figure 2. Interference scene and response. (**a**) Interference injection from the power supply; (**b**) injection-pulling phenomenon; (**c**) injection-locking phenomenon.

With massive and detailed simulation and measurement verification, an empirical injection-locking condition was summarized [18], which can be expressed by the relationship between interference period T_{RFI} and average gate-delay τ_{ave}:

$$T_{RFI} = m\tau_{ave} \tag{1}$$

m is a positive integer indicating different locking modes. The locking strength and locking range of the RO are the largest with the mode where m is equal to two. In the following discussion, we defaulted to the fact that m was equal to two because of its high representativeness. If the mode of $m = 2$ has high immunity, modes with a smaller locking range are more robust. The RO consisted of an odd number of inverters, so period T_{RO}:

$$T_{RO} = 2N\tau_{ave} \tag{2}$$

The RO stage is denoted as N. According to Equations (1) and (2), the relationship between f_{RFI} and f_{RO_locked} when the RO is locked is deduced as follows:

$$f_{RO\_locked} = \frac{m}{2N} f_{RFI} \tag{3}$$

The larger f_{RFI} is, the larger f_{RO_locked} is. The response curves of the RO to A_{RFI} under different f_{RFI} are shown in Figure 3. As shown in Equation (3), the theoretical f_{RO_locked} can be calculated from f_{RFI}. When the offset of f_{RO_locked} from f_{RO_free} is small, the RO can be locked with small interference; the larger the offset is, the larger A_{RFI} is needed to lock the RO. When even the maximal A_{RFI} cannot lock the RO, the response curve is only determined by the pulling effect. Therefore, we can obtain a conical locking region from which we can infer the A_{RFI} and f_{RFI} needed to lock the ROs. Any combination of interference A_{RFI} and f_{RFI} outside the region cannot lock the RO.

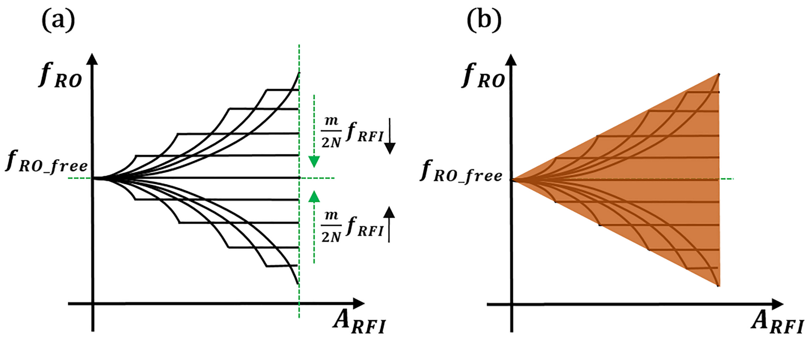

Figure 3. Derivation of the conical locking region. (**a**) Response curves under different f_{RFI}; (**b**) conical locking region.

To prove the existence of the conical locking region, four 41-stage ROs were built with the SMIC-65, SMIC-130, SMIC-180, and TSMC-180 nm process libraries, respectively. The response curves of f_{RO} to A_{RFI} under different interference frequencies f_{RFI} was simulated by HSPICE, and the locking regions were obtained, as shown in Figure 4. The f_{RO_free} of the four ROs were 1085, 555, 259, and 257 MHz, respectively. The locking region was approximately conical. The locked frequency with A_{RFI} equal to 0.5 V and the interference frequency were recorded and converted into the average gate-delay and interference period, as shown in Figure 5. The dotted line represents the empirical relationship in (1), with m equal to two. The ROs of different CMOS processes occupied different positions, where the advanced SMIC-65 nm process had the minimal average gate-delay. When RO locking occurs, the average gate-delays of all ROs linearly increased with the interference period, and the curves coincided with the dotted line. When the RO was released from the locking state, it was out of the linear relationship and dominated by injection pulling, as shown by the SMIC-180 nm and TSMC-180 nm curves in Figure 5. The simulation results were consistent with those of theoretical analysis.

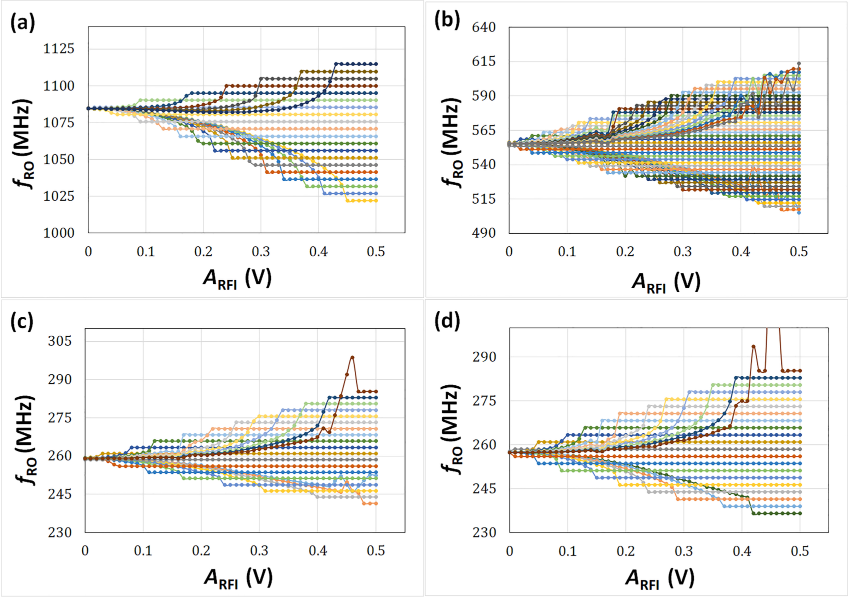

Figure 4. Conical locking regions of the 41-stage ROs under different CMOS processes. (**a**) SMIC-65 nm process; (**b**) SMIC-130 nm process; (**c**) SMIC-180 nm process; (**d**) TSMC-180 nm process.

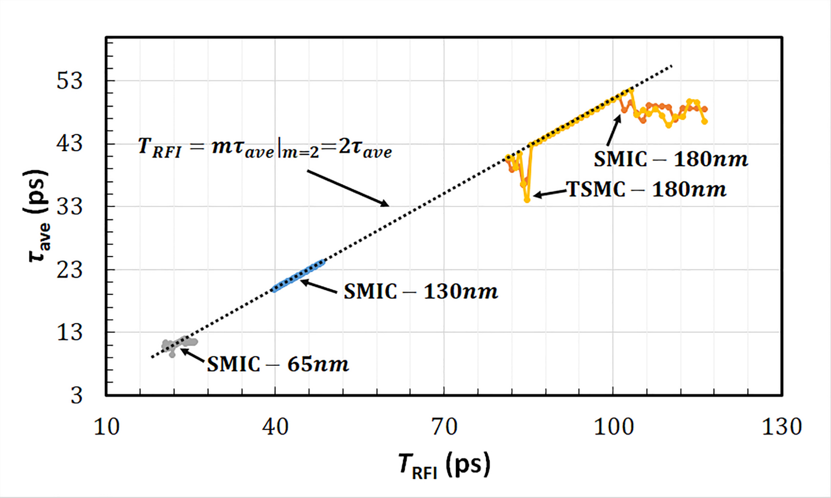

Figure 5. Relationship between interference period and average gate-delay. A_{RFI} is equal to 0.5 V, and m is equal to 2.

2.2. Synchronous Locking of the Ring Oscillator Array

In the above section, empirical Equation (1) shows the interference condition to lock an RO. This locking condition is different from traditional LC oscillator injection locking. It is the integral of multiple relationships between the period of the interference signal and the average gate-delay of the RO, whereas traditional LC locking is the harmonic relationship between frequencies. The injection-locking condition does not contain any RO stage information. This means that, as long as the gate-delay or the process, voltage, and temperature (PVT) condition of the RO are consistent, locking always appears. This is a novel and interesting locking phenomenon.

To verify the locking independent of stage, forty-one-, forty-three-, and forty-five-stage ROs of the SMIC-65, SMIC-130, SMIC-180, and TSMC-180 nm processes, respectively, were implemented and simulated by HSPICE. With the interference frequency of 43,050 MHz, the response curves of the RO to A_{RFI} were obtained and are shown in Figure 6. The f_{RO_locked} and τ_{ave} values were recorded and are listed in Table 1. To emphasize the stage independent of RO locking, τ_{ave} values are marked red.

Table 1. Simulation results of stage-independent locking with different CMOS processes, f_{RFI} = 43,050 MHz.

	SMIC-65 nm			**SMIC-130 nm**		
	41-Stage	**43-Stage**	**45-Stage**	**41-Stage**	**43-Stage**	**45-Stage**
f_{RO_locked} (MHz)	1050	1001	957	540	515	492
τ_{ave} (ps)	11.61	11.61	11.61	22.58	22.58	22.58
	SMIC-180 nm			**TSMC-180 nm**		
	41-Stage	**43-Stage**	**45-Stage**	**41-Stage**	**43-Stage**	**45-Stage**
f_{RO_locked} (MHz)	250	238	228	250	238	228
τ_{ave} (ps)	48.78	48.78	48.78	48.78	48.78	48.78

For the SMIC-65 nm RO simulation case, the free-oscillating frequencies of the three ROs were 1084, 1034, and 988 MHz, which were locked to 1050, 1001, and 957 MHz, respectively. The calculation results of the average gate-delays were 11.61 ps, which is satisfied with Equation (1), with m equal to two. Therefore, the curves of oscillating frequency vs. interference amplitude in Figure 6(a1) can be transformed into the curves of average gate-delay vs. interference amplitude in Figure 6(a2), and all the curves coincide. In the SMIC-130, SMIC-180, and TSMC-180 nm RO simulation results, it showed the same characteristic. If the intrinsic gate-delay of the RO was the same, they were pulled and locked to the same value. Therefore, this locking mechanism was independent of RO stage.

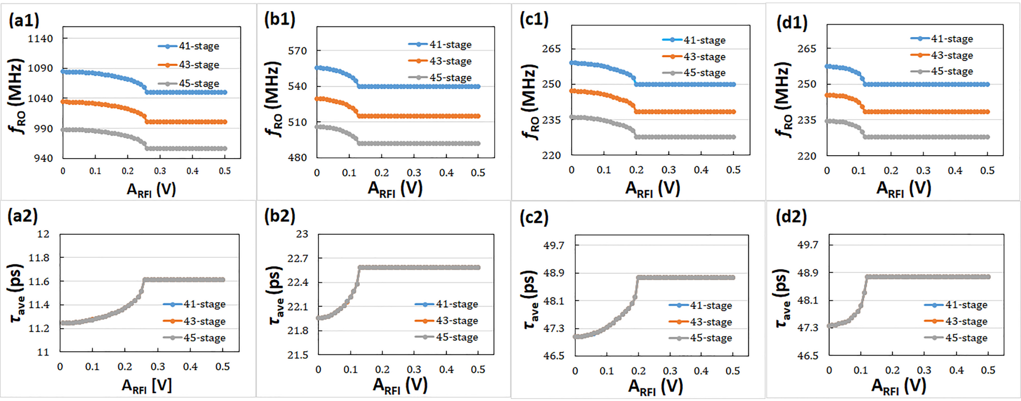

Figure 6. Stage-independent verification of locking: (**a1**) frequency response of the SMIC-65 nm process; (**a2**) average gate-delay response of the SMIC-65 nm process; (**b1**) frequency response of the SMIC-130 nm process; (**b2**) average gate-delay response of the SMIC-130 nm process; (**c1**) frequency response of the SMIC-180 nm process; (**c2**) average gate-delay response of the SMIC-180 nm process; (**d1**) frequency response of the TSMC-180 nm process; (**d2**) average gate-delay response of the TSMC-180 nm process.

An RO array scenario was considered in which the average gate-delay of each RO was the same. From the above analysis of stage-independent locking, as long as the A_{RFI} can lock one RO of the array, it locks the other ROs regardless of stage discrepancy. In other words, the synchronous locking phenomenon occurs. For the RO array on the actual chip, the average gate-delay of each RO was slightly different due to the fluctuations of PVT condition, but this subtle difference could be overcome by intentional EMI. Lastly, with a suitable interference condition, all ROs in the array were synchronously locked.

As shown in Figure 7, the 22,550 MHz sinusoidal interference was injected into the power-supply port of a 41-stage RO. To simulate the effect of process deviation, the width of the NMOS and PMOS in the inverter was intentionally modified from the size of the SMIC-130 nm inverter standard cell INVX1 (w_n = 0.42 μ, w_p = 0.64 μ) to w_n = 1.62 μ, w_p = 2.47 μ. The response curves of each size were recorded by the simulation.

Figure 7a shows that the free-oscillating frequencies of the RO with different inverter sizes were slightly different. With the increase in interference amplitude, all ROs could be locked to 550 MHz, which conformed to the conclusion of Equation (3). The more the oscillating frequency deviated from 550 MHz, the greater the interference amplitude that was required for locking. The response curves of average gate-delay to interference amplitude are shown in Figure 7b. The difference in gate-delay caused by intentional process deviation can be overcome by electromagnetic interference, and the oscillator system was synchronously locked.

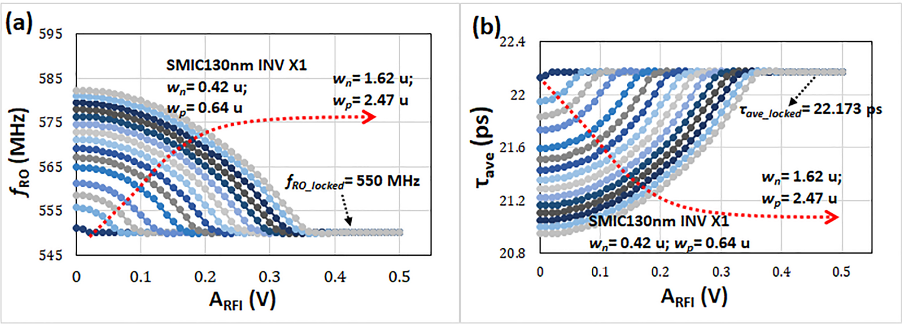

Figure 7. Synchronous locking verification of the 41-stage RO with process deviation. (**a**) Frequency-response curves; (**b**) average gate-delay-response curves.

3. RO-Based TRNG Immunity Modeling and Optimization

3.1. RO-Based TRNG Randomness-Degradation Mechanism

Both radiated and conducted interference can suppress the jitter of ROs and degenerate the randomness of the RO-based TRNG. As shown in Figure 8, the uncertain logic value can be sampled when the oscillating signal of the RO jitters. Otherwise, the D flip-flops the certain logic, which means that the output is not random. With the RO array, the jitter range covers the whole sampling period [1]. Good-quality random bitstreams can be generated by the TRNG. When the RO-based TRNG was disturbed by intentional EMI, the ROs were locked, and the jitter was suppressed [7], as shown in Figure 8d. Therefore, the randomness of the output bitstream deteriorated.

The reason for this disastrous result was that the injection-locking condition of the RO was independent of the stage and only related to the gate-delay. With the same CMOS process, the gate-delays were consistent, and all ROs had to be synchronously locked once locking occurred. Even with the existing process deviation, it was overcome by EMI to achieve synchronization, according to Section 2.2.

To prove the correctness of the above explanation, a specific RO-based TRNG circuit was built using an SMIC-130 nm process library and was simulated by HSPICE in which the array consisted of two ROs of 7, 9, 11, and 13 stages, respectively. To simulate the noise environment in the actual circuit, a −28 dBm Gaussian white-noise voltage was generated in MATLAB, which was superimposed onto the DC power supply of the circuit. Noise voltage was essential to cause the oscillating signal to jitter.

The simulated oscillating parameters are shown in Table 2. The free-oscillating frequencies of the ROs were 3166, 2476, 2034, and 1726 MHz, and the average gate-delay was about 22.56, 22.44, 22.35, and 22.29 ps, respectively, with a slight difference. According to Equation (1), the 22,550 MHz sinusoidal EMI wave could overcome the delay difference and lock all ROs where the average gate-delays were equal to 22.17 ps and oscillating frequencies were fixed to the corresponding values. The standard deviation of the period distribution, which can represent jitter strength, was calculated. Under EMI conditions of 0.35 V and 22,550 MHz, all ROs were locked, and the jitters were 1.14, 1.14, 1.15, and 1.15 ps. Compared with the no-EMI condition in Table 2, jitters were suppressed by 60%, 64%, 67%, and 70%. This phenomenon is also represented by the period-distribution histograms in Figure 9b,d.

Figure 9a,c represents the bitstream output by the TRNG. Black and white pixels are used to represent zero and one, respectively. The binary images can be obtained by scanning the bitstream from left to right and from top to bottom. In the no-EMI case, the binary image was arranged in a disordered manner, which represents a certain degree of randomness. When all ROs were locked by the EMI, the binary image tended to be completely black, and the occurrence probability of zero and one was not uniform. It could not even pass the first test of the NIST Statistical Test Suite [3], which detects whether zero and one appear the same number of times, called the monobit test.

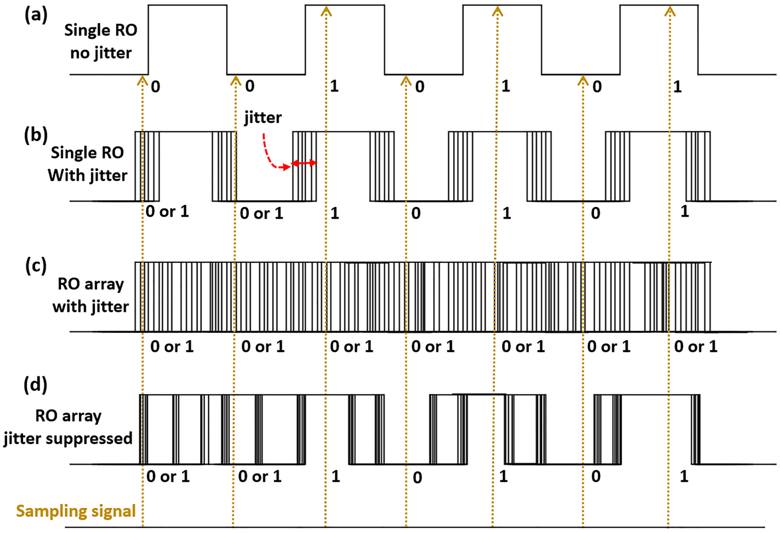

Figure 8. Sampling of the RO oscillating signal. (**a**) Single RO without jitter; (**b**) single RO with jitter; (**c**) RO array with jitter; (**d**) RO array when jitter was suppressed by EMI.

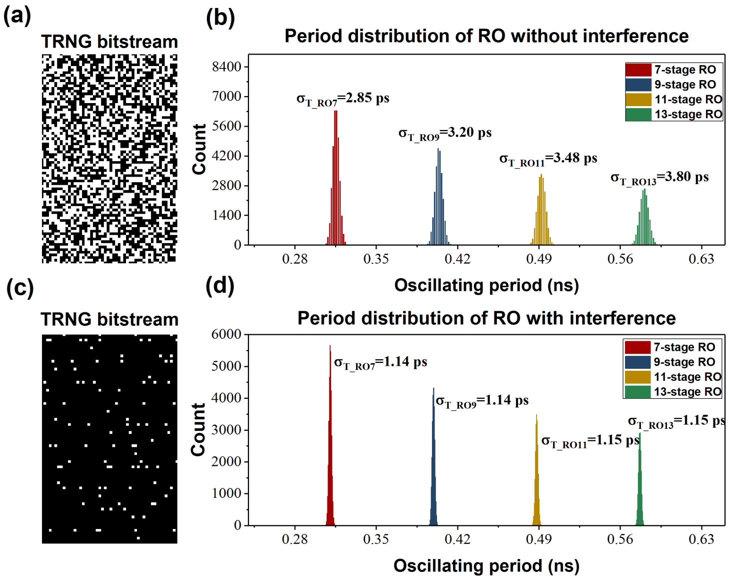

Figure 9. Interference experiment of the RO-based TRNG. (**a**) Output bitstream of the RO-based TRNG without EMI; (**b**) period distribution of the RO without EMI; (**c**) output bitstream of the RO-based TRNG with EMI; (**d**) period distribution of the RO with EMI.

Table 2. Behavioral parameters of the RO in the RO-based TRNG with and without EMI.

	7-Stage RO	9-Stage RO	11-Stage RO	13-Stage RO
f_{RO_free}	3166 MHz	2476 MHz	2034 MHz	1726 MHz
τ_{ave}	22.56 ps	22.44 ps	22.35 ps	22.29 ps
Jitter without EMI	2.85 ps	3.20 ps	3.48 ps	3.80 ps
Jitter with EMI	1.14 ps	1.14 ps	1.15 ps	1.15 ps
Percentage of suppressed jitter	60%	64%	67%	70%

3.2. Immunity Modeling and Gate-Delay Differentiation

To solve the problem of the randomness of the RO-based TRNG deteriorating sharply due to synchronous locking, the design method of gate-delay differentiation was proposed in this paper: the average gate-delay of each RO in the TRNG was intentionally set to be different so that the locking regions of ROs were staggered from each other. This avoided all the ROs being locked in some EMI situations.

An array with four ROs was considered, composed of inverters with different gate-delays. According to the conclusion of Section 2.1, each RO had a conical locking region. Due to the difference in gate-delay, the conical locking regions of the four ROs were staggered, as shown in Figure 10a.

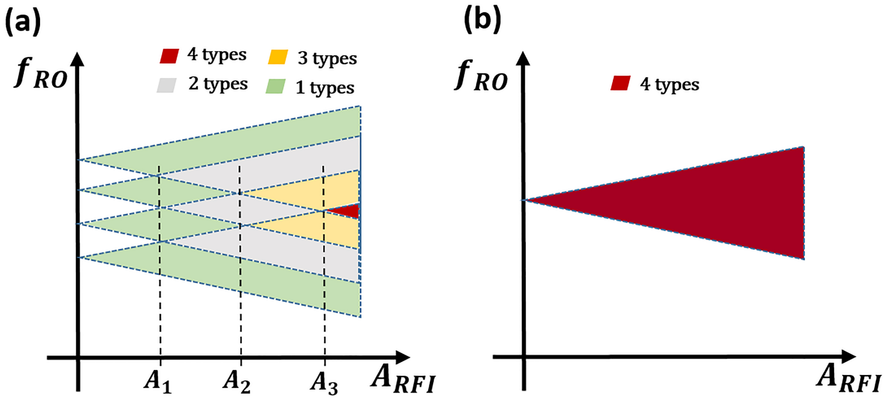

Figure 10. Immunity modeling and comparison of the RO-based TRNG. (**a**) Locking cones staggering with gate-delay differentiation; (**b**) locking cones overlapping without gate-delay differentiation.

The scattered distribution was beneficial to the EMI immunity of the RO-based TRNG:

- To lock all four types of ROs, available f_{RFI} and A_{RFI} can only be selected in the red area, which is the overlapping area of the four conical locking regions. The required A_{RFI} had to be greater than A_3, and the selection of f_{RFI} was also very harsh;
- To lock three types of ROs, the available f_{RFI} and A_{RFI} can only be selected in the yellow area. This required that $A_{RFI} > A_2$, and the available selection range of f_{RFI} was also small;
- To lock two types of ROs, f_{RFI} and A_{RFI} can only be selected from the gray area. In such a case, it required $A_{RFI} > A_1$, and the selection range of f_{RFI} was large. However, randomness did not become much worse because of only two types of ROs being locked;
- To lock one type of RO, f_{RFI} and A_{RFI} can only be selected from the light green area, which is easy to achieve. The influence of one type of RO locked on randomness can be ignored.

In a traditional EM attack on RO-based TRNG, the gate-delays of four types of RO were the same, and there was no staggering between conical locking regions, as shown in Figure 10b. It was easy to realize synchronous locking for all ROs, which was destructive to the RO-based TRNG.

In Figure 10, we considered the locking region of the frequency. Similarly, average gate-delay τ_{ave}, which can be converted from f_{RFI}, also had a conical locking region. It was clearer and more appropriate to analyze the locking situation of the RO array, because the analytical method of τ_{ave} discarded the independent factor of the RO stage, which made it easier for us to see the essence of locking. In the following simulation and test, we used the τ_{ave}-type conical locking region to illustrate this.

To improve immunity, the gate-delay difference of each RO must be increased. The ideal situation is only one type of RO locking under any interference condition. To differentiate gate-delays, changing the channel width of transistors in the inverter, the load of each inverter, and the interconnect length are feasible because of the simplicity of implementation and low cost. Meanwhile, we can flexibly choose the implementation according to the situation: for the RO-based TRNG on application-specific integrated circuits (ASICs), changing the channel width of transistors is the first choice; for the RO-based TRNG on an FPGA, the load of each inverter and the interconnect length are appropriate. For a specific CMOS process, the response of the oscillating RO frequency to different capacitor loads and different transistor sizes can be simulated in advance. According to the response data, suitable capacitor loads and transistor size parameters can be selected and assigned for the ROs. Increasing the number of ROs with different average gate-delays matters, so that there is a smaller proportion of ROs in the locked state.

Therefore, we verified the design method of gate-delay differentiation with HSPICE using the RO-based TRNG circuit in Section 3.1. Two implementation strategies for differentiating gate-delay are shown in Table 3: Case 1 is changing the inverter size, and Case 2 is changing the capacitor load of the inverter. Although increasing the size of the inverter and capacitance load slowed down the circuit and caused additional power consumption, these shortcomings were tolerable compared with the goal of improving immunity.

Table 3. Strategies of differentiation gate-delays.

	7-Stage RO	**9-Stage RO**	**11-Stage RO**	**13-Stage RO**
Case 1	w_n = 0.40 μ; w_p = 0.61 μ	w_n = 0.98 μ; w_p = 1.49 μ	w_n = 2.22 μ; w_p = 3.38 μ	w_n = 7.70 μ; w_p = 11.74 μ
Case 2	C_{load} = 0 fF	C_{load} = 0.13 fF	C_{load} = 0.28 fF	C_{load} = 0.44 fF

For Case 1, the inverters composed of 7-, 9-, 11-, and 13-stage ROs were designed with the sizes in Table 3, which led to different gate-delays. The simulation results are shown in Figure 11. In Figure 11a, the conical locking regions are shown to be staggered. Only when the A_{RFI} > 0.36 V could all ROs in the array be locked. To observe the output bitstream of RO-based TRNG, some representative interferences were selected to realize the locking of 0, 1, 2, 3, and 4 types of RO, respectively; see Table 4 for the interference and jitter information. The jitters of locked ROs, which are marked as red, were much lower than those of unlocked ROs.

Interference seemed to result in two kinds of consequences: one was suppressing jitter, as we know, and the other was intensifying it. In the unlocked state, as shown in the black data, the larger the A_{RFI} was, the more severe the jitter was; in the locked state, as shown in the red data, the larger A_{RFI} was, the more strongly the jitter was suppressed.

Bitstream binary images were obtained, as shown in Figure 11(b1–b5). When there were three or more types of ROs locked, output bitstreams showed strong regularity, and the randomness of the RO-based TRNG was greatly reduced. However, the required A_{RFI} was also large. When only one or two types of RO were locked, the randomness hardly changed. This agreed well with our theoretical analysis. To obtain the quantization results of the randomness, the bitstream was tested in the NIST suite. When three or four types of ROs were locked, the p-value was far less than 0.01, which shows that the randomness was seriously damaged.

Table 4. Case 1: inverter sizes.

$(A_{RFI}, f_{RFI})_n$	Jitters of ROs (ps)			
(V, MHz)	7-Stage	9-Stage	11-Stage	13-Stage
$(0.05, 23{,}700)_0$	3.37	3.92	4.08	3.69
$(0.15, 22{,}500)_1$	1.90	5.73	5.07	4.16
$(0.30, 22{,}800)_2$	1.27	1.31	9.16	5.60
$(0.45, 23{,}100)_3$	0.92	0.87	1.01	9.05
$(0.48, 23{,}370)_4$	0.90	0.81	0.85	1.51

The subscript n in $(A_{RFI}, f_{RFI})_n$ indicates the number of types of locked ROs.

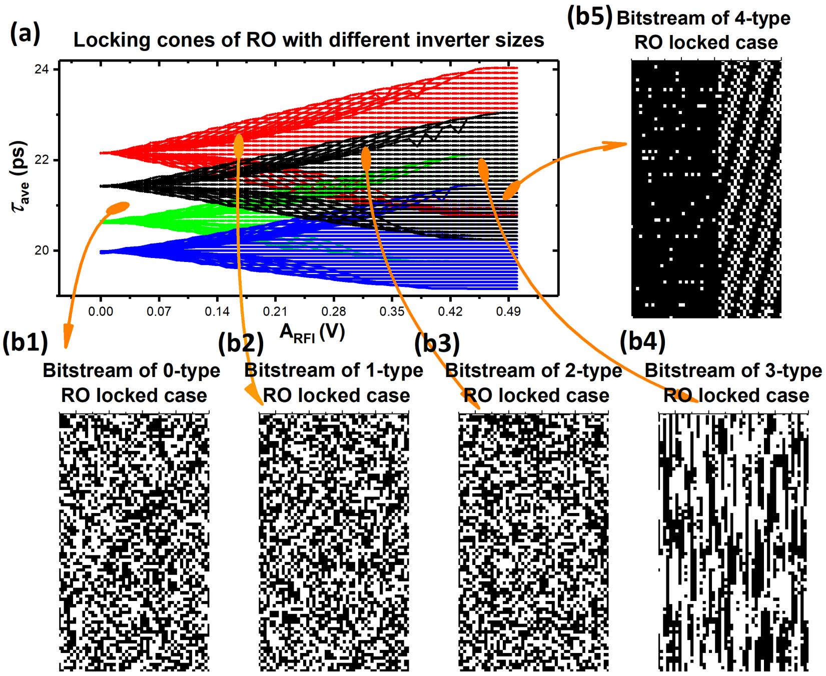

Figure 11. Experiment results of Case 1: changing inverter case. (**a**) Locking cones of ROs with different inverter sizes; (**b1**–**b5**) bitstream maps with different types of ROs locked.

For Case 2, each inverter of the 7-, 9-, 11-, and 13-stage RO was loaded with 0, 0.13, 0.28, and 0.44 fF capacitors, respectively. The simulation results are shown in Figure 12, which were very similar to those of Case 1. Detailed jitter and interference information is shown in Table 5. Adding different capacitor loads can also stagger the locking regions of the ROs to improve electromagnetic immunity.

Table 5. Case 1: capacitor loads.

$(A_{RFI}, f_{RFI})_n$	Jitters of ROs (ps)			
(V, MHz)	7-Stage	9-Stage	11-Stage	13-Stage
$(0.10, 18{,}050)_0$	3.70	4.67	4.75	4.81
$(0.47, 18{,}868)_1$	10.89	13.20	14.77	1.17
$(0.47, 19{,}455)_2$	13.49	13.63	1.20	1.00
$(0.47, 20{,}080)_3$	10.62	1.20	0.99	0.94
$(0.47, 20{,}408)_4$	1.32	1.06	0.96	0.92

Subscript n in $(A_{RFI}, f_{RFI})_n$ indicates the number of types of locked ROs.

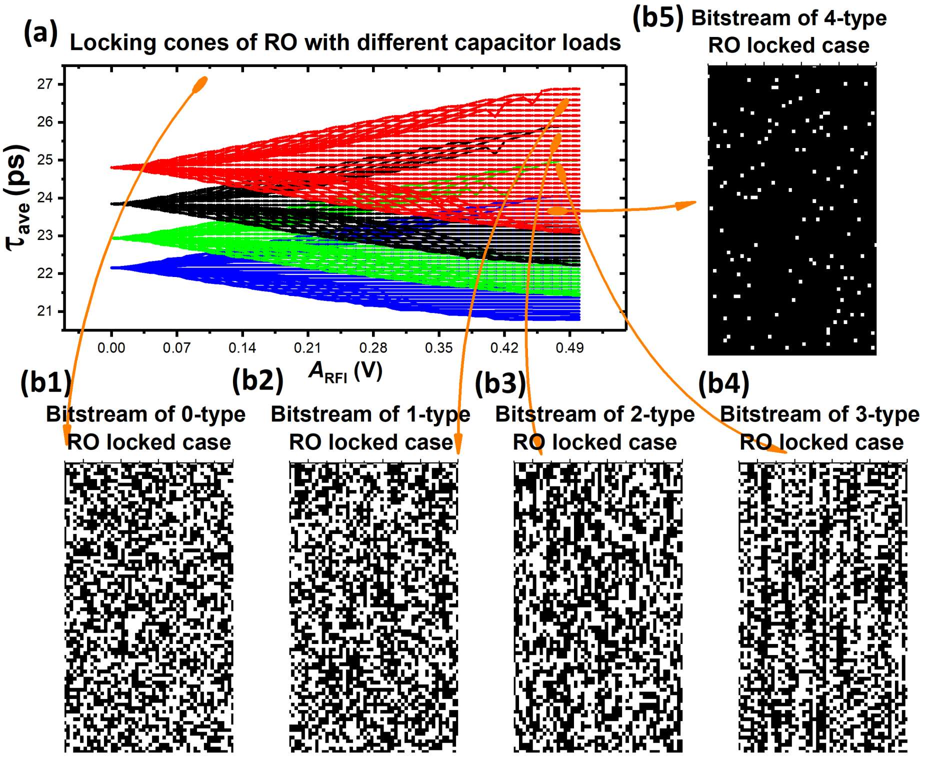

Figure 12. Experiment results of Case 2: changing capacitor load case. (**a**) Locking cones of ROs with different capacitor loads; (**b1**–**b5**) bitstream maps with different types of ROs locked.

To prove that the design method of gate-delay differentiation to improve the immunity did not depend on the CMOS process, the RO-based TRNG built with SMIC 65-nm was simulated by HSPICE. The circuit setting was the same as Case 2 in the above experiment. To simulate such a situation, the corresponding average gate-delays of ROs loaded with 0, 0.037, 0.074, and 0.111 fF capacitors were 11.90, 12.25, 12.59, and 12.94 ps. According to Equation (1), these ROs could be locked by the interference of 41,700, 40,300, 39,300, and 38,300 MHz, respectively. This suggested that if the inverters in TRNG were loaded with the same capacitors as above, all the ROs would be locked synchronously, and the randomness deteriorated, as shown in Figure 13(c1–c4). If each inverter of the 7-, 9-, 11-, and 13-stage RO was loaded with 0, 0.037, 0.074, and 0.111 fF capacitors, respectively, the locking regions were staggered, as shown in Figure 13a. The same interference conditions above could not lock all the ROs synchronously, and the randomness of the bitstream did not become worse, which can be seen in Figure 13(b1–b4). The results proved that the improvement of immunity was independent of the CMOS process.

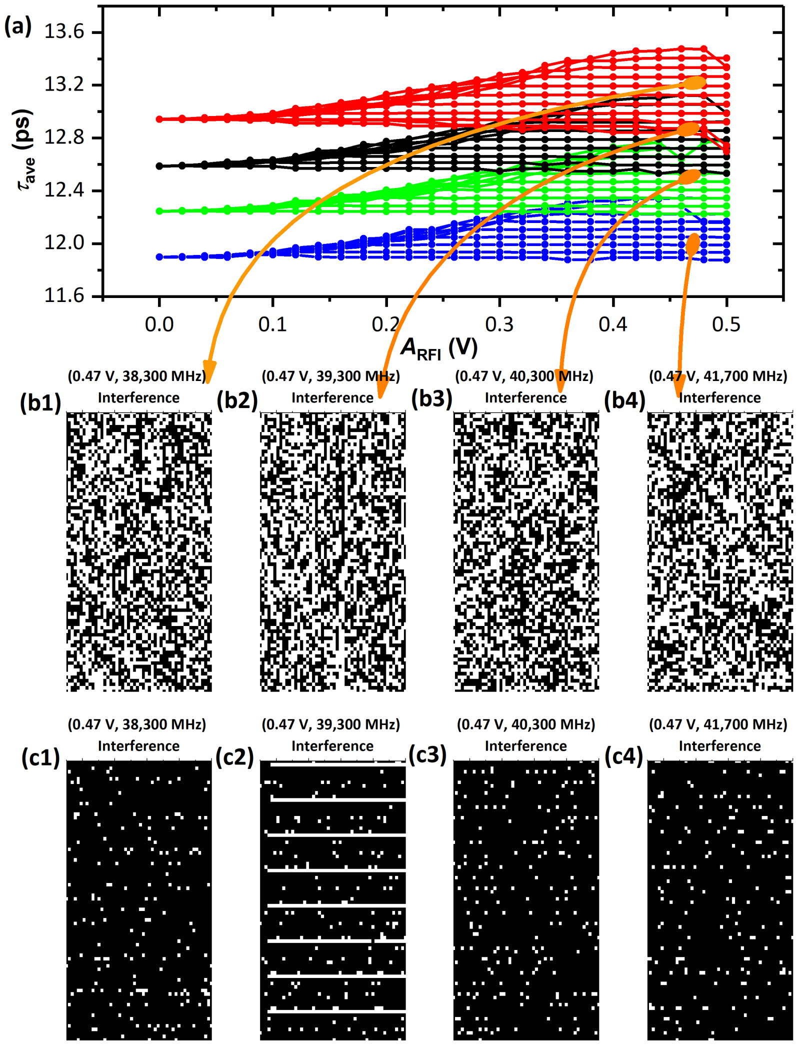

Figure 13. CMOS process-independent verification: (**a**) locking cones of ROs with different capacitor loads; (**b1**–**b4**) bitstream maps with different capacitor loads; (**c1**–**c4**) bitstream maps with all ROs loaded with 0, 0.037, 0.074, or 0.111 fF capacitors, respectively.

4. Measurement

In this section, the measurement of the design method for gate-delay differentiation to verify its feasibility is described. On a printed circuit board (PCB), the 7-, 9-, 11-, and 13-stage RO circuits were built with the single inverter chip SN74LVC1G04DBVR. Some design considerations were as follows: For the convenience of controlling the gate-delays of the ROs and the consistency of A_{RFI} reaching the power-supply port of each inverter, inverters in the same RO were arranged in a circle, and the spacing between adjacent inverters was strictly equal. The wiring length from the interference injection SMA connector to the power-supply port of the inverter should be equal. In order to not affect the uniform load of the ROs, an inverter was applied at the output port of each inverter in the bottom layer to isolate the oscillating circuit from the observation circuit. The circuit structure is shown in Figure 14. The D flip-flops and the XOR-tree circuits were implemented on an XC7A100t chip (Xilinx Artix-7 FPGA). The test platform is shown in Figure 15. The PC controlled the interference source to generate an interference wave with a specific frequency and amplitude, which was injected into the RO array board through a power amplifier, an isolator, and an attenuator. The attenuator was mainly used to weaken the reflection wave caused by the board and protect the amplifier. Similarly, the PC also controlled the oscilloscope and FPGA for data acquisition.

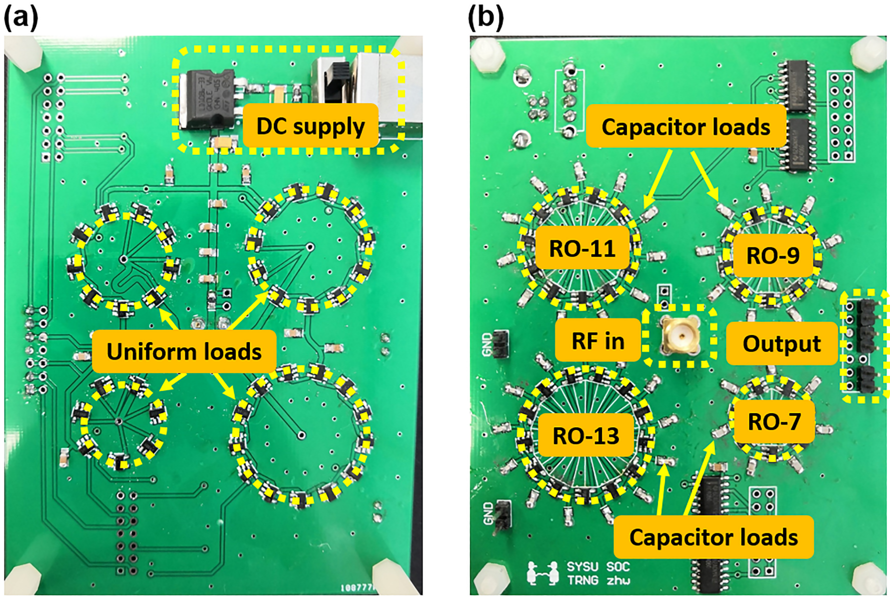

Figure 14. RO array at the PCB level. (**a**) PCB bottom layer; (**b**) PCB top layer.

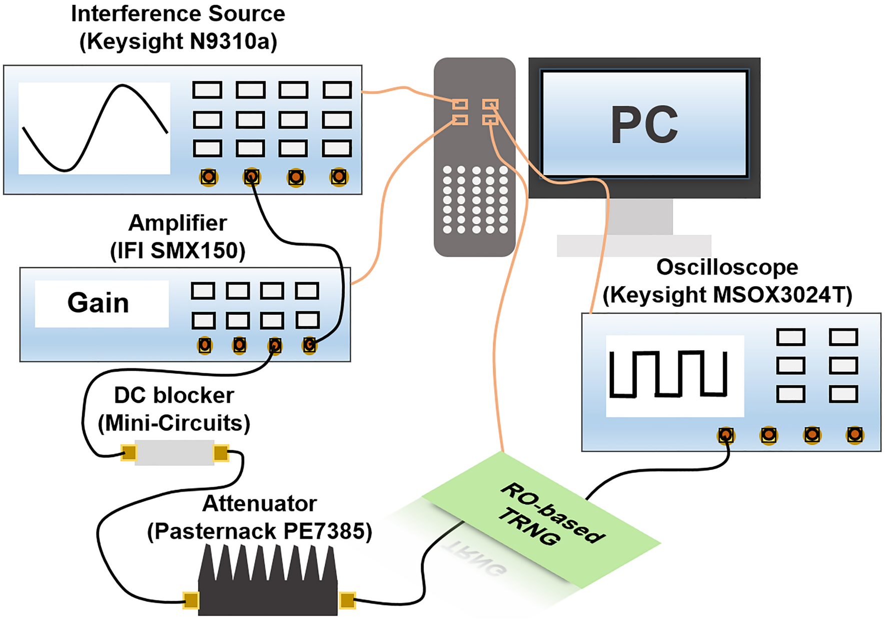

Figure 15. Test platform.

For the control group, each inverter in the RO array was loaded with a 120 pF capacitor. Under the same load, the free oscillation frequencies of the 7-, 9-, 11-, and 13-stage ROs were 21.11, 16.55, 13.26, and 11.21 MHz, respectively. The average gate-delays were 3.38, 3.38, 3.43, and 3.43 ns, which were almost equal. Interference was applied to measure the locking region of each RO, as shown in Figure 16. The locking cones of the four ROs were almost coincidental on the vertical gate-delay axis, which was consistent with the theoretical analysis in Section 2. For this condition, it was very easy to inject interference to lock all ROs in the array and drastically degrade the randomness of the TRNG. There were many interference frequencies and amplitudes from which to choose.

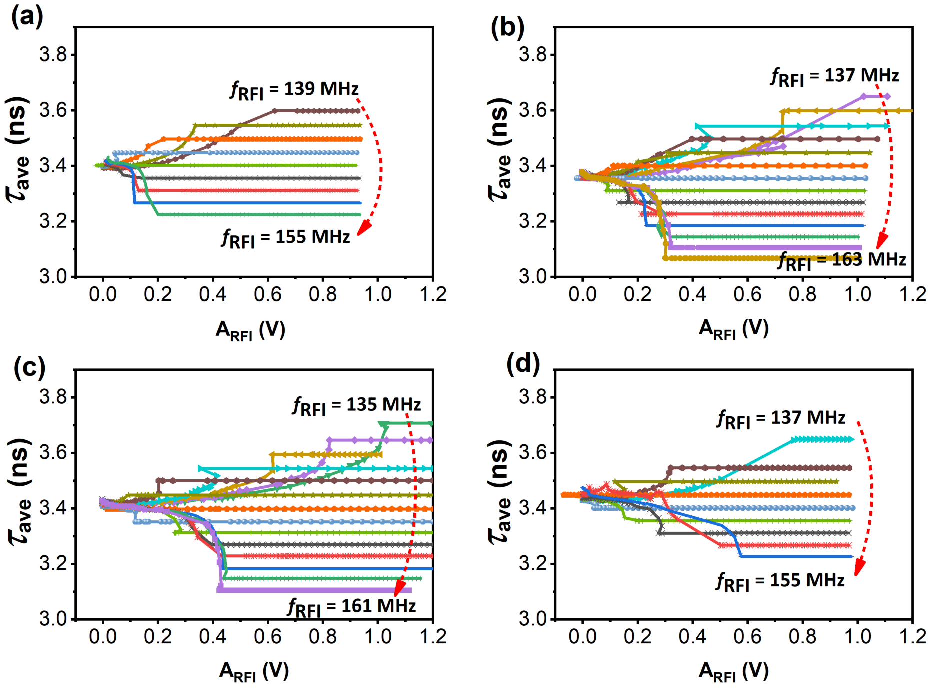

Figure 16. Locking cones of ROs with the same 120 pF capacitor loads: (**a**) 7-stage RO; (**b**) 9-stage RO; (**c**) 11-stage RO; (**d**) 13-stage RO.

Three kinds of interference were selected for comparison: no interference, 0.9 V and 145 MHz, and 0.9 V and 150 MHz. The bitstream is shown in Figure 17. The latter two kinds of interference could easily lock all ROs. Binary images show that, when all ROs were locked, the output bitstream of the TRNG presented a certain regularity. A discrete Fourier transform (DFT) test in the NIST suite was carried out to detect the periodicity of the bitstream. The *p*-value was far less than 0.01, which represents the latter two conditions that destroy the randomness of the TRNG output.

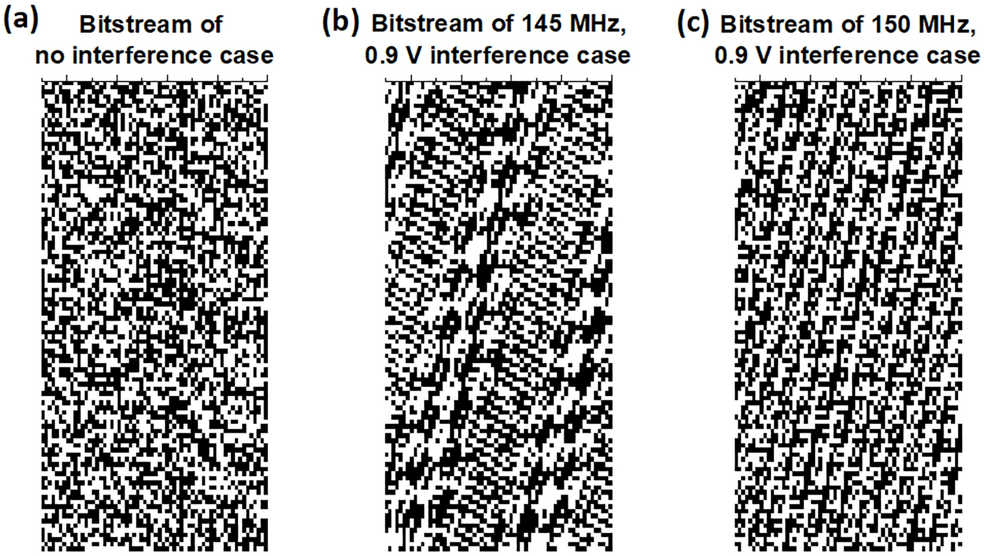

Figure 17. Bitstream of the TRNG under selected interference conditions: (**a**) no interference; (**b**) condition of (A_{RFI}, f_{RFI}) = (0.9 V, 145 MHz); (**c**) condition of (A_{RFI}, f_{RFI}) = (0.9 V, 150 MHz).

For the experience group, we changed the load-capacitance values of the inverters in the four ROs as shown in Table 6. The free-oscillating frequencies of the 7-, 9-, 11-, and

13-stage ROs were 14.28, 13.81, 13.00, and 12.82 MHz, respectively. The average gate-delays were 5.00, 4.02, 3.50, and 3.00 ns, which were quite different. According to theoretical analysis, the locking regions of each RO were staggered in the vertical axis, as shown in Figure 18. It was impossible to lock all four types of ROs within a reasonable range of interference amplitude. At most, two kinds of ROs could be locked. In the range of soft failure caused by EMI, it was impossible to reduce the TRNG randomness. The immunity was greatly improved.

Table 6. Capacitor-load arrangement.

7-Stage RO	9-Stage RO	11-Stage RO	13-Stage RO
C_{load} = 0 fF	C_{load} = 0.13 fF	C_{load} = 0.28 fF	C_{load} = 0.44 fF

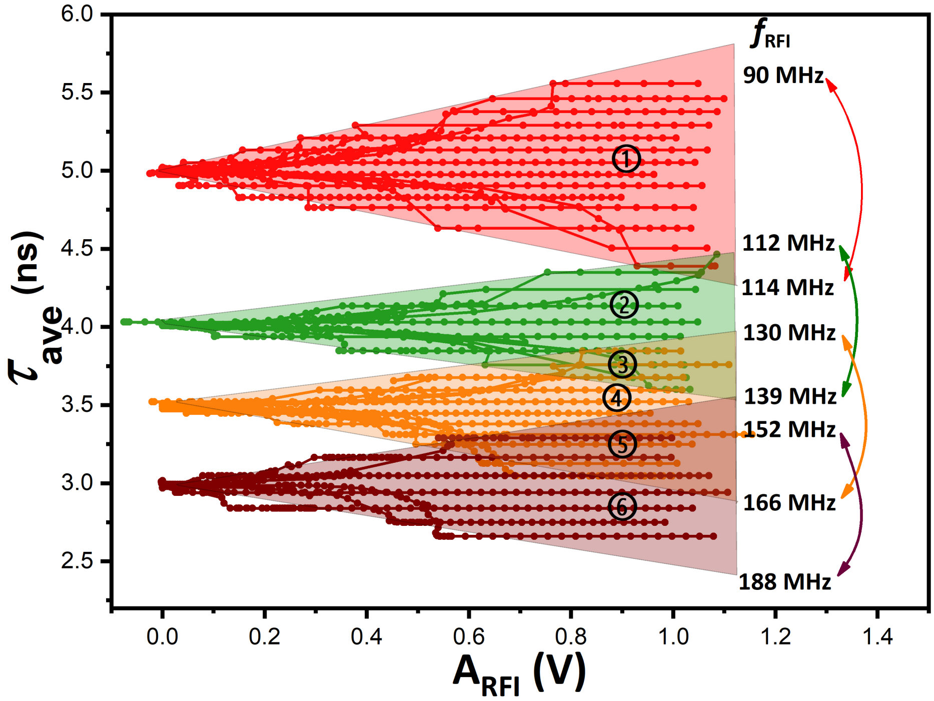

Figure 18. Locking cones of ROs with different capacitor loads.

To prove the above conjectures, the amplitude of the injected interference was maintained at 0.9V, and interference frequencies of 95, 125, 133, 143, 154, and 167 MHz were selected, corresponding to the serial number marked in Figure 18. In addition to the 133 and 154 MHz cases, only one type of RO could be realized. The TRNG binary images are shown in Figure 19. The randomness of the bitstream was greatly improved compared with in the latter two cases of all ROs locked in Figure 17, which was also confirmed by NIST testing. Therefore, we verified the effectiveness of the design method of gate-delay differentiation.

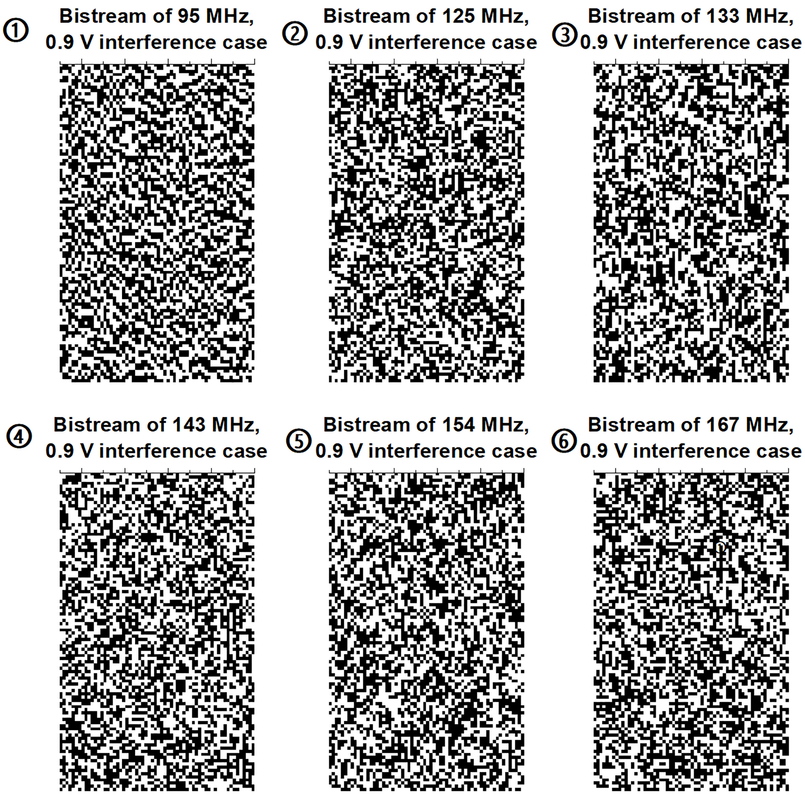

Figure 19. Bitstream of the improved TRNG under the selected interference conditions.

5. Conclusions

This study analyzed the injection locking of an RO array under an EMI wave. Synchronous locking was proposed to summarize the response of an RO array in the RO-based TRNG, which could explain the randomness-deterioration mechanism of the bitstream.

To improve the EM immunity of the RO-based TRNG, the design method of gate-delay differentiation was proposed: by reasonably increasing the gate-delay difference of each RO, the locking regions were staggered, and the situation of most ROs being locked was avoided. The specific implementation methods of changing transistor sizes and capacitance loads were successfully verified by HSPICE simulations and PCB measurements. RO-based TRNG chips could be fabricated in CMOS processes, and the effectiveness of the above implementation methods can be verified in more detail.

Enriching the design method of gate-delay differentiation, the locking phenomenon of a single RO having inverter gates with different propagation delays is our future study direction. This can enrich our understanding of the locking phenomenon and inspire anti-interference research of RO-based TRNGs. We could also integrate the method with electronic design automation (EDA) tools to guide the immunity design of TRNGs.

Author Contributions: Conceptualization, Z.Z. and T.S.; methodology, Z.Z.; software, Z.Z.; validation, Z.Z.; formal analysis, Z.Z.; investigation, Z.Z.; resources, Z.Z. and T.S.; data curation, Z.Z.; writing—original draft preparation, Z.Z.; writing—review and editing, Z.Z.; visualization, Z.Z.; supervision, T.S.; project administration, T.S.; funding acquisition, T.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Science and Technology Program of Guangdong province under Grant No. 2019B010140002 and the Guangdong Provincial Natural Science Foundation general program, Grant No. 2021A1515011922.

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

References

1. Sunar, B.; Martin, W.J.; Stinson, D.R. A provably secure true random number generator with built-in tolerance to active attacks. *IEEE Trans. Comput.* **2007**, *56*, 109–119. [CrossRef]
2. Wold, K.; Tan, C.H. Analysis and Enhancement of Random Number Generator in FPGA Based on Oscillator Rings. *Int. J. Reconfigurable Comput.* **2009**, *2009*, 4. [CrossRef]
3. Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E.; Leigh, S.; Levenson, M.; Vangel, M.; Banks, D.; Heckert, A.; et al. *NIST Special Publication 800-22: A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications*; 2010 Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2010.
4. Markettos, A.T.; Moore, S.W. The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators. In Proceedings of the Cryptographic Hardware and Embedded Systems—Ches, Lausanne, Switzerland, 6–9 September 2009; Volume 5747, pp. 317–331.
5. Bayon, P.; Bossuet, L.; Aubert, A.; Fischer, V.; Poucheret, F.; Robisson, B.; Maurine, P. Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator. In Proceedings of the International Workshop on Constructive Side-Channel Analysis and Secure Design, Darmstadt, Germany, 3–4 May 2012; Springer: Berlin/Heidelberg, Germany, 2012.
6. Bayon, P.; Bossuet, L.; Aubert, A.; Fischer, V. Fault model of electromagnetic attacks targeting ring oscillator-based true random number generators. *J. Cryptogr. Eng.* **2016**, *6*, 61–74. [CrossRef]
7. Osuka, S.; Fujimoto, D.; Hayashi, Y.; Homma, N.; Beckers, A.; Balasch, J.; Gierlichs, B.; Verbauwhede, I. EM Information Security Threats Against RO-Based TRNGs: The Frequency Injection Attack Based on IEMI and EM Information Leakage. *IEEE Trans. Electromagn. Compat.* **2019**, *61*, 1122–1128. [CrossRef]
8. Schimmack, M.; Mercorelli, P. A structural property of the wavelet packet transform method to localise incoherency of a signal. *J. Frankl. Inst.* **2019**, *356*, 10123–10137. [CrossRef]
9. Schimmack, M.; Mercorelli, P. An on-line orthogonal wavelet denoising algorithm for high-resolution surface scans. *J. Frankl. Inst.* **2018**, *355*, 9245–9270. [CrossRef]
10. Ogasahara, Y.; Hashimoto, M.; Onoye, T. All-Digital Ring-Oscillator-Based Macro for Sensing Dynamic Supply Noise Waveform. *IEEE J. Solid State Circuits* **2009**, *44*, 1745–1755. [CrossRef]
11. An, Y.J.; Jung, D.H.; Ryu, K.; Yim, H.S.; Jung, S.O. All-Digital ON-Chip Process Sensor Using Ratioed Inverter-Based Ring Oscillator. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2016**, *24*, 3232–3242. [CrossRef]
12. Hong, B.; Hajimiri, A. A Phasor-Based Analysis of Sinusoidal Injection Locking in LC and Ring Oscillators. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2019**, *66*, 355–368. [CrossRef]
13. Liu, S.; Zheng, Y.; Lim, W.M.; Yang, W. Ring Oscillator Based Injection Locked Frequency Divider Using Dual Injection Paths. *IEEE Microw. Wirel. Compon. Lett.* **2015**, *25*, 322–324. [CrossRef]
14. Mirzaei, A.; Heidari, M.E.; Bagheri, R.; Abidi, A.A. Multi-Phase Injection Widens Lock Range of Ring-Oscillator-Based Frequency Dividers. *IEEE J. Solid State Circuits* **2008**, *43*, 656–671. [CrossRef]
15. Razavi, B. A study of injection locking and pulling in oscillators. *IEEE J. Solid State Circuits* **2004**, *39*, 1415–1424. [CrossRef]
16. Mureddu, U.; Bochard, N.; Bossuet, L.; Fischer, V. Experimental Study of Locking Phenomena on Oscillating Rings Implemented in Logic Devices. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2019**, *66*, 2560–2571. [CrossRef]
17. Su, T.; Li, F.; Lian, Z.; Feng, Z.; Li, Y.; Liu, Z. Frequency Shift of Ring Oscillators Due to Radio Frequency Interference on the Supply. *IEEE Trans. Electromagn. Compat.* **2015**, *57*, 1365–1373. [CrossRef]
18. Xiao, Z.; Chen, D.; Su, T. Locking of RO due to RF interference in supply. *Electron. Lett.* **2019**, *55*, 254–256. [CrossRef]