100 MHz Random Number Generator Design Using Interleaved Metastable NAND/NOR Latches*

Chua-Chin Wang[1]
Department of Electrical Engineering
National Sun Yat-Sen University
Kaohsiung, Taiwan 80424
Email: ccwang@ee.nsysu.edu.tw

Shao-Wei Lu
Department of Electrical Engineering
National Sun Yat-Sen University
Kaohsiung, Taiwan 80424
Email: wayne@vlsi.ee.nsysu.edu.tw

Abstract—This investigation demonstrates a wide bandwidth random number generator (RNG) based on interleaved NAND-/NOR-based SR (set-reset) latches. More specifically, the metastability of SR latches driven by the same input causing undefined output states is exploited. To achieve higher irregular sampling of the SR latches, not only NAND-based SR latches and NOR-based SR latches are interleaved integrated, their inputs are also randomly selected by another array of metastable SR latches. Namely, a 2-layer RNG architecture is realized to avoid locking phenomenon and enhance randomness. The proposed 2-layer RNG is realized using typical 40-nm CMOS process. All-PTV-corner (process, temperature, voltage) post-layout simulations validate that the proposed RNG passes long run test and mono-bit test given 100 MHz clock rate.

Index Terms—metastable, CMOS, SR latch, RNG, long run test

I. Introduction

With the booming of electronic devices, real random number generators (RNG) become very demanding ever since the secrecy of spread-spectrum communication needs to be ensured [1]. The major reason is the information the security of networks and wireless communications is definitely a priority over speed and bandwidth. In other words, to guarantee the confidentiality, the integrity and the authenticity of information, a cryptographic protocol in any communication system is required, which at least comprises two fundamental elements: 1) an encryption/decryption algorithm; 2) a random number generator (RNG). The RNG mainly is in charge of providing key values for the encryption/decryption algorithms such that information authentication can be executed. Apparently, a weak or vulnerable RNG will result in the break of any strong diphering algorithm. An RNG deployed in the cryptosystem, therefore, must at least meet the following secrecy criteria :

- Very hard to predict the output sequence
- Very hard to be repeated
- Easy to be integrated with digital communication systems

Although most of those software-based RNG algorithms are highly compatible with digital communication systems, the generation of entropy in digital domain usually require high number of replicated structures which increase hardware cost and power consumption. They are vulnerable to many crack programs. By contrast, hardware-based RNGs exploiting entropy from physical devices, e.g., thermal resistors, avalanche diodes, or LFSR (linear feedback shift register), are considered an alternative and better solution. Hardware-based RNGs are classified into two categories, namely analog type (e.g., thermal resistors, avalanche diodes, etc.), and digital type (e.g., LFSR or FPGA-based solutions). The former needs other auxiliary circuits to carry out analog to digital conversion. The latter usually is suffered from poor randomness, since this type of RNGs is pseudo-random in reality. Nevertheless, prior researchers have already reported many hardware approaches to implement RNGs, where three major trends are direct amplification, oscillator sampling, and discrete-time chaos (DTC) [2], [3], [4]. Even though the DTC method is very welcomed due to its compatibility with digital systems, it suffers from several difficulties, including large area, slow speed, large power dissipation, and sensitive to process drifting.

A commonly used entropy source using FPGAs or other digital circuits is the phase jitter in a ring oscillator (RO), e.g., [5], [6], [7], [8]. An RNG based on XORing the outputs of a number of classical ROs and regularly sampling the output of the XOR gate was proposed [5]. However, the output of this RNG requires statistical post-processing steps to satisfy tests of randomness. An improved version of this RNG by adding D flip-flops at the output of each RO before the XOR gate was reported [6], [7]. However, if this RNG was realized on FPGAs, the security of the RO-based RNG will be deteriorated by coupling an identical circuit to it on another identical FPGA. The reason is that the correlation between the outputs of a possible attacker and the target RNG significantly is increased due to coupling between adjacent structures. In other

*This investigation was partially supported by Ministry of Science and Technology, Taiwan, under grant MOST 108-2218-E-110-002 and 109-2218-E-110-007.

[1]Prof. C.-C. Wang is also with Inst. of Undersea Tech., National Sun Yat-Sen Univ, Kaohsiung, Taiwan.

978-1-7281-9396-0/20/$31.00 ©2020 IEEE

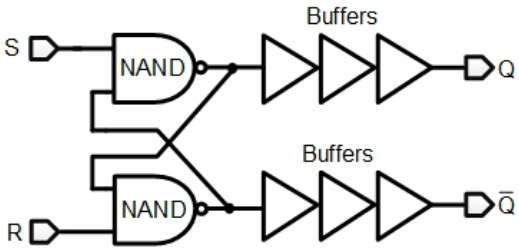

Fig. 1. NAND-based TERO

words, RO-based RNGs require each RO to be completely independent by any means. Otherwise, the ring oscillators can become dependent, i.e., locked to each other, called locking phenomenon [9]. Besides, another maor drawbacks of prior RO-based RNG on FPGAs is the low speed, which drastically hinders them to be directly applied in high-speed communication systems.

To resolve all of the mentioned problems, a high-speed wide-bandwidth random number generator (RNG) based on interleaved NAND-/NOR-based SR latches. Two arrays of interleaved NAND-/NOR-based SR latches driven by the same clock are the first layer of the proposed RNG, where their outputs are coupled to a multiplexer (MUX). Notably, the selection signals of the MUX are generated by another two arrays of interleaved NAND-/NOR-based SR latches to form the second layer of randomness generation. The proposed 2-layer RNG is realized using a typical 40-nm CMOS technology. All-PTV-corner (process, temperature, voltage) post-layout simulations demonstrate that it passes long run test and mono-bit test with 23.4 mW at 100 MHz clock rate.

II. 2-layer RNG Using SR Latches

In order to randomize the output as much as possible, not only SR latches driven by the same input are used to attain metastability, a 2-layer architecture composed of SR latches is proposed to achieve wide bandwidth and high-speed random number generation.

A. TERO circuits based on SR latches

Referring to Fig. 1, a transient effect ring oscillator (TERO) composed of a NAND-based SR latch and inverters is disclosed. As well known in any logic textbook, when the NAND-based SR latch is driven by CLK=S=R=1, the output Q is undefined, as shown in Table I. Namely, the outcomes at Q are unpredictable, called metastability. The functions of the buffers at the outputs is to extend the path and delay thereof, if necessary.

By contrast, Fig. 2 is another TERO composed of a NOR-based SR latch and inverters. Thus, if CLK=S=R=0, the outputs Q and Qbar are undefined, as shown in Table II. Certainly, buffers can be added to

TABLE I
Truth Table of NAND-based SR latch

S	R	Q
0	0	1
1	1	undefined

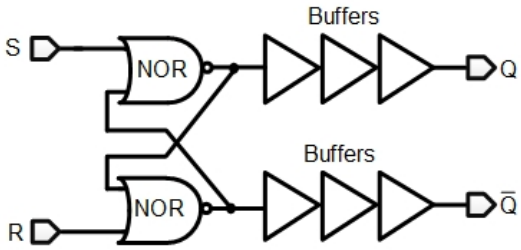

Fig. 2. NOR-based TERO

extend the oscillator path and delay just like those in the NAND-based version.

Before these TEROs are integrated to construct any RNG, thorough simulations are required to differentiate the characteristics of these two TEROs. By using Monte-Carlo simulation over 1000 times to attain enough number of meaningful statistics, Fig. 3 and Fig. 4 show the outputs of NAND-based TERO and NOR-based TERO. Apparently, NAND-based TERO generates more "1" pulses, while NOR-based TERO has more "0" ones. These features indicate the following facts.

- Neither NAND-based TERO nor NOR-based TERO alone can be used as the function units for any RNG design.
- An additional scrambling mechanism is preferred to enhance the randomness.

B. 2-layer RNG architecture

Based upon the analysis and the features of the TEROs in the previous section, a 2-layer RNG architecture is proposed as shown in Fig. 5, where I_Array_0 comprises NAND-based TERO, NOR-based TERO, …, which are n TEROs arranged interleavedly, while I_Array_1 is composed of NOR-based TERO, NAND-based TERO, …, as the counterpart. The outputs of the first array are coupled to MUX0 of which the selection signals are generated by S_Array_0, which has the same formation like I_Array_0 except the number of TEROs is $\log_2(n)$. Similarly, MUX1 is driven by the output of S_Array_1 to

TABLE II
Truth Table of NOR-based SR latch

S	R	Q
0	0	undefined
1	1	0

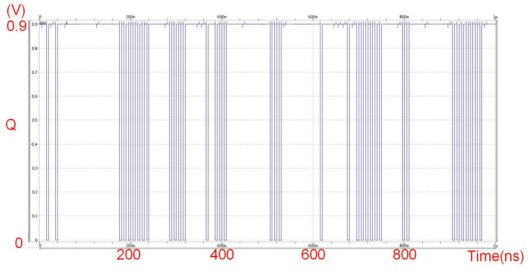

Fig. 3. Output waveform of NAND-based TERO

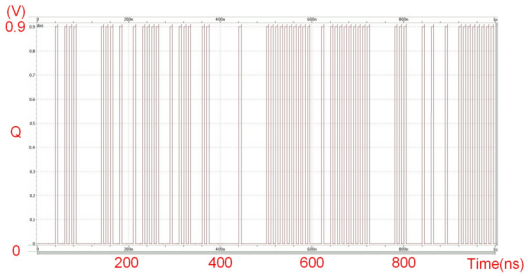

Fig. 4. Output waveform of NOR-based TERO

select one of the TEROs' outputs in I_Array_1. Finally, the selected outputs from MUX0 and MUX1 are XORed to generate the final output signal.

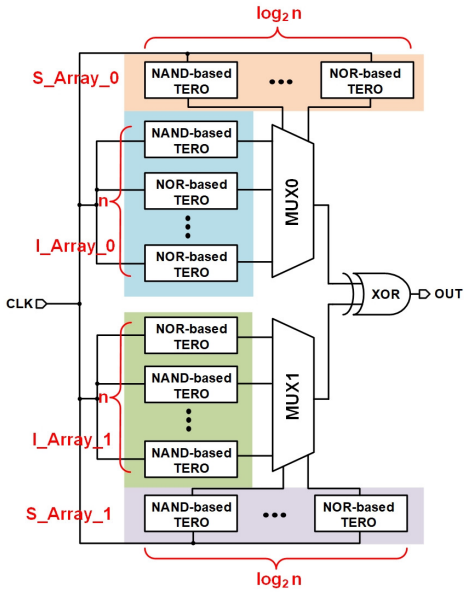

Fig. 5. Proposed 2-layer RNG design

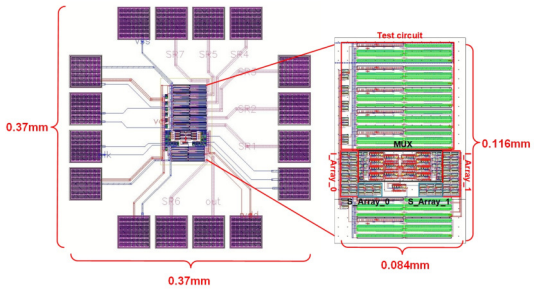

Fig. 6. Layout of the proposed 2-layer RNG design

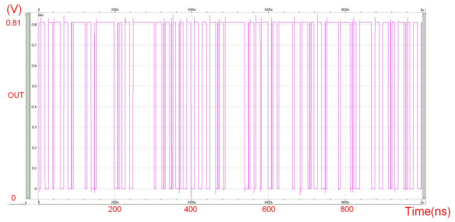

Fig. 7. Output waveform at SS corner

III. Simulation and Validation

To manifest the randomness superiority of the proposed design, an n=8 2-layer RNG is realized using typical 40-nm CMOS process. Fig. 6 is the layout, where the entire chip area is 116x84 μm^2, and the core is 37x37 μm^2. The power dissipation is 23.4 mW at maximal clock rate = 100 MHz.

A. All-PVT-corner post-layout simulations

Fig. 7, 8, and 9 are the output waveforms at 3 extreme PVT (process, voltage, temperature) corners, respectively. Apparently, there is no periodic sequence in any of these waveforms, which proves the basic randomness in time domain.

B. Validation of randomness

According to the requirement of FIPS 140-1 statistical random number generator tests [10], the following tests are fundamental.

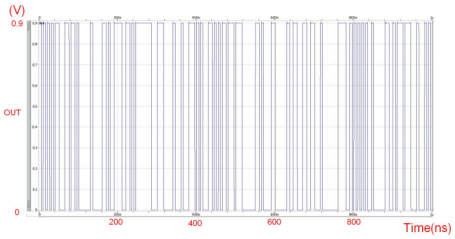

Fig. 8. Output waveform at TT corner

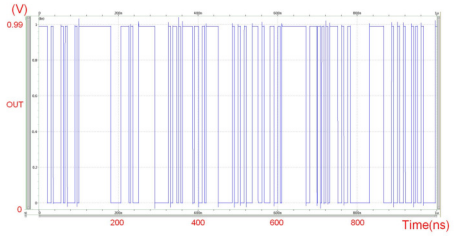

Fig. 9. Output waveform at FF corner

Continuous 0

Length of Run	Required Interval
1	2701
2	709
3	507
4	210
5	193
6	82
else	253

Continuous 1

Length of Run	Required Interval
1	2702
2	786
3	524
4	218
5	155
6	88
else	182

Fig. 10. Distribution of runs generated by the proposed RNG

• Monobit Test : Count the number of ones in the 20,000 bit stream. Denote this quantity by X. The test is passed if 9,654 < X < 10,346.
• Long Runs Test : On the sample of 20,000 bits, the test is passed if there are no long runs. A long run is defined to be a run of length 34 or more (of either zeros or ones).

By the 20,000 bits generated by the post-layout simulation of the proposed 2-layer RNG design given n=8, both of the above tests are passed. Fig. 10 is the distribution of the runs in several top bins. The comparison of several prior RNG designs is tabulated in Table III. Not only the proposed design attains the least normalized area, it also the only solution to achieve 100 MHz to provide wide bandwidth and high speed

TABLE III
Performance comparison with prior RNGs

	INDICON [11]	EDSSC [12]	ICSIT [13]	EDL [14]	this work
Year	2019	2017	2017	2012	2020
process (nm)	N/A	130	N/A	65	40
verification	FPGA	FPGA	FPGA	simu.	simu.
clock (MHz)	33	1	0.5	0.001	100
area (mm^2)	N/A	N/A	N/A	0.0045	0.0016
norm. area	N/A	N/A	N/A	1.06	1.00

IV. Conclusion

By taking advantage of the metastability of NAND and NOR, two types of TEROs are disclosed in this work. Both NAND-based TERO and NOR-based TERO are assembled interleavedly to maximize the randomness in the proposed RNG. Furthermore, the 2nd layer of randomization is carried out by other arrays consisting of NAND-based TERO and NOR-based TERO similar to the 1st layer. Post-layout simulation results validate that the proposed RNG attains the highest speed by far to become a solution with very wide bandwidth.

Acknowledgment

The authors would like to express our deepest appreciation to TSRI (Taiwan Semiconductor Research Institute) in NARL (Nation Applied Research Laboratories), Taiwan, for the assistance of EDA tool support.

References

[1] C. Chien, "Digital radio systems on a chip," Reading: Kluwer Academic Publishers, 2001.
[2] C.-C. Wang, J.-M. Huang, H.-C. Cheng, and R. Hu, "Switched-current 3-bit CMOS 4.0 MHz wideband random signal generator," IEEE J. of Solid-State Circuits, vol. 40, no. 6, pp. 1360-1365, June 2005.
[3] A. Rodriguez-Vazquez, M. Delgado, S. Espejo, and J. L. Huertas, "Switched-capacitor broadband noise generator for CMOS VLSI," Electronics Letters, vol. 27, no. 21, pp. 1913-1914, Oct. 1991.
[4] M. Degaldo-Restituto, and A. Rodriguez-Vazquez,, "Integrated chaos generators," Proc. of the IEEE, vol. 90, no. 5, pp. 747-767, May 2002.
[5] B. Sunar, W. J. Martin, and D. R. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," IEEE Transactions on Computers, vol. 56, no. 1, pp. 109–119, 2006.
[6] K. Wold and C. H. Tan, "Analysis and enhancement of random number generator in FPGA based on oscillator rings," International Journal of Reconfigurable Computing, vol. 2009, pp. 1-8, Sep. 2009. (DOI: 10.1155/2009/501672)
[7] B. Acar and S. Ergun, "Correlation-based cryptanalysis of a ring oscillator based random number generator," in Proc. 2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 1050–1053, Aug. 2018.
[8] K. Demir and S. Ergun, "Random number generators based on irregular sampling and fibonacci–galois ring oscillators," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 66, no. 10, pp. 1718–1722, Oct. 2019.
[9] M. Varchola and M. Drutarovsky, "New high entropy element for fpga based true random number generators," in Proc. International Workshop on Cryptographic Hardware and Embedded Systems, Springer, pp. 351–365, 2010.
[10] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography," ISBN: 0-8493-8523-7, CRC Press, 1996.
[11] P. Zode, P. Zode and R. Deshmukh, "FPGA based novel true random number generator using LFSR with dynamic seed," in Proc. 2019 IEEE 16th India Council International Conference (INDICON), pp. 1-3 , 2019.
[12] T. Li, L. Wu, X. Zhang, X. Wu, J. Zhou, and X. Wang, "A novel transition effect ring oscillator based true random number generator for a security SoC," in Proc. IEEE 2017 International Conference on Electron Devices and Solid-State Circuits (EDSSC), pp. 1–2, Oct. 2017.
[13] M. Siswanto, and B. Rudiyanto, "Designing of quantum random number generator (QRNG) for security application," in Proc. 2017 3rd International Conference on Science in Information Technology (ICSITech), pp. 273-277, 2017.
[14] C. Huang, W. C. Shen, Y. Tseng, Y. King and C. Lin, "A contact-resistive random-access-memory-based true random number generator," IEEE Electron Device Letters, vol. 33, no. 8, pp. 1108-1110, June 2012.