Analysis of Ring-Oscillator-based True Random Number Generator on FPGAs

Soyeon Choi
Dept. of Electronics Engineering
Chungnam National University
Daejeon, Korea
sychoi.cas@gmail.com

Yerin Shin
Dept. of Electronics Engineering
Chungnam National University
Daejeon, Korea
yrshin.cas@gmail.com

Hoyoung Yoo
Dept. of Electronics Engineering
Chungnam National University
Daejeon, Korea
hyyoo@cnu.ac.kr

***Abstract*— In this paper, randomness of ring-oscillator-based True Random Number Generators (TRNGs) on Field Programmable Gate Arrays (FPGAs) are analyzed according to the number of constituent inverters and the number of ring oscillators. A typical ring oscillator is composed of an odd number of inverter chain, in which the output of the last inverter is fed back to the input of the first inverter. TRNG utilizes a different jitter caused by PVT variations as an entropy source. To evaluate ring-oscillator-based TRNG on FPGAs, we implement various TRNGs with different numbers of constituent inverters and ring oscillators on Xilinx Spartan-3 FPGA, and the randomness is evaluated by the NIST SP 800-22 test. According to experimental results, it shows that TRNG with the smaller number of constituent inverters and the larger number of ring oscillators provides the stronger randomness.**

Keywords—True random number generator(TRNG); ring oscillator; FPGA; Look-Up Table(LUT); jitter

I. INTRODUCTION

True random number generators (TRNGs) are widely used in various areas including cryptographic systems, computer games, and probabilistic algorithms. In particular, TRNGs are mainly used in cryptographic algorithms for key generation [1]. Recently, the use of Field Programmable Gate Arrays (FPGAs) have increased to implement cryptographic systems due to low development cost, resource efficiency, and encryption speed close to Application-Specific Integrated Circuits (ASICs) [2]. Accordingly, various techniques to implement the TRNG on FPGA have been studied [1-3].

When implementing TRNGs on FPGAs, simple and effective method is to use a ring oscillator as entropy source that is configured with an inverter chain using an odd number of inverters as shown in Fig. 1 [3]. The delay of ring oscillator T_{osc} is calculated by (1), where T_d is the delay of an inverter and L is the number constituent inverters.

$$T_{osc} = 2 \times L \times T_d \,. \tag{1}$$

When the output of the last inverter is fed back to the first inverter, the period T_{osc} of the output of the ring oscillator vibrates in a random manner. As a result, the practical T_{osc} can be expressed as

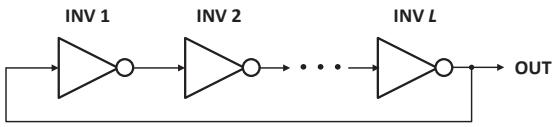


Fig. 1. Structure of a typical ring oscillator.

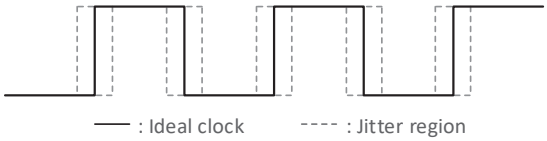


Fig. 2. Periodic jitter region of output from a ring oscillator.

$$T_{osc} = T_{osc} + \hat{T} \,, \tag{2}$$

where $\hat{T}$ is extremely small time compared to the original period T_{osc}. The very small period $\hat{T}$ is called jitter, and the jitter occurred from a ring oscillator is used as entropy source of TRNG [4].

In this paper, we analyze the performance of random bit generated by ring-oscillator-based TRNGs on Xilinx Spartan-3 FPGAs with NIST SP 800-22 test suite [5], and effective structure of the ring-oscillator-based TRNGs are presented consequently.

II. RING OSCILLATOR BASED TRNG ON FPGAS

In this paper, the ring-oscillator-based TRNG as shown in Fig. 3 presented in [1] is adopted as the base structure. In Fig. 3, a ring oscillator is composed of 1 AND gate and L inverters, which the AND gate applies the enable signal to the ring oscillator with the feedback signal of the last inverter. Note that the delay of the ring oscillator increases as much as the delay of the additional AND gate compared to Fig. 1. To improve the randomness of TRNG further, [6] presented multiple ring-oscillator structures whose outputs resulting from D Flip-Flops are combined with XORs. As a result, the base structure to be used for randomness evaluation consists of N ring oscillator with 1 AND gate and L constituent inverters, N+1 D Flip-Flops and N-1 2-input XORs as shown in Fig. 3.

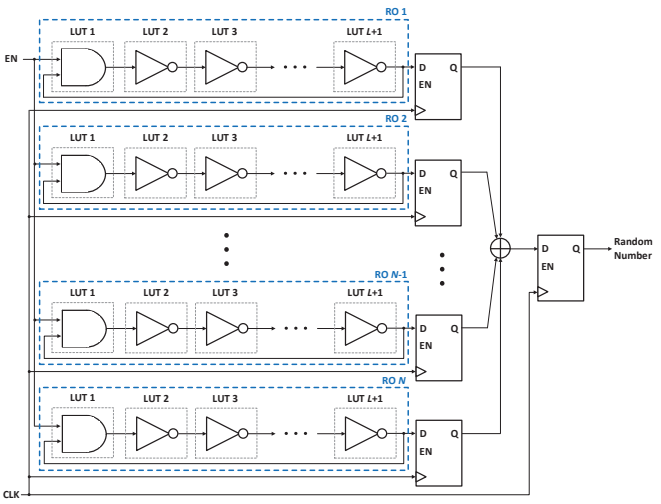


Fig. 3. Base structure of ring-oscillator-based TRNG [1].

```
// LUT4: 4-input Look-Up Table with general output
// Spartan-3
// Xilinx HDL Libraries Guide, version 14.7
LUT4 #(
.INIT(16'h5555) // Specify LUT Contents
) LUT4_inst (
.O(O), // LUT general output
.I0(I0), // LUT input
.I1(I1), // LUT input
.I2(I2), // LUT input
.I3(I3) // LUT input
);
// End of LUT4_inst instantiation
```

Xilinx primitive of 4-input LUT

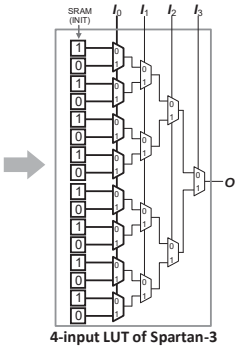
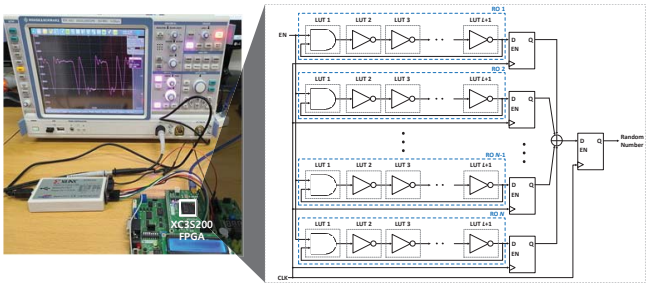


Fig. 4. Xilinx primitive and internal structure of 4-input LUT for Xilinx Spartan-3.

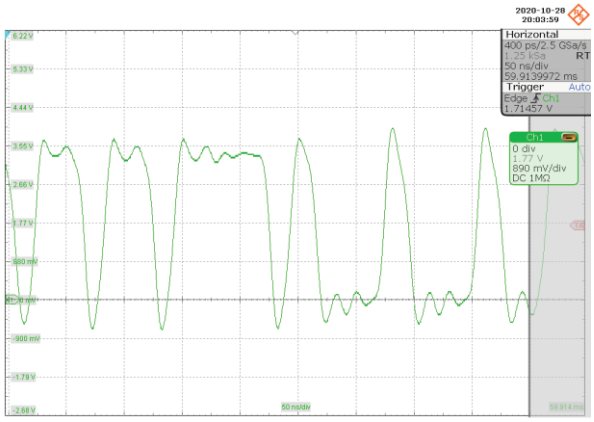
The tiles of Look-Up Tables (LUTs) and registers are placed on FPGAs leading to programmability. Especially, LUT is used to configure various types of combinational logics such as multiplexers, adders, etc. For example, Xilinx Spartan-3 utilizes 4-input LUTs to represents the combinational logics as shown in Fig. 4. In order to design only one gate in one LUT as the architecture proposed in [1], the LUT primitive provided by Xilinx in Fig. 4 is used, and the value stored in the SRAM constituting the LUT is represented with INIT that means initial value of LUT as shown in Fig. 4. For instance, assuming that I_0 among the four inputs of LUT is used as the input of the inverter, one LUT can be declared to represent only one inverter by setting the initial value INIT to 16'h5555. Thus, a total of L+1 4-input LUTs are required to implement one ring oscillator in Fig. 3 because 1 AND gate and L inverters are needed.

III. Exprimental Results

To analyze the randomness of ring-oscillator-based TRNGs, we implement various structures with different number of inverters L and the number of ring oscillators N. Xilinx Spartan-3 XC3S200 Chip is used to implement TRNGs, and the operating frequency is set to 50MHz. In addition, the



(a)



(b)

Fig. 5 (a) Experimental environments and (b) waveform measured with oscilloscope.

random bit sequences generated from TRNG on FPGA is extracted by measuring the waveform with an oscilloscope. The measurement environments are configured as represented in Fig. 5(a), and the waveform of oscilloscope is shown in Fig. 5 (b). For fair comparison, we tested 100 bit sequences with a length of 10,000-bit for each ring-oscillator-based TRNG.

Among several test suites to evaluate the randomness of TRNG, NIST SP 800-22 test suite [5] is the most widely used due to its statistical property. NIST SP 800-22 test evaluates randomness of bit sequences and provides the proportion of bit sequences that pass the test [5] as output. According to [5], the range of proportion to determine the sequence as random is computed as

$$\hat{p} - 3\sqrt{\frac{\hat{p}(1-\hat{p})}{b}} \le p \le \hat{p} + 3\sqrt{\frac{\hat{p}(1-\hat{p})}{b}}, \qquad (3)$$

where $\hat{p} = 1-\alpha$ and α sets to 0.01 by [5], and b is the number of bit sequences. Note that, if the number of bit sequences is 100, the range of success proportion p to determine the bit sequence as random is $0.9602 \le p \le 1$.

Fig. 6 shows the test results of TRNG implemented with the number of inverters L is changed to 3, 9, 15, and 21, when the number of ring oscillators N is fixed to 8. As the number of inverters of a ring oscillator increase, the number of bit sequences that pass the test tends to decease. Especially, the number of inverters L is 9 or larger, the success proportion of the bit sequences is lower than the criterion of 0.9602 that

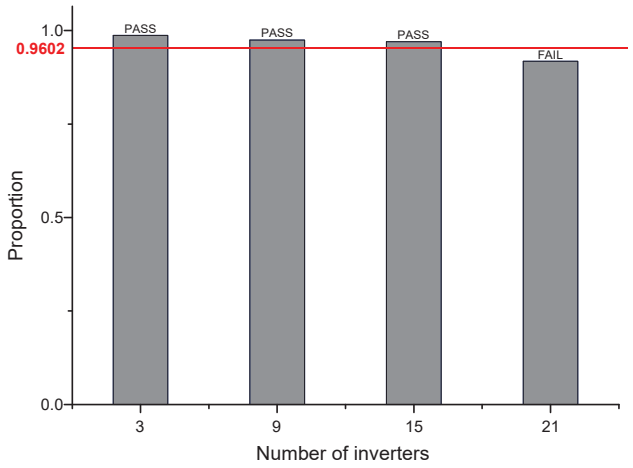


Fig. 6. Proportion of the bit sequences passing the test according to the number of inverters *L*.

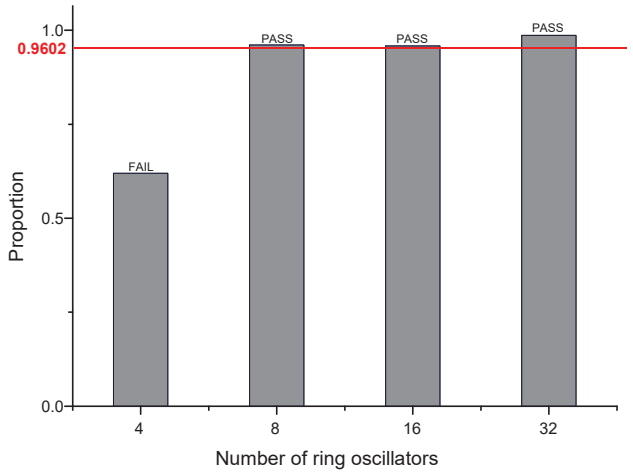


Fig. 7. Proportion of the bit sequences passing the test according to the number of ring oscillators *N*.

means the ring-oscillator-based TRNG is no longer random. When the delay T_{osc} of ring oscillators in (1) increases, the randomness leading from the effect of jitters become smaller since the jitter are also accumulated as the delay increases. As a result, the number of bit sequences passing the test decreases as the number of inverters *L* increases.

Fig. 7 shows the test results of random numbers that TRNG is implemented with the number of ring oscillators *N* is changed 4, 8, 16, and 32, when the number of inverters *L* is fixed at 3. According to Fig. 7, when the number of ring oscillators *N* is 4, the proportion of bit sequence the passes the test does not meet the criterion value of 0.9602, and the test pass ratio tends to increase as the number of ring oscillators increases. Since the TRNG is composed of multiple ring oscillators to reduce the correlation between ring oscillators, the proportion of the bit sequence passing the test increases as the number of ring oscillators increases.

IV. Conclusions

In this paper, the randomness of the TRNG according to the number of inverters and the number of ring oscillators is compared when the ring oscillator based TRNG is implemented on FPGA. It is verified that the success ratio of the bit sequence for random test NIST SP 800-22 test suite [5] increases as the number of inverters decreases and the number of ring oscillators increases. Our next research aim is to analyze the randomness for various bit stream obtained from different post processing as studied in [1-3] and to propose the most efficient structure to generate true random numbers on FPGAs.

References

[1] N. Nalla Anandakumar, S. K. Sanadhya and M. S. Hashmi, “FPGA-Based True Random Number Generation Using Programmable Delays in Oscillator-Rings,” in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 67, no. 3, pp. 570-574, March 2020.

[2] P. Kohlbrenner and K. Gaj, “An embedded true random number generator for FPGAs,” FPGA 2004, pp.71-78, ACM, 2004.

[3] 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, Jan. 2007.

[4] A. Hajimiri, S. Limotyrakis and T. H. Lee, “Jitter and phase noise in ring oscillators,” in IEEE Journal of Solid-State Circuits, vol. 34, no. 6, pp. 790-804, June 1999.

[5] L. E. Bassham, III et al., “A statistical test suite for random and pseudorandom number generators for cryptographic applications, Rev. 1a,” U.S. Dept. Commerce, Nat. Inst. Stand. Technol., Rep. SP 800–22, 2010.

[6] K. Wold and C. H. Tan, "Analysis and Enhancement of Random Number Generator in FPGA Based on Oscillator Rings," in proceedings 2008 International Conference on Reconfigurable Computing and FPGAs, Cancun, 2008, pp. 385-390.

[7] K. Wold and S. Petrovivc, “Security properties of oscillator rings in true random number generators,” in Proc. IEEE 15th Int. Symp. Design Diagn. Electron. Circuits Syst. (DDECS), Apr. 2012, pp. 145–150.