Ring Oscillator Based TRNG with Bit Swapping LFSR

[1]Amalu Sunil P, [2]Bency Varghese A
[1]M.Tech student in VLSI Design, [2]Assistant Professor ECE Department
[1,2]IES College of Engineering, Thrissur, India
[1]amalusunil@gmail.com, [2]bencyvarghesea@gmail.com

Abstract

The design of ring oscillator-based truly random number generator (TRNG) with bit swapping linear feedback shift register (BS-LFSR) is presented. The oscillator sampling technique is exploited and a tetrahedral oscillator with large jitter has been employed to realize the TRNG. Post digital processor is added to further enhance the randomness of the output bits. The proposed post digital processor is realized by 64bits Linear Feedback Shift Register (LFSR) and 4 non-linear combined functions, which can improve the unpredictability and de-correlation of output random sequence. The proposed design, called bit-swapping LFSR (BS-LFSR), is composed of an LFSR and a 2 × 1 multiplexer, it reduces the number of transitions when compared to a conventional LFSR. Hence, it reduces the overall switching activity in the circuit. The proposed TRNG has a power consumption of 187mW. An important objective of post digital processor is to provide robustness of the statistical properties of the TRNG output sequence

Keywords: **TRNG; LFSR; Bit-swapping LFSR; Tetrahedral oscillator**

1. INTRODUCTION

True random numbers and physical nondeterministic random number generators (RNGs) seem to be of an ever increasing importance. Random numbers are essential in cryptography (mathematical, stochastic and quantum), Monte Carlo calculations, numerical simulations, statistical research, randomized algorithms, lottery etc.

Today, true random numbers are most critically required in cryptography and its numerous applications to our everyday life: mobile communications e-mail access, online payments, cashless payments, ATMs, e-banking etc. High quality random number generation is essentially demanded for security. True random numbers are produced from physical random sources. Each bit of the bit streams is independent from the other bits and the probabilities of 1/0 occurrences are identical. Because true random numbers cannot be predicted by computational methods, they are highly desirable for security purposes [1]-[2]. The security of the smart cards relies on the generation of unpredictable and irreproducible digital key streams using a nondeterministic random number generator. In [3] a fully digital, high speed ASIC random number generator based on ring oscillators presented.

Thermal noises and shot noises of devices are random sources used to generate truly random numbers. Therefore, TRNGs which use internal random noises are popular and widely studied [4]. Oscillator-based TRNG [5]-[9], which utilizes random period jitter of oscillators as random source, is one of the popular circuits for generating truly random numbers. In this paper [6], a high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC is presented. [6] RNG is based on the oscillator sampling technique and a jittered oscillator with an explicit thermal noise

source has been designed in order to improve output rate and statistical quality of the generated bit sequence.

An ultra-low power TRNG for anti-collision purpose in passive ultra-high frequency RFID tags is proposed in [10]. The TRNG generates random number by sampling the 900 MHz input signal with a local 320 KHz jittery clock. The power consumption is as low as 0.55 μW due to the reuse of the 900 MHz input signal. However, statistical performance of the TRNG's output bits is sensitive to the latch's input offset voltage caused by process variation. Besides, the TRNG generates only 3-bit random number, limiting the randomness of the output bits.Besides, the TRNG generates only 3-bit random number, limiting the randomness of the output bits. A low voltage low-power TRNG for Gen2 RFID tag is presented in [11]. Minimum supply voltage of the TRNG is 0.8 V and the power consumption is 1.04 μW.

Power and area are limited resources in most smart cards. Most TRNGs mentioned above have either high power consumption or low statistical property. A low-power ring oscillator-based TRNG with high randomicity and less delay for encryption is presented in this paper.

2. RING OSCILLATOR-BASED TRNG

Though the oscillator-based TRNG can be easily implemented with CMOS gates or FPGA the amount of the internal noises, that is, the jitter of the oscillators is so small that highly random bitstreams cannot be generated. A long inverter chain or a frequency divider provides the sufficient jitter at the enormous sacrifice of area or throughput.

A low frequency oscillator samples the output of a high frequency oscillator using a D flip-flop. Thermal noise of the devices is converted to jitter by oscillator and the jitter is used as random source. When the frequency of each oscillator randomly drifts with each cycle, the output bit streams will be random. The level of randomness heavily depends on the mean frequency separation of the oscillators and the amount of achievable jitter.

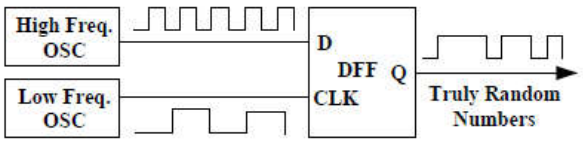

Figure 1. Ring oscillator based TRNG

Larger frequency separation and jitter result in better randomness. The ring oscillator-based TRNG is more robust to deterministic noise and 1/f noise. In addition, ring oscillator-based TRNGs are easy to be implemented and occupy small area, suitable to be integrated in low-cost low-power systems such as smart cards and RFID tags**.**

3. ARCHITECTURE OF THE PROPOSED TRNG

The architecture of the proposed TRNG, which consists of two oscillators named as OSC1 and OSC2, a low-power XNOR gate and a D flip-flop. The outputs of OSC1 and OSC2 are

combined by the XNOR operation to yield Seed, a random sequence of higher statistical quality.

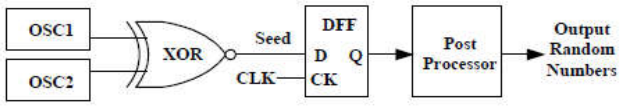

Figure 2. Architecture of the proposed system

The XOR operation is preferred owning to the even probability of 0s and 1s for Seed. Then Seed is sampled by using the D flip-flop. Post digital processor is added to further improve the randomness of the output random numbers.

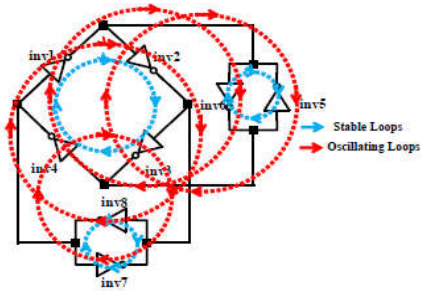

Figure 3 .Topology of the tetrahedral oscillator

Figure 3 illustrates the topology of the tetrahedral oscillator exploited to implement OSC1 and OSC2. There are three stable loops and four oscillating loops in the circuit. The three stable loops are: 1) the loop composed of inv1, inv2, inv3 and inv4, 2) the loop composed of inv5 and inv6, 3) the loop composed of inv7 and inv8. The four oscillating loops are: 1) the loop composed of inv1, inv2 and inv8, 2) the loop composed of inv2, inv3 and inv5, 3) the loop composed of inv3, inv4 and inv7, 4) the loop composed of inv4, inv1 and inv6. In comparison with the traditional ring oscillator consisted of directly cascaded inverter, the tetrahedral oscillator has the following merits. Firstly, the ring loop contains several fast and slow loops and they nest with each other, which makes the circuit full of wire-or logic and signal competitions, resulting in logic mess and bringing about metastability. Secondly, the perturbation of noise makes the oscillation to be aroused easier. Furthermore, due to the conflicts among diverse loops, large jitter can be achieved to enhance the randomness of output bits.

3.2 POST PROCESSOR

Typically, a TRNG consists of random seed generator and a post digital processor, which produces the final output. An important objective of post digital processor is to provide robustness of the statistical properties of the TRNG output sequence. The scheme of post digital processor is shown in Fig. 3.3. The proposed post digital processor is realized by 64bits Linear Feedback Shift Register (LFSR) and 4 non-linear combined functions, which can improve the unpredictability and de-correlation of output random sequence. A linear-feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state. The most commonly used linear function of single bits is exclusive or (XOR). Thus, an LFSR is most often a shift register whose input bit is drive driven by the XOR of some bits of the overall shift register value.

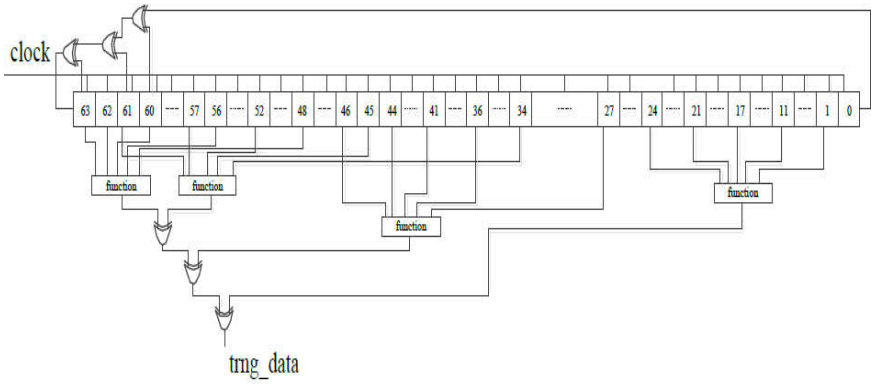

Figure 4. Post Processor

3.3 FUCTIONAL BLOCK

The post digital processor in the proposed system contain 4 nonlinear combined fuction.Each function block is combination of XOR and AND gates. The function block has 5 inputs that are taken from the LFSR .That is first function block takes input from the 1,11,17,21,24 bit positions of 64 bit LFSR.Similarly, Second function block takes input from 27,36,41,44 and 46. Third function takes input from 34,45,52,57,61.Fourth function block takes input from 48,56,60,62,63 bit positions

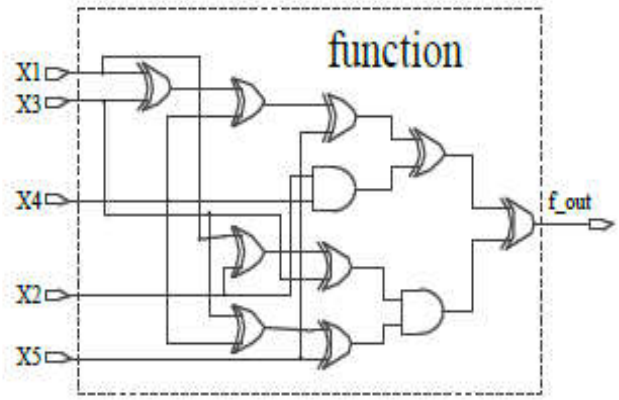

Figure 5. Nonlinear combined function block

3.4 BIT SWAPPING POST PROCESSOR

The proposed design, called bit-swapping LFSR (BS-LFSR), is composed of an LFSR and a 2 × 1 multiplexer, it reduces the number of transitions when compared to a conventional LFSR. Hence, it reduces the overall switching activity in the circuit.

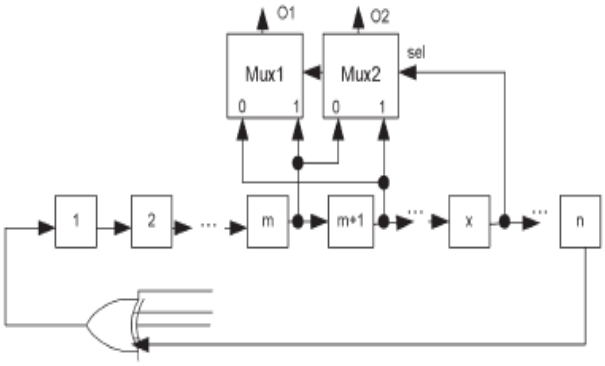

Figure 6. Swapping arrangement for an LFSR.

Bit swapping LFSR (BS LFSR) is a modified version of conventional LFSR which generate pseudo random pattern at output of LFSR with less transition between 0 and 1, which occur in the LFSR output stream. It reduces the average power dissipated by reduction in internal switching activity.

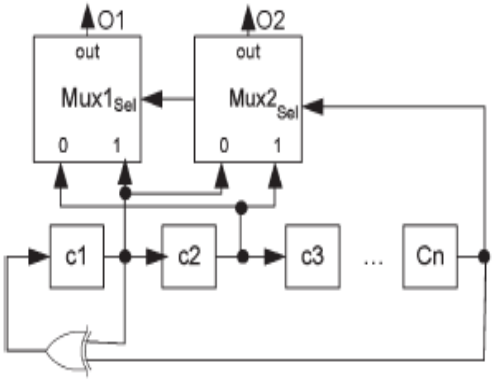

Figure 7. Proposed swapping arrangement

4. SOFTWARE IMPLEMENTTION RESULTS

The proposed system can be divided into 2 sections. The first section consists of the seed generator and a post processor. In second section post processor is replaced by a bit swapping linear feedback shift register.

4.1 PROPOSED TRNG

TRNG consists of a random seed generator and a post digital processor, which produces the final output. Seed generator section includes 2 oscillators connected to a XNOR gate and D flip flop. Oscillator frequency is divided using a toggle flip flop to produce a random sequence. These random bits are feed to the D flip flop. The output of the D flip flop is known as seed value. The seed sequence is given to the post processor.

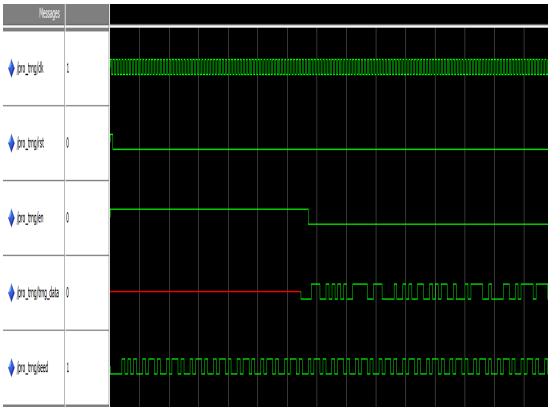

Figure 8. Output waveform of proposed TRNG

4.2 BIT SWAPPED POST PROCESSOR

The second section is the modification of proposed TRNG.In bit swapping arrangement two 2:1 multiplexer is connected to the post digital processor. First 2:1 multiplexer connected to the 60, 61 bit positions of LFSR and second multiplexer connected to the 62, 63 bit positions of LFSR in post digital processor. This section reduces the number of transitions of bits and also produces more random number sequence. Since the number of transitions reduced power also reduced. The output waveform of bit swapped post processor shown in figure.

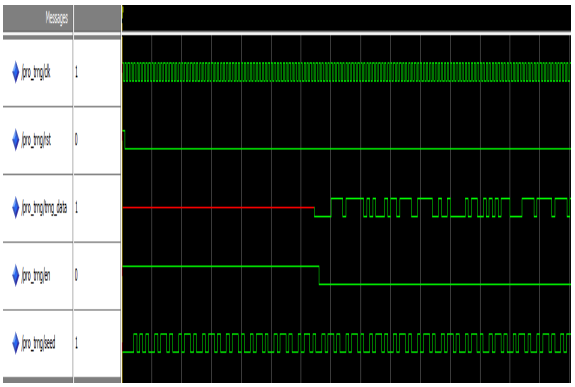

Figure 9. Output waveform of bit swapped post processor

Table 1: Performance Analysis

	Proposed System	Modified System
Power	275mW	187mW
Delay	3.815ns	3.5ns

5. CONCLUSION

Ring oscillator-based truly random number generator (TRNG) with bit swapping linear feedback shift register (BS-LFSR), designed. This system produced more unpredictable and decorrelated output random sequence. Modified system has less power consumption than conventional system. Also the critical path delay is decreased. Verified the results using simulation softwares like Xilinx and Modelsim and compared with the performance of conventional systems.
The system is used for security purposes. High-quality random number generation is essentially demanded for security and cryptography applications. The security of the smart cards relies on the generation of unpredictable and irreproducible digital key streams using a nondeterministic random number generator. In this produces unpredictable random numbers and it suitable for smart card.

ACKNOWLEDGMENTS

I express my sincere thanks to my guide Ms. Bency Varghese A for her valuable guidance and useful suggestions, which helped me throughout this work.

REFERENCES

[1] Vassilev and T. A. Hall (2014), "The importance of entropy to information security," *IEEE Trans.Comput*., vol.47, no.2, pp. 78-81.

[2] B.S. Vikram and P.B. Wayne D. Golic, (2015) "Entropy and Energy Bounds for Metastability Based TRNG with Lightweight Post-Processing," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 7, pp. 1785-1793.

[3] Ü.Güler and E.Salih, (2012) "A high speed, fully digital IC random number generator," *Int. J. Electron. Commun(AEÜ*), vol.66, no.2, pp.143-149.

[4] Takehiko Amaki, Masanori Hashimoto and Takao Onoye, (2011) "An Oscillator-Based True Random Number Generator with Jitter Amplifier," *IEEE Trans.Circuits.pp.* 725-728.

[5] K.Yang, D.Fick,M.B.Henry, Y.Lee,D.Blaauw and D.Sylvester, (2014)"A 23 Mb/s 23 pJ/b fully synthesized true-random-number generator in 28 nm and 65 nm CMOS," in Proc. *IEEE Int. Solid-State Circuits Conf*., vol. 16, pp. 280-283.

[6] M. Bucci, L. Germani, R. Luzzi, A.Trifiletti, and M. Varanonuovo, (2003) "A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC," *IEEE Trans. Comput*., vol.52, no.4, pp. 403-409.

[7] R. Stewart, B. Leung and G. Gong, (2014) "Truly Random Number Generator Based on Ring oscillator Utilizing Last Passage Time*," IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 61, no. 12, pp. 937-941.

[8] D. Lubicz and N. Bochard, (2015) "Towards an Oscillator Based TRNG with a Certified Entropy Rate," *IEEE Trans. Comput*., vol.64, no.4, pp. 1191-1200.

[9] C.S. Petrie and J.A. Connelly, (1996) "Modeling and Simulation of Oscillator-Based Random Number Generators," Proc. *IEEE Int'l Symp. Circuits and Systems* (ISCAS '96), vol. 4, pp. 324-327