A Ring Oscillator Based Random Generator for Cryptography Applications

R.Dinesh, Ramalatha Marimuthu

Abstract: ***A ring oscillator based Random number generator (RNG) for Cryptography applications is presented. The paper explains about the requirements and generation of high randomness based codes, used to improve the security in data communication. The methodology used is sampling technique, adopted in the oscillator for the random number generation. To get better randomness in the output bits of RNG, a processor module based on Linear feedback shift register is used. The proposed RNG is designed with bit rate is 100kb/s, with a power consumption of 37µw. After implementation in hardware, this can be used for cryptography encryption applications to enhance the security. The system is simulated and synthesized with Xilinx ISE and the results are compared with the existing system based on randomness, power consumption, etc.***

Keywords: Random Number Generator (RNG), Ring Oscillator (RO), Linear Feedback Shift Register (LFSR).

I. INTRODUCTION

Due to the development of Cryptography, Secured data transfer is used in all wired and wireless communications. Unpredictability of random sequence is the essential feature expected in random binary sequence generator [1]. The Unpredictable random binary sequence generated by random number generator should have a good quality for cryptography and smart card applications. Due to the low power, low cost, good feasibility, True random number generators are used with RF ID tags [2]. The smart card security depends on generation of unpredictable and irreproducible digit codes

The two types of random number generation codes are Pseudo random number generator and true random number generator. Nowadays random number generation sequence are implemented in FPGA because of its reconfigurability and fast implementation. Post processing is a method used along with random generation to eliminate the bias present in the random sequence [3].

Ring oscillators are constructed by combination of odd number of inverters in a closed circuit. The frequency of ring oscillator depends on number of inverters connected and the delay of each inverter stage. Multi loop ring oscillators will provide additional gain path [4]. Ring oscillators are utilized for random generation application because of its good stability, low power consumption compared to LC type oscillators and easy generation of random sequence. CMOS ring oscillators are the essential design for SOC design [5].

Revised Manuscript Received on September 03, 2019

R.Dinesh, Research scholar, Sathyabama Institute of Science and Technology
dinaofc@ yahoo.co.in
Dr.Ramalatha Marimuthu, Professor/ECE Kumaraguru college of technology
ramalatha.marimuthu@gmail.com

The paper is organised as follows Section II covers related works ,section III covers problem statement, section IV covers proposed methodology, section V covers results and inference and conclusion is given in section VI.

II. RELATED WORKS

Liu Dongsheng etal designed a true binary sequence generator by utilizing ring oscillators [6]. Two oscillators and sampling technique are used to realize True Random binary sequence generator. The author used digital processor to enhance the randomness of the output sequence. The system is targeted for encryption application.

P.Choi etal designed a random generator based on multiple sampling [7]. The architecture is designed by utilizing all the gates of ring oscillators. The output binary sequence is more compact and faster than the earlier random sequence.

Jovan .Dj.Golic designed a true random sequence based on asynchronous logic circuits [8]. A self clock controlled LFSR is used for pre processing of data. The generated binary sequence has a very high speed and high entropy rate. The post processing will expand the randomness of the output sequence.

Sal˙ih Ergün presented a random generator based on Cross coupled Chaotic oscillator [9].The non invertible binary sequence are generated based on chaotic signal. The system generates higher and constant throughput rates and fulfill the NIST test.

Sylvain Guilleyetal generates the random codes and undergoes various tests to check the randomness [10]. In order to check the functionality and randomness, author conducted various test such as fault intersection test, two point test etc.

Jeremy Holleman etal presented a novel hardware based random generator [11]. The first random number generator designed with DC nulling with low power utilization and the second random number generator designed to remove the unwanted components in the output sequence. A pre-processing system is used to improve the randomness. The entire system designed with low power consumption.

III. PROBLEMS STATEMENT

In cryptography, encryption algorithms required high randomness based sequence for key generation to prevent the information from the Intruders. .Random number based analog circuit's gives more power wastages. The aging and temperature drifts, fabrication limits will affects the correlation of the sequence. Earlier methods used in random number sequence such as amplification of noise with gain amplifier and discrete time based analog processing technique utilize more

power consumption and the methods requires larger gain for amplification. The sampling method based oscillator consumes less power and also gives good quality, high randomness compared to the previous methods. The pre-processor techniques enhance the randomness.

IV. PROPOSED METHOD

A. Random Number Generation Methodology

The main contributions of this paper are

(a) High randomness obtained with sampling technique and LFSR based processor.

(b)Unpredictable codes obtained with low power consumption.

The block diagram of a truly random number generator based on ring oscillator is shown in fig [1].

A ring oscillator with five stages and ring oscillator with three stages are used to generate low frequency and high frequency. A three stage oscillator output frequency is sampled by five stage oscillator output frequency by using D-flip flop.

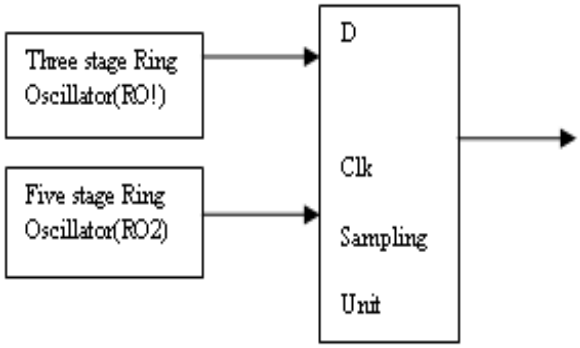

Fig. 1. TRNG based on two oscillators

A ring oscillator will have a deviation in the output signal from its ideal position is called as jitter. There is a chance of drifting in the oscillator frequencies in various cycles. The mean frequency separation and the jitter percentage is important and it is directly proportional to randomness of binary sequence.. Ring oscillator is selected compare to LC oscillators because of its small area occupancy and low power consumption.

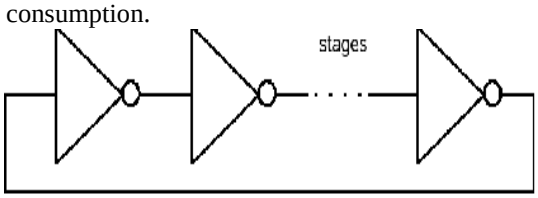

Fig. 2. Ring oscillator constructed with inverters

The below diagram shows the diagram of proposed TRNG.

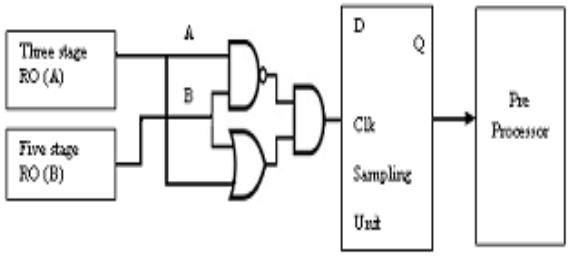

Fig. 3. Proposed TRNG with digital processor

The system consists of two ring oscillators with different stages , XOR gate and D- flip flop. The two oscillator outputs are fed back to the XOR gate to produce BISQ (Binary sequence). The two oscillators centre frequencies are 79.5 MHZ and 49 MHZ The frequencies of the output of XOR is not the integer multiple of clock frequencies.

The output of XOR operation is sampled by a 6.MHZ clock based D-flip flop. The D-flip flop output is fed as an input to digital processor. The processor will improve the percentage of randomness.

The strength of the random binary sequence depends on two things namely- Functionality, robustness of randomness

B. Digital Processor

A Linear feedback shift register is an important block used in various security applications like cryptography, spread spectrum based Code Division multiple Access (CDMA), etc. In spread spectrum based CDMA, LFSR is used to expand the code and at the same time, it will provide high security for the information

A digital processor consists of 32 bit linear feedback shift register with combined functions. The feedback shift register make the random code as an unpredictable and random sequence. Six functional blocks are used with random inputs from the bit sequence. XOR gates are used to enhance the randomness of the pre-processor block.

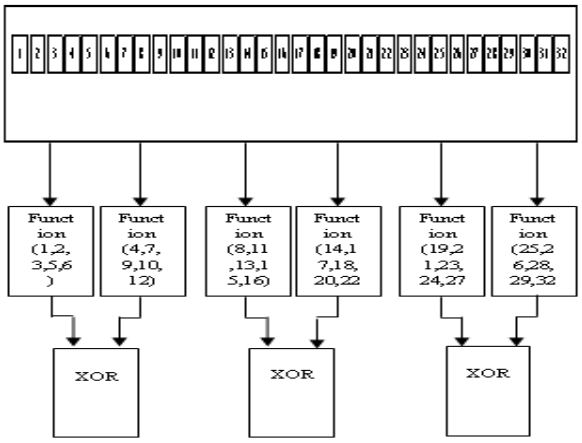

Fig. 4. LFSR based Pre processor

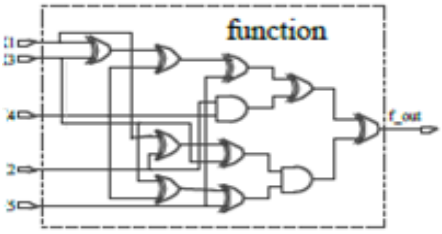

Fig. 5. Function in the Prep processor

Different types of test are used to check the randomness. The test will check two important features: functionality and validating its robustness during attack. The important test include Die hard test and NIST FPS test. Die hard is a simple test with two steps by considering randomness effect and robustness during attack, etc.

V. RESULTS AND DISCUSSIONS

The entire proposed system is coded in Verilog HDL and the functionality checking, Simulation and synthesized with Xilinx ISE tool. The power analyzer tool is used to find the power consumption.

The entire test is done in windows 7 based operating system with good RAM capacity. Fig 6 and 7 represents the inner and outer RTL schematic. The CLB's and gate count are very low compared to the existing systems. Fig 8 represents the true random number output sequence with LFSR processor, it provides high randomness.

Fig. 6. Outer representation

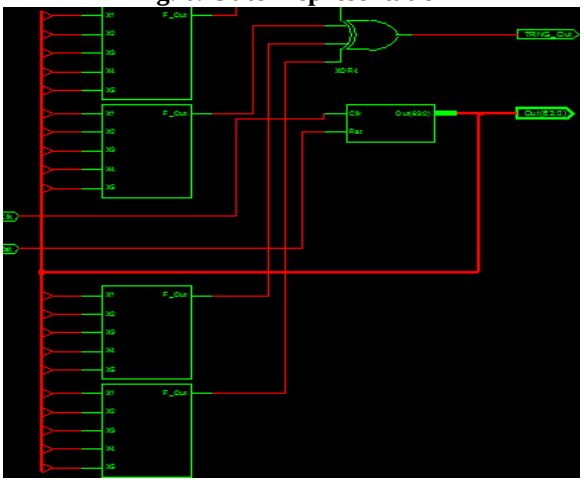

Fig. 7. Inner representation

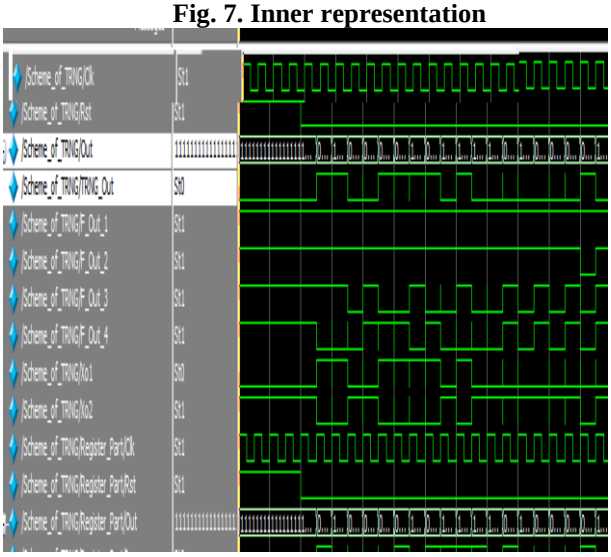

Fig. 8. TRNG output sequence

Table- I clearly indicates that flip-flops and Lookup-tables utilization are very low. So the area occupied is also low. Ring oscillators utilized low power and occupy low area. Now day's designers are giving first priority to ring oscillators compare to LC oscillators. These factors enhance the hardware utilization of FPGA.

Spartan family	Slice Flip flops	4 input LUTs	Slices	Gate count
Used	64	8	68	563
Available	3840	3840	1520	-

Table- I: Hardware Utilization

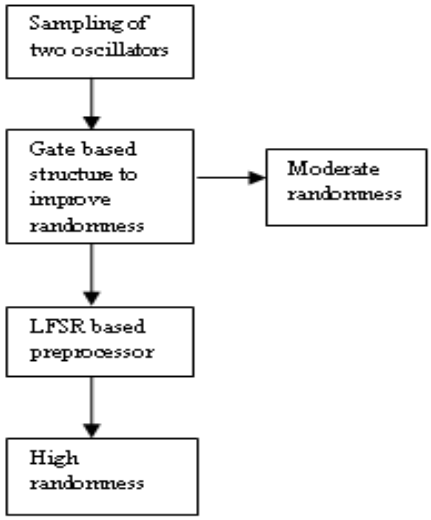

Fig. 9. Flow chart of the proposed method

Table- II: Comparison with other works

	[6]	[8]	[11]	This work
Power(µw)	0.55 µw	40 µW	180 µw	37 µW
Bit rate(Mbps)	12.5	0.1	0.050	0.1
Randomness	Medium (no preprocessing technique)	High	High	High
Application	Security based communications	Smart card	embedded	Cryptographic encryption

From the table, it is clear that power consumption is low compare to the previous works and also TRNG plus digital processor produces high randomness number. Earlier systems targeted for different applications such as general security, smart card, embedded system, cryptography, etc. This system is designed for cryptography encryption application. It can also be used for smart card and other security applications with slight modifications. The system gives high randomness with simple linear feedback shift register , few XOR gates and the pre-processor circuit , simple compared to the existing works. The bit rate is not high and can be

improved by increasing the stages in oscillator.

VI. CONCLUSIONS

The paper surveyed about earlier methods followed to generate random codes and also discussed about their drawbacks. The earlier method like direct amplification based random number generation requires larger gain and wide amplification. The paper explained the reason for selecting oscillator based random number generation. An oscillator based random number generation avoids the problems of direct amplification based random number generation and it also provides high randomness with low power consumption and can be easily integrated with signal processing circuits. This paper explained about a Random Number Generator (RNG) by utilizing two different stages ring oscillators and a sampling technique. Ring oscillator is preferred because of its low power consumption compare to the oscillators like LC oscillator. The randomness improved by combining independent random numbers into single one. The system gives high randomness and also consumes low power compare to the previous system. The important contribution of this paper is Linear Feedback Shift Register based processor produces unpredictable codes, enhances the randomness of output binary sequences and the bit rate produced in 100kb/s.

The verilog code for the full system is simulated and synthesised using Xilinx ISE. From the synthesis report, it is noted that the power consumption of the entire system is 36 µw, system utilizes less lookup-table with less gate count..The system can be applied for cryptographic encryption technique, smart card applications, security based communications,etc,

In the future, to improve the randomness, LFSR can be modified by changing the function or increase the LFSR bit sequence. The LC oscillator can also be fixed in the place of ring oscillator and comparison can be done with respect to power consumption, randomness and complexity in the circuit.

REFERENCES

1. M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, “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, Apr. 2003.
2. W. Chen et al., “A 1.04 µW truly random number generator for Gen2 RFID tags,” in Proc. IEEE A-SSCC, Nov. 2009,pp. 117–120.
3. M. Jessa and L. Matuszewski, “Enhancing the randomness of a combined true random number generator based on the ring oscillator sampling method,” in Proc. Int. Conf. ReConFig Comput. FPGAs, Cancun, Mexico, Nov. 30–Dec. 2, 2011, pp. 274–279.
4. E.J.Pankratz and E.Sánchez-Sinencio, “Multiloop high power supply rejection quadrature ring oscillator,” IEEE J. Solid-State Circuits, vol. 47, no. 9, pp. 2033–2048, Sep. 2012.
5. L. Dai and R. Harjani, “Design of low phase noise CMOS ring oscillators,” IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process., vol. 49, no. 5, pp. 328–338, May 2002.
6. Dongsheng Liu, Zilong Liu, Lun Li, and Xuecheng Zou”.A low cost low power ring oscillator based truly random number generator for encryption on smart cards”, IEEE Trans IEEE Transactions on circuits and systems vol. 63, no. 6, june 2016.
7. P. Choi, M.-K. Lee and D.K. Kim,” Fast compact true random numbergenerator based on multiple sampling”’, ELECTRONICS LETTERS 22nd June 2017 Vol. 53 No. 13 pp. 841–843.
8. Jovan D,” New Methods for Digital Generation and Postprocessing of Random Data”,IEEE Transactions on computers, vol. 55, no. 10, october 2006.
9. Sal˙ih Ergün,”A Truly random number Generator based on a pulse-excited cross-coupled chaotic oscillator”, The Computer Journal, Vol. 54 No. 10, 2011.
10. Sylvain Guilley and Youssef El Housn,” Random numbers generation: tests and attacks”, 2018 Workshop on Fault Diagnosis and Tolerance in Cryptography.
11. Jeremy Holleman ,Brian Otis, Seth Bridges, Ania Mitros, Chris Diorio,”A 2.92 µw hardware random generator”, 2006 Proceedings of the 32nd European Solid-State Circuits Conference, February 2007.

AUTHORS PROFILE

Mr.R.Dinesh has been in teaching for 14 years and currently working as Associate Professor in ECE in Marthandam College of Engineering &Technology, India. He has received the B.E degree in Electronics and communication from Bharathidasan university, India , M.E degree in Optical Communication from Anna university, India and M.B.A degree from Madurai Kamaraj University, India. Currently he is doing PhD in VLSI. He has published 15 technical papers in International conferences and journal in the areas of optical communication, VLSI and signal processing. His research are of interest include, Low power VLSI, Clock Synchronization, ADPLL etc.

Dr Ramalatha Marimuthu has been in teaching for 30 years and currently working as Professor in ECE in Kumaraguru College of Technology. She has published six technical books and over thirty research papers in international conferences and journals in the areas of Vedic Mathematics, Embedded System Design, Data Sciences and VLSI. Her interest in building assistive systems for the health care and special needs people has culminated into developing unique solutions for dyslexia, speech impaired, drop foot and autism. This earned her invitations from Google and various universities all over the world to deliver special lectures. She has won many international awards from organisations like IEEE, USA, Lions Club and Anita Borg Institute for Women and Technology, California for her work towards the community.