International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

An Efficient Approach of True Random Number Generation using Serial Input Parallel Output Register & Tree based Interleaver

Prateek Agnihotri, Preeti Agarwal Mittal
Electronics Engineering Department,
HBTU Kanpur, India

***Abstract*:- In this paper we propose a new method for generation of TRNG using tree based interleaving technique. The output of one oscillator is send to SIPO register using a XOR gate. The other input of XOR gate is kept at '1'. The property of XOR gate is that the output bit will be independent if its input bits are independent. After the SIPO register the output is connected to the XOR based postprocessor. Among Von Neuman, BCH code and XOR based preprocessor we have used XOR based preprocessor due to ease of implementation. Finally, for implementing tree based interleaving multiplexer is used with its select lines connected to binary up down counter.**

Index words: True Random Number Generators (TRNG), Pusedo Random Number Generators (PRNG), Xilinx, Random Number Generators (RNG), Xilinx, metastability, AIMSPICE.

1. INTRODUCTION

True random number generators (TRNG) have enormous applications in banking sectors, games, encoding and encryption of data. Manufacturing of TRNG is not an easy task. Since if TRNG is designed on known concepts then its randomness is lost. It will generate the codes on known methods. Some designs of TRNG is available in literature [1,2] based on randomization of delay between flip flops and generation of different source with lots of random bits. This paper presents with the concept of delay and having a preprocessor with TRNG based interleaving technique.

2. TRUE RANDOM NUMBER GENERATORS

Related Works- TRNG can be made by hardware i.e. by using non deterministic methods. It can be classified by probability rules [3,4]. Generally it has almost even probability for generation of 1 and 0 (unlike from Pusedo Random Number Generator) due to large extent of randomness. Major classification of Random Numbers which are available in literature are noise based RNG, Free running oscillator based RNG, chaos RNG and quantum RNG. TRNG can also be by implemented by digital circuits by giving the randome delay by one stage to another. Randomness can also be increased by using preprocessor [5]. In literature Von Neuman, Ex OR and BCH based decoders [6-7] are available. The implementation of ExOR based decoder is easier as compared to other preprocessors. One important property of ExOR based decoder is independency of output bits are sure if its inputs are independent.

Proposed Work- Fig. 1 shows the block diagram of block diagram of tree based interleaver consist of seed , ExOR based preprocessor and tree based interleaving technique. The output obtained after oscillator consist of large randomness which can be further controlled through preprocessor. Preprocessor which is used in this purpose is of XOR type. It is easy to implement and have compression rate which is fixed as 0.5[light weight]. Further the tree based interleaving is applied to get the controlled and maximum amount of randomness. As it is easy to understand that from seed due t jitter the randomness is high but becomes uncontrollable. By the use of Preprocessor the controllability on randomness is increased. It may have some repetitions of signal which can be controlled by the use of tree based interleaving [8] .

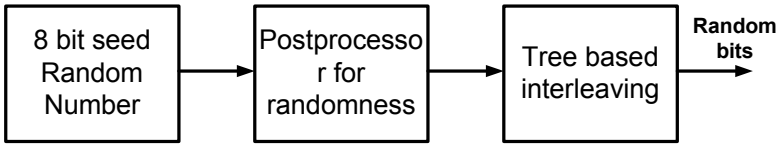

Fig.1 Block diagram of proposed methods

Tree based circuit is popular because of increase in controllability on increasing the number of bits for generation. It also assures that on increasing the number of bits there is very less chance of repletion.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

3. OVERALL PROPOSED TRNG ARCHITECTURE USING POST PROCESSOR

Metastability state is generally the cause of random bit generation. It also requires complex placement strategies because of unpredictability of metastable stage. In this paper 3 stage and 5 stage ring oscillator is used to get the oscillation. The frequency ratio of oscillation between three stage and five stage should be greater than 0.5. So that the output frequency of the system becomes ambiguous. The 3 stage ring oscillator is used as a clock to SIPO register. While 5 stage oscillator output is fed to the input of ExOR gate. The study of delay has already been discussed in [10]. Overall delay is discussed [9]. According to this the delay due to multiple stages can be given by equation (1) Where D_i is the constant delay of the ith gate and (i+1)th gate. $\Delta d_{Li,j}$ it is time delay caused by individual local delay. . $\Delta d_{Gi,j}$ it is time delay caused by global delay.

$$d_{i,j} = D_i + \Delta d_{Li,j} + \Delta d_{Gi,j} \qquad (1)$$

Now, the frequency of 5 stage oscillator is less 3 stage oscillator is more. Due to ambiguous nature of metastability stage it becomes difficult to be rely on frequency of the system. For that in last stage two bit binary up down counter is used to provide the constant frequency to the system. Now it becomes

clear for knowledge of proper operating frequency of the system probability of metastability should be defined. The probability of metastability at the i^{th} flip flop can be expressed as [15]

$$P_m(i) = 2\varepsilon f \qquad (2)$$

Where ε is the skewness of the clock and f is the frequency of input applied to SIPO register. For creating randomness sensing clock of SIPO should be at metastability stage. Since Each phase of the inverter has different delay so it can be seen that the jitter obeys the normal distribution. [15 highly flexible]. When sampling of Flip Flop array on the ith trigger getting a binary data '1' is P_{oi1}. So the probability that the sampling gets According to the definition of entropy information probability of sampling '1' is given by equation (3). The probability of occurring $P_{oi0}=1-P_{oi}$ in equation (4). While equation (5) and (6) shows its elaborated form.

$$P_{i1} = P_{i(1\to 0)} - P_{i(0\to 1)} \qquad (3)$$

$$P_{i0} = 1 - (P_{i(1\to 0)} - P_{i(0\to 1)}) \qquad (4)$$、、

$$Pi(1 \to 0) = P_{oi1} \times (1 - P_{mi1}) \times P_{m(i)} \qquad (5)$$

$$Pi(0 \to 1) = P_{oi1} + (1 - P_{oi1}) \times P_{mi1} P_{m(i)} \qquad (6)$$

After calculating P_{oi1} and P_{oi0} entropy of the information can be calculated from equation (7). For the case of TRNG the probability of occurring 1 and 0 i.e. P_{oi1} and P_{oi0} should be equal to 0.5. Then the maximum value of entropy approaches to '1'.

$$H(i) = -P_{oi1} \times \log_2 P_{oi1} - (1 - P_{oi1}) \times \log_2 (1 - P_{oi1}) \qquad (7)$$

Schematic diagram of proposed topology is shown in Fig. 2. It consists of oscillator 3 stages Ring Oscillator and 5 stage oscillator. Five stage ring oscillator is used as clock for SIPO register. Its output is connected to Ex OR based Preprocessor. 6 XOR gates it takes X_0, X_1, X_2, X_3 bits are taken for further calculations. The SIPO output is given to Multiplexer 4X1 and input to the XOR based postprocessor as shown in Fig. 3. It can be said that output bit of XOR based postprocessor is bit wise independent if its input are bitwise independent [7]. The output to the post processor bit is send to the enable pin of multiplexer. Depending upon that multiplexer will work. The select lines of multiplexer are connected to the Two bit updown counter to implement Tree based interleaving technique.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

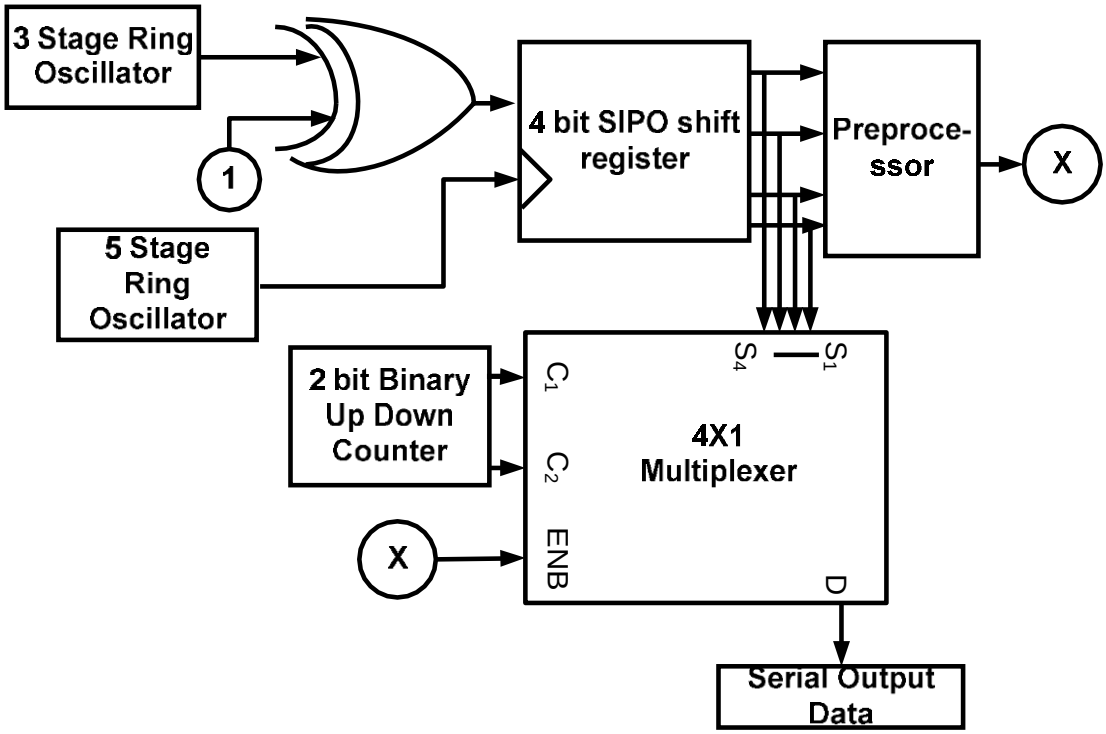

Fig. 2 Schematic diagram of proposed TRNG

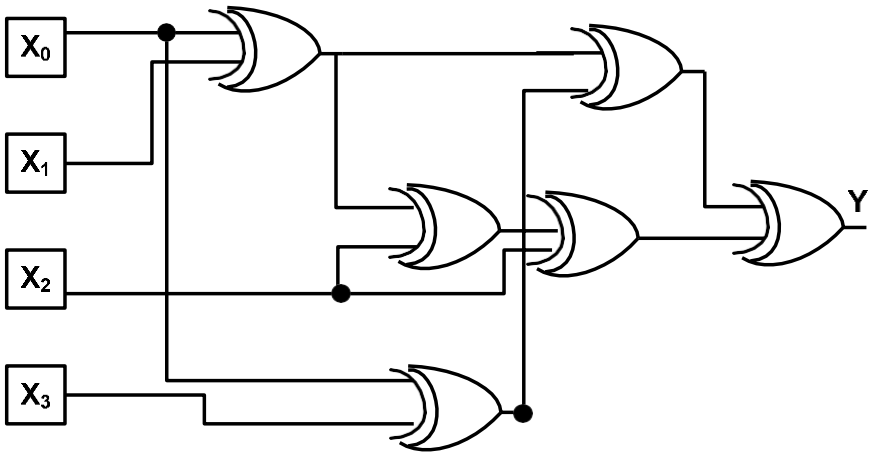

Fig. 3Post Processor consists of 6 XORs

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

4. SIMULATION RESULTS

A prototype has been developed for oscillator in AIMSPICE. For inverter CMOS topology is used with 0.25µm technology. Depending upon delay calculated using AIMSPICE the maximum frequency of 3 stage oscillator is about 10 MHz. The output voltage at different stage is shown in Fig.

4. From figure it can be said that the maximum frequency on which system can work is near about 6 MHz. After calculating the delay same delay has been given in student version of Xilinx 9.2i oscillator code. The complete prototype of proposed topology is developed in Xilinx 9.2i Since the oscillator may have jitter the system exact frequency on which it work will depends upon up down counter in which it's output is used as input for select lines of multiplexer.

Fig. 4 shows the output voltage waveform of AIMSPICE software. While Fig. 5 and 6 shows the bit pattern of final output for multilevel stage. The output bit can be increased by simply repeating the stage in the nibble pattern. For the implementation of this technique 20 macrocells are used.

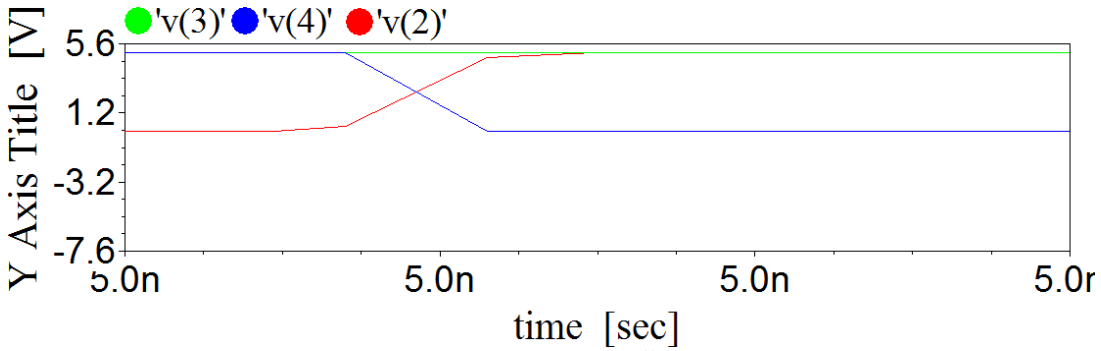

Fig 4. Oscillator AIM SPICE output at different stage

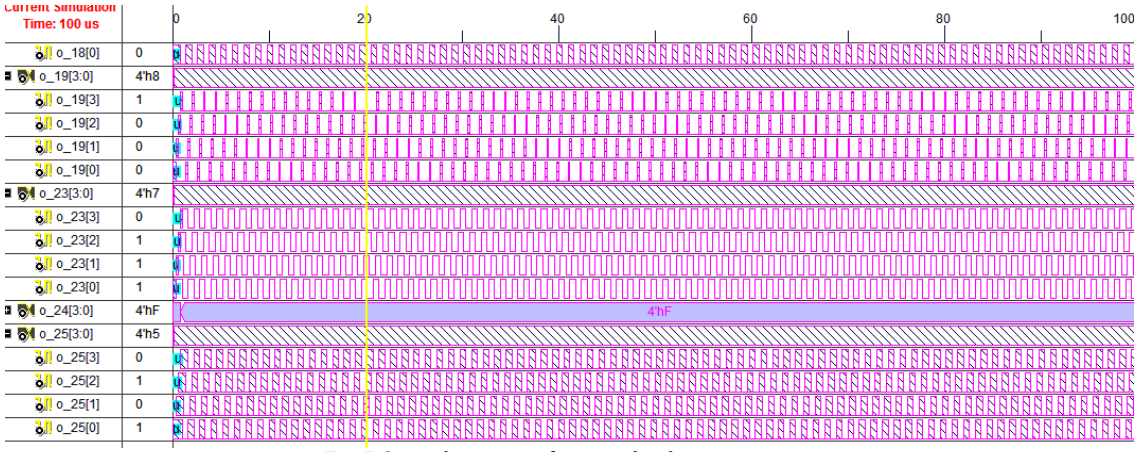

Fig. 5 Output bit pattern of proposed technique

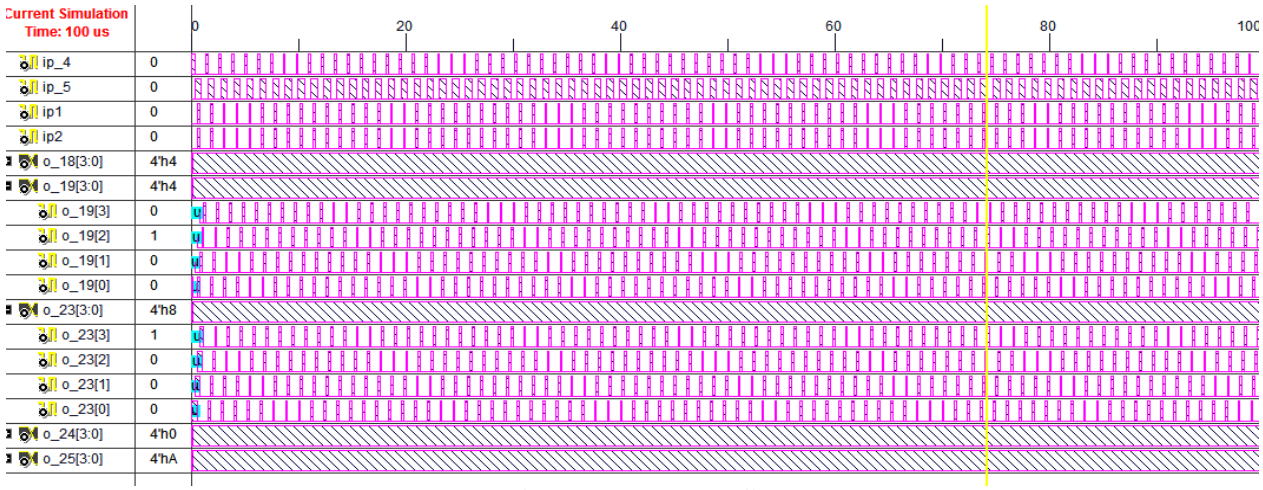

Fig. 6 Output bit pattern of proposed technique at different stage

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

From previous research [11-13] sources of random are gate delay, metastability and self timed circuits. In this paper we have combined all the parameters with tree based interleaving technique. The maximum rate on which system can work is 200-220 MHz the path delay is order of nano seconds.

5. CONCLUSION

In this paper a new idea for generation of TRNG is produced by using metastablity, XOR based post processor and tree based interleaving technique. The beauty of this work that for increasing number of bits this module can be repeated. Simultaneously generation of multiple bits it can be easily used. If input to the system is known then it can also be used in cryptography. It has lots of application in banking sectors, games and lottery systems. It can also be easily utilized in light weight envoirment.

REFERENCES

[1] Liu, Dongsheng, 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 Transactions on Circuits and Systems II: Express Briefs* 63, no. 6 (2016): 608-612.

[2] Golic, Jovan Dj. "New methods for digital generation and postprocessing of random data." *IEEE transactions on computers* 55, no. 10 (2006): 1217-1229.

[3] Mei, Faqiang, Lei Zhang, Chongyan Gu, Yuan Cao, Chenghua Wang, and Weiqiang Liu. "A highly flexible lightweight and high speed true random number generator on FPGA." In *2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pp. 399-404. IEEE, 2018.

[4] Park, Hojoong, Yongjin Yeom, and Ju-Sung Kang. "A Lightweight BCH Code Corrector of TRNG with Measurable Dependence." *Security and Communication Networks* 2019 (2019).

[5] Golic, Jovan Dj. "New methods for digital generation and postprocessing of random data." *IEEE transactions on computers* 55, no. 10 (2006): 1217-1229.

[6] Y.-S. Kim, J.-W. Jang, and D.-W. Lim, "Linear corrector overcoming minimum distance limitation for secure TRNG from (17, 9, 5) quadratic residue code," *ETRI Journal*, vol. 32, no. 1, pp. 93–101, 2010.

[7] S. Kwok, Y. Ee, G. Chew, K. Zheng, K. Khoo, and C. Tan, "A Comparison of Post- Processing Techniques for Biased Random Number Generators," in *Information Security theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication*, vol. 6633 of *Lecture Notes in Computer Science*, pp. 175–190, Springer, Berlin, Germany, 2011.

[8] Shukla, Manoj, Vinay Kumar Srivastava, and S. Tiwari. "Analysis and design of tree based interleaver for multiuser receivers in IDMA scheme." In *2008 16th IEEE International Conference on Networks*, pp. 1-4. IEEE, 2008.

[9] Liu, Dongsheng, 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 Transactions on Circuits and Systems II: Express Briefs* 63, no. 6 (2016): 608-612.

[10] Federal Information Processing Standard 180-4, Secure Hash Standard (SHS), 2015.

[11] H. Hata and S. Ichikawa, "FPGA implementation of metastability-based true random number generator," *IEICE Trans. Information & Systems*, vol. 95-D, pp. 426-436, 2012.

[12] N. De`ak, T. GyËorfi, K. M`arton, L. Vacariu, and O. Cret, "Highly efficient true random number generator in FPGA devices using phase-locked loops," *Proc. Int. Conf. Control Systems & Computer Science*, pp. 453-458, 2015.

[13] H. Martin, P. Peris-Lopez, JE. Tapiador and ES. Millan, "A new TRNG based on coherent sampling with self-timed rings," *IEEE Transactions on Industrial Informatics*, pp. 91-100, 2016.