ISSN: 2278-4632
Vol-13, Issue-06, June 2023

# A Novel Ultra-Compact FPGA-Compatible TRNG Architecture Exploiting Latched Ring Oscillators

[1]PITHANI BHAGYA SWATHI, [2]SIRIPALLI RAGHAVA RAO, [3]BODDAPALLI VENKATA RAMANA.
[1]PG Student, Dept. of ECE, BVC Institute of Technology and Science, Amalapuram. A.P
[2] Associate professor, Dept. of ECE, BVC Institute of Technology and Science, Amalapuram. A.P.
[3]Professor, Dept. of ECE, BVC Institute of Technology and Science, Amalapuram. A.P.

**ABSTRACT:** True random number generators (TRNGs) are widely used in cryptographic applications such as key generation, random padding bits, and generation of challenges and nonces in authentication protocol. This paper proposes a new and efficient method to generate true random numbers in XILINX by utilizing the random jitter of free running oscillators as a source of randomness. The main advantage of the proposed true random number generator utilizing programmable delay lines is to reduce correlation between several equal length oscillator rings, and thus improve the randomness qualities. Generalised FIFO is used to store generated sequence of patterns. clock gating architecture to limit the switching activity of the address decoder which improves the power efficiency of the proposed number generator. element structure is adapted to evaluate the clock cycle to the present ring counter block and to release the clock pulse to the next ring counter block.
**KEYWORDS:** True random number generators, Von-Neumann correction, Linear Feedback Shift Register, Look Up table.

**INTRODUCTION:** Computer systems and telecommunications play an important role in modern world technology. The communication and data transfer through computers touches almost every aspect of life, i.e. transferring data, tracking personal data, trading over the internet, online banking and sending emails. As more vital information is transferred through wire or wireless means, the need to safeguard all this data from hackers is growing. All these security concerns emphasize the importance of developing methods and technology for the transformation of data to hide its information content, prevent its modification, and prevent unauthorized use. Random number generation is a fundamental process for protecting the privacy of electronic communications. It is a key component of the encryption process that protects information from hackers by making it unreadable without the proper decryption process. Since the strength of an encryption mechanism is directly related to the randomness of the binary numbers used in it, there has been an enormous need to design and develop an efficient random number generator that can produce true random numbers to implement a safe and secure cryptographic system. In addition to cyber security, random number generators (RNGs) are a vital ingredient in many other areas such as computer simulations, statistical sampling, and commercial applications like lottery games and slot machines. Random numbers are needed in some areas in computer science, such as authentication, secret key generation, game theory, and simulations. In these applications, particularly numbers should have good statistical properties and be unpredictable and non-reproducible. In modern cryptographic systems, security is based on the statistical quality and on the unpredictability of confidential keys. These keys are generated in random number generators (RNGs) using random physical phenomena that occur in the hardware devices in which the system is implemented. A widespread source of randomness in digital devices is the jitter of the clock signal generated inside the device using free running oscillators such as ring oscillators [SMS07, BLMT11, RYDV15], or self-timed rings [CFAF13]. The statistical quality and unpredictability of the generated numbers depend on the size and quality (e.g. the spectrum) of the clock jitter. It is therefore good practice to continuously monitor this jitter using an embedded jitter measurement method. As required in the document AIS-20/31 published by the German Federal Office for Information Security (German acronym BSI) [KS11], the measured jitter parameters should then be used as input parameters in the stochastic model used to estimate entropy, which characterizes the unpredictability of generated numbers.

**LITERATURE REVIEW**: This section highlights the literature survey which has been done to review the critical points of the related works in recent days. In an irreversible circuit, if

ISSN: 2278-4632
Vol-13, Issue-06, June 2023

one bit information is lost then at least KTln2 joules of energy is dissipated. Where K is Boltzmann's constant and T is absolute temperature. This was stated by Landauer R in 1961. In 1973, Bennett proved that, KTln2 joules of energy dissipated due to information loss in irreversible circuit can be controlled by reversible logic where the reversible circuit allows to reproduce the inputs from output resulting in no information loss. He also showed that reversible systems can do the same computations as the classical or irreversible systems at same efficiency. This leads to the evolution of reversible logic based systems. Any reversible gate should have equal number of inputs and outputs such that, inputs can be recovered uniquely from outputs at any point of time. In paper [3], by ShibinuA.R ,Rajkumar, a 4- bit LFSR design using Muller expression is proposed. This paper also gives realization of both edge triggered and level triggered D flip flop using reversible logic. At the end, comparative analysis has been given between conventional LFSR and Reversible LFSR. From this it is observed that, the proposed technique is efficient than conventional technique in implementing LFSR in terms of cost metrics like power, quantum cost, garbage output and gate count. D. Muthih and A. ArockiaBazil Raj [4] have presented a parallel architecture for designing high speed LFSR and explained that, BCH encoders and CRC operations are normally carried out by using LFSR. A novel approach for high speed BCH encoder is proposed. This paper presents two key points. First, it presents a linear transformation algorithm for converting a serial LFSR into parallel architecture, which can be used for generating polynomials in CRC and BCH encoders. Secondly, a new approach is proposed to amend parallel LFSR into pipelining and retiming algorithm. In paper [5], authors have presented two design approaches for designing reversible D FF with asynchronous set/reset which are optimized in terms of quantum cost, delay and garbage outputs. It also includes the design of 3 bit LFSR using two design approaches. The application of these FF's as LFSR is designed and discussed. The application of LFSR as pseudo random bit sequence generator is proposed. The paper is concluded with the comparative analysis of proposed approaches against performance parameters like garbage output, delay and quantum cost. Research paper [6], presents three different automated techniques for implementing LFSR as well as D flip flop so that the layout area and power consumption will be minimized. It is illustrated that LFSR is key component to provide self-test of an Integrated Circuit (IC). This paper implements LFSR upto layout level which will be a key component for low power application. The research explores the LFSR as well as D flip flop using different architecture in a 0.18µm CMOS technology; so that the layout area will be minimized and consumes less power.

**ARCHITECTURE OF TRUE RANDOM NUMBER GENERATOR:**

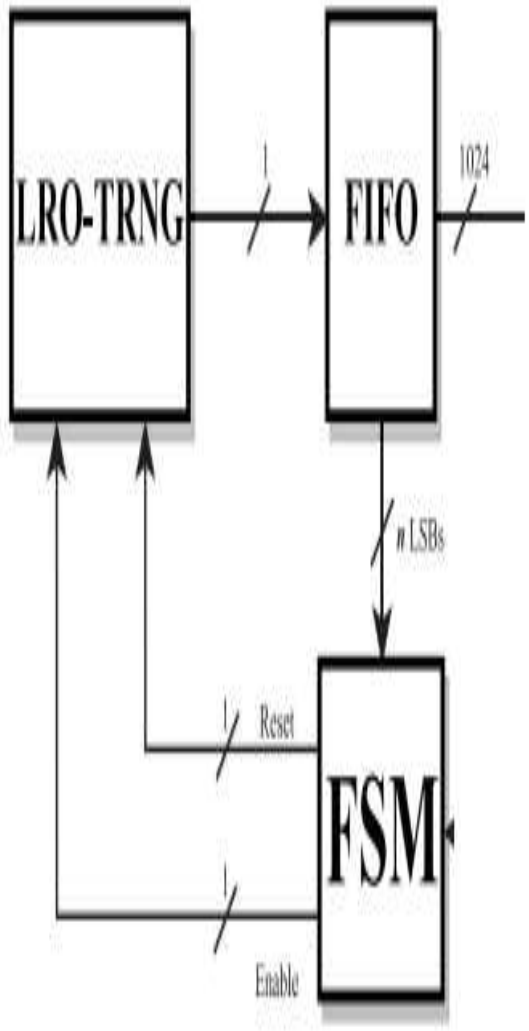


Fig. 1. Block scheme of the TRNG validation testbed.

ISSN: 2278-4632
Vol-13, Issue-06, June 2023

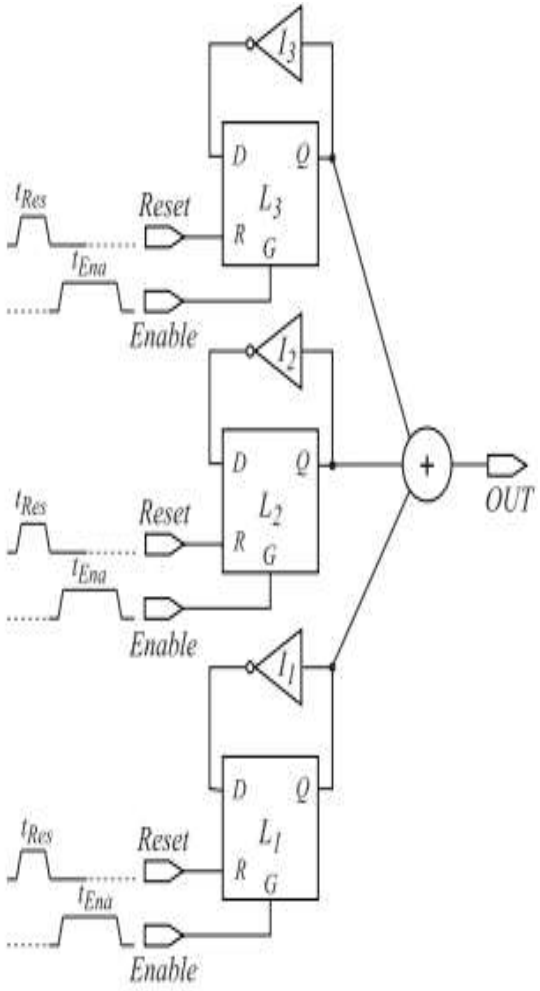


Fig. 2 TRNG Architecture.

The block scheme of the proposed TRNG architecture is shown in Fig. 1 The single TRNG cell exploits three latches L1, L2 and L3 closed in a ring oscillator configuration through three inverters I1, I2 and I3 respectively. When a logic '0' is applied to the Gate inputs (G) of the D-Latches, they are in the hold state and are insensitive to variations on the D inputs. On the other hand, when the G inputs of the latches are set to logic '1', the latches become transparent and their outputs Q follow the variations on the D inputs. According to this behavior, when the latches are transparent a free running oscillation comes out, whereas, when they enter in the hold state, the logic value of the output bit is sampled. Since the propagation delay from the D inputs to the Q outputs

tDQi, (i = 1, 2, 3) of D-Latches L1, L2 and L3, and the propagation delay tIVi, (i = 1, 2, 3) of the inverters I1, I2 and I3, are dependent on the physical implementation and on the delay of the routing path of the three latches, each RO exhibits an oscillation period (denoted as TROi) equals to:

$$T_{ROi} = \frac{1}{2 \cdot (t_{DQi} + t_{IVi})} \quad (1)$$

The operation of the proposed TRNG requires the following excitation sequence: 1) Set the Reset signals to logic '1' for a time tRes in order to reset the outputs of the three D-Latches to logic '0'; 2) Set a logic '0' on the Reset inputs and set the Enable signals to logic '1' for a time tEna thus enabling the three ROs; 3) After a time tEna, set a logic '0' on the Enable input in order to sample the output random bit. Each bit has to be generated by means of the above Reset and Enable sequence. It is evident, from these considerations, that the overall throughput (TP) is limited by the time tRes + tEna and the bit-sequence throughput is given by the following equation: TP = 1 tRes + tEna

bit s (2) As will clarified in the next sections, the entropy of the output random sequence is directly related to the accumulated jitter and therefore to the excitation time tEna of the ROs. In fact, since an increase of tEna results in an increase of the entropy and in a reduction of the throughput, the proposed TRNG architecture requires to optimize the trade-off between these two figures of merit. For this purpose, it is important to remark that the behavior of the proposed LRO-TRNG is quite different from the one of conventional RO-TRNGs. In fact, previous works exploit the jitter of the ROs and the metastability of D-flip-flops by sampling the stream started in a single instant. It has to be noticed that in the proposed LRO-TRNG, when the gates are closed (i.e., the G inputs are at logic '0' and the data is sampled) a metastable state can be captured, thus increasing the entropy due to the metastability of D-Latches. However, since process, supply voltage and temperature (PVT) variations affect the oscillation frequencies of the three LROs of a single cell in the same way (i.e., are seen as common mode variations), the XOR operation between the output of the three D-Latches L1, L2 and L3 greatly improves the resilience of the proposed TRNG to PVT variations, thus providing very good statistical performances in spite of working condition variations as will be shown in Section IV-B. Another important point to remark is that, if the oscillation frequencies of the three LROs are extremely close to each other, locking phenomena can occur [7], and the statistical performances of the TRNG can be worsened, thus requiring additional postprocessing to perform on the output sequence. To avoid these issues, the oscillation

ISSN: 2278-4632
Vol-13, Issue-06, June 2023

frequencies of the three LROs have to be properly unbalanced during the implementation phase by exploiting the different delays available through the different FPGA blocks and routing resources. The whole design flow and routing strategies have been investigated accordingly to [8] The LRO-TRNG has been implemented in a single FPGA Slice by means of four LUTs and three Latches. Several

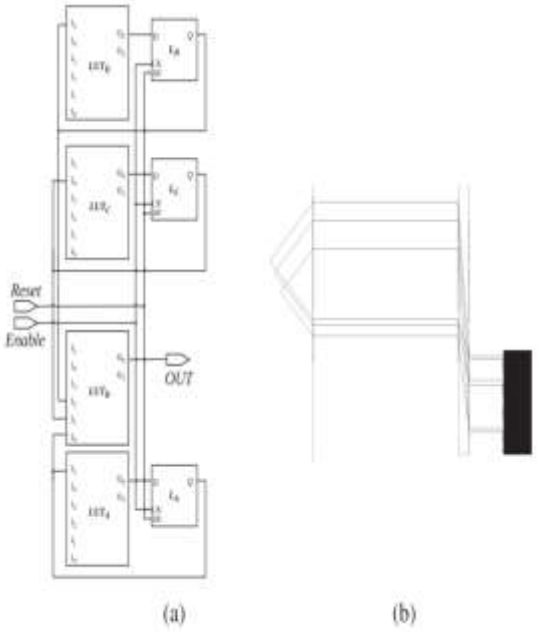


Fig.3. Slice implementation of the proposed TRNG (a); FPGA-editor's view of the Slice's intra-connections (b).

routing configurations have been investigated and the one that gives the best performances in terms of randomness and entropy has been selected and depicted in Fig. 2(a). As can be observed in Fig. 2(a) the LUTA, LUTC and LUTD have been employed to implement the inverters depicted in Fig. 1, whereas the three flip-flops configured as latches are FFA, FFC and FFD. Finally the three outputs of the D-Latches are XOR-ed by means of LUTB. The FPGA-Editor floorplan view of the feedback-connections of the LRO-TRNG macro-cell is reported in Fig. 2(b). An in-depth study of the switchmatrix block and the Placement Constraints provided by the Xilinx Guide [21] allowed us to choose the intra-connections resulting in optimal randomness performance. Delays of the routed paths of LUTA, LUTC and LUTD are denoted as tQI5A , tQI5C and tQI5D respectively. The nominal value of the delay between the LUTs' inputs and the D-Latches' outputs is about 950ps,1 according to [2]. As can be observed the three frequencies are in the range of [300,400] MHz; in this estimation we have also taken into account the fan-in effect of the LUTB.

Another important feature of the proposed implementation is the possibility for the three D-Latches to share the same Reset and Enable signals, thus improving the synchronism of the excitation sequence.

**MEMORY ARCHITECTURE**

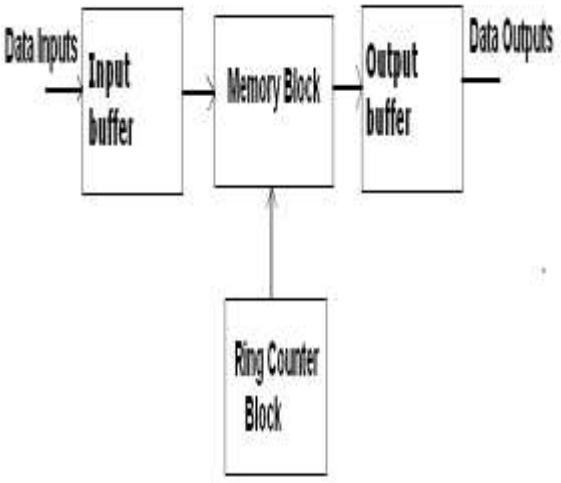


**Fig4: Memory Organisation**

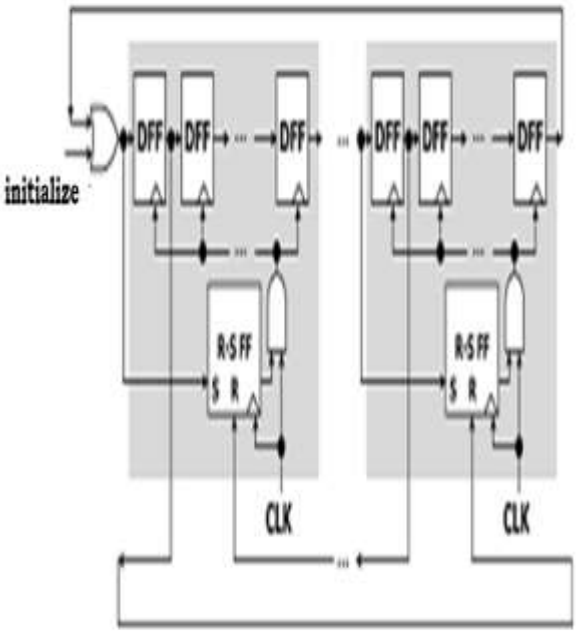


**Fig5 : Ring Counter With SR Flip-Flops**

The above block diagram shows the power controlled Ring counter. First, total block is divided into two blocks. Each block is having one SR FLIPFLOP controller to reduce constrained parameters.

**RESULT:**

ISSN: 2278-4632
Vol-13, Issue-06, June 2023

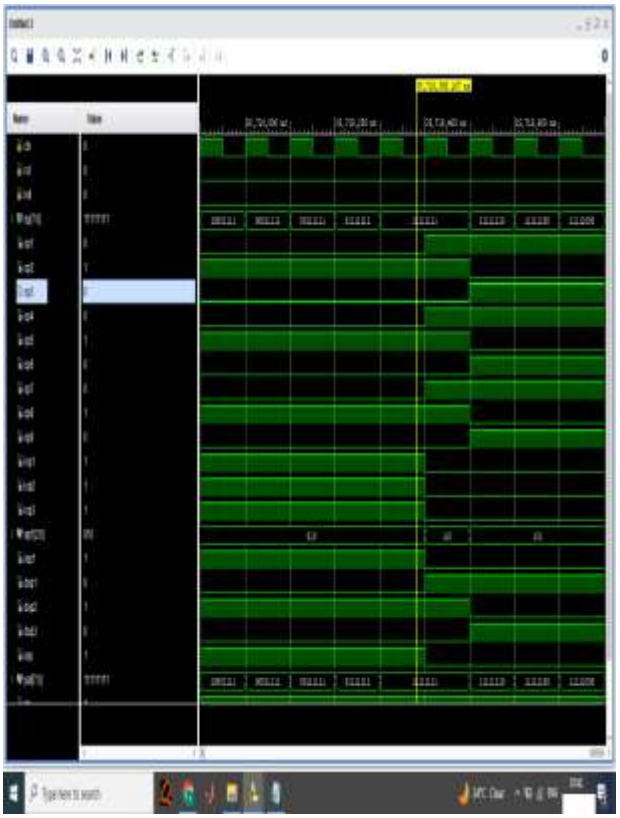

**Fig Proposed simulation result**

Above shown simulation results represents 8 bit patterns using proposed clock gating method in XILINX vivado2018 with modified structured memory organisation. Power supply will be transferred to corresponding block, which is accessed to store pattern of organised memory (RAM). For each and every simulation input signal 'clk' have to be clocked with raising edge as '1' and falling edge as '0'.

## CONCLUSION and FUTURE SCOPE:

A novel TRNG architecture that leverages the benefits of both the jitter of ring oscillators and the D-Latches' metastability has been proposed. A feedback strategy to randomly set the 4 LSBs of the control word defining the excitation time has been exploited to enhance the randomness and increase the entropy. The randomness of the raw response, shows that also when supply voltage variations are considered the TRNG is able to ful-fill the test requirements. The bit-swapping LFSR used to generates a random test sequence with low switching power by finding hamming distance between two adjacent patterns and minimizing that distance by using combinational logic. To further reduce the average power, dual threshold voltages are assigned. By using this method and finding out the critical and non-critical paths present in BIST and then assigning a low threshold voltage for critical path, and high threshold voltage for non-critical path, a further reduction in total power, especially leakage power, can be obtained.

## REFERENCES

[1] K. Nohl, D. Evans, S. Starbug, and H. Plotz, "Reverse-engineering a ¨ Cryptographic RFID Tag," in Proceedings of the 17th Conference on Security Symposium. USENIX Association, 2008, pp. 185–193.
[2] G. Marsaglia, "Diehard: A Battery of Tests of Randomness," 1996.
[3] ShibinuA.R ,Rajkumar. et. al, "Implementation of power efficient 4-bit reversible linear feedback shift register for BIST," Tech. Rep., 2010.
[4] D. Muthih and A. ArockiaBazil Raj, "mplementation of high-speed LFSR design with parallel architectures," 2014.
[5] Jayasanthi M, Kowsalyadevi AK, "Low Power Implementation of Linear Feedback Shift Registers ",2019
[6] M. Majzoobi, F. Koushanfar, and S. Devadas, "FPGA-Based True Random Number Generation Using Circuit Metastability with Adaptive Feedback Control," in Cryptographic Hardware and Embedded Systems – CHES 2011. Springer Berlin Heidelberg, 2011, pp. 17–32.
[7] H. Hata and S. Ichikawa, "FPGA Implementation of Metastability-Based True Random Number Generator," IEICE Transactions on Information and Systems, vol. E95.D, no. 2, pp. 426–436, 2012.
[8] A. P. Johnson, R. S. Chakraborty, and D. Mukhopadhyay, "An Improved DCM-Based Tunable True Random Number Generator for Xilinx FPGA," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 64, no. 4, pp. 452–456, April 2017.
[9] D. Liu, Z. Liu, L. Li, and X. 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, vol. 63, no. 6, pp. 608–612, June 2016.
[10] A. Beirami and H. Nejati, "A Framework for Investigating the Performance of Chaotic-Map Truly Random Number Generators," IEEE

ISSN: 2278-4632
Vol-13, Issue-06, June 2023

Transactions on Circuits and Systems II: Express Briefs, vol. 60, no. 7, pp. 446–450, July 2013.
[11] J. von Neumann, “Various techniques used in connection with random digits,” in Monte Carlo Method. National Bureau of Standards Applied Mathematics Series, 12, 1951, pp. 36–38. [12] 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.
[13] M. Dichtl and J. D. Golic, “High-Speed True Random Number Genera- ´ tion with Logic Gates Only,” in Cryptographic Hardware and Embedded Systems - CHES 2007. Springer Berlin Heidelberg, 2007, pp. 45–62.
[14] Harshitha G; Kishore E J; Manoj R; Priyanka R Devarmani; Praveen Kumar Y G; M Z Kurian, “Gate-Diffusion Input based Linear Feedback Shift Register : A Review,” in 2092 .
[15] K. Wold and C. H. Tan, “Analysis and Enhancement of Random Number Generator in FPGA Based on Oscillator Rings,” in Int. Conf. on Reconfigurable Computing and FPGAs, Dec 2008, pp. 385–390.
[16] O. Petura, U. Mureddu, N. Bochard, V. Fischer, and L. Bossuet, “A survey of ais-20/31 compliant trng cores suitable for fpga devices,” in 2016 26th International Conference on Field Programmable Logic and Applications (FPL), Aug 2016, pp. 1–10.
[17] N. Bochard, F. Bernard, V. Fischer, and B. Valtchanov, “TrueRandomness and Pseudo-Randomness in Ring Oscillator-Based True Random Number Generators,” Int. J. Reconfig. Comp., vol. 2010, pp. 879 281:1–879 281:13, 2010.