IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 9, September 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209040 |

Power optimized &True Random Number Generation Using Programmable Delays in Oscillator-Rings

Cheruvu Veera Suharsha[1], Dr.A.M.Prasad[2]

Student, M.Tech, VLSI&Embedded Systems, Dept. of ECE, UCEK (A), JNTUK, Kakinada, India[1]

Professor, Dept .of ECE, UCEK (A), JNTUK, Kakinada, India[2]

ABSTRACT: This study offers a novel and effective technique for producing real random numbers in XILINX, which find significant applications in cryptography, including key generation, random padding bits, and challenges/nonce in authentication protocols. The suggested method uses free-running oscillators' random jitter as a source of randomness. A key advantage of the method is its use of programmable delay lines, reducing correlation between equal length oscillator rings and thereby enhancing the randomness of the generated numbers. To store the generated sequence of patterns, a Generalized FIFO is utilized. Moreover, In order to reduce switching activity in the address decoder and hence increase the proposed number generator's power efficiency, the study offers a clock gating architecture. The element structure has also been modified to evaluate the current ring counter block's clock cycle and release the clock pulse to the following ring counter block.

KEYWORDS: True random number generators, Von-Neumann correction, Linear Feedback Shift Register, Look Up table.

I. INTRODUCTION

Computer systems and telecommunications are essential components of modern technology, permeating various aspects of our lives, including data transfer, personal tracking, online banking, and email communication. As the transmission of vital information occurs through both wired and wireless means, the necessity to protect this data from hackers has become increasingly crucial. Addressing these security concerns calls for the development of advanced techniques and technologies that can transform data, concealing its content, preventing modifications, and thwarting unauthorized use.

A fundamental process in safeguarding electronic communications is random number generation, a key element in encryption methods that render information unreadable without the appropriate decryption process. The strength of an encryption mechanism relies heavily on the randomness of the binary numbers it employs. Consequently, the demand for efficient random number generators capable of producing true random numbers has grown significantly, ensuring the implementation of secure and fool proof cryptographic systems.

Beyond its role in cyber security, random number generation serves as a critical component in various other domains, including computer simulations, statistical sampling, and commercial applications like lottery games and slot machines. In computer science, random numbers are indispensable in areas such as simulations, game theory, secret key generation, and authentication. The generated numbers must be very unexpected, non-reproducible, and have strong statistical features in various applications.

The statistical reliability and unpredictable nature of private keys are fundamental components of contemporary cryptography systems. Random number generators (RNGs) use arbitrary physical phenomena that happen randomly in the hardware components that the system uses to do this. The jitter of the clock signal, produced by free-running oscillators like ring oscillators or self-timed rings, is a typical source of unpredictability in digital systems. Aspects like the size and quality of the clock jitter's spectrum have an impact on the generated numbers' quality and predictability. It is recommended as best practise to continuously monitor this jitter using an incorporated jitter measurement approach.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209040 |

The German Federal Office for Information Security (BSI) document AIS-20/31 emphasizes the importance of utilizing the measured jitter parameters as input in a stochastic model for estimating entropy, which describes the randomness of the generated numbers. By adhering to these guidelines and implementing effective random number generation techniques, secure and reliable cryptographic systems can be established to protect sensitive data and ensure the integrity of electronic communications.

II. LITERATURE REVIEW

This section presents a comprehensive literature survey conducted to review critical points from recent works. It begins by discussing the concept of irreversibility in circuits, where the loss of one bit of information results in the dissipation According to Landauer R. in 1961, there must be at least KTln2 joules of energy. Bennett, however, showed in 1973 that reversible logic can regulate this energy loss brought on by irreversible circuit information loss. Reversible circuits make it possible to replicate inputs from outputs, which prompted the creation of systems based on reversible logic. In order to ensure that inputs may always be separately recovered from outputs, reversible gates must have an equal number of inputs and outputs.

ShibinuA.R. and Rajkumar suggest a 4-bit LFSR architecture employing the Muller expression in their research work [3]. The research also shows reversible logic realisations of edge-triggered and level-triggered D flip flops. Reversible LFSRs and traditional LFSRs are compared, with the results showing that the suggested method is more effective in terms of cost parameters including power, quantum cost, trash output, and gate count. Another study by D. Muthih and A. Arockia is available at [4].Bazil Raj examines the usage of high-speed LFSRs in BCH encoders and CRC procedures and introduces a parallel architecture for creating them. In addition to outlining a linear transformation algorithm to transform a serial LFSR into a parallel architecture, the research suggests a novel strategy for high-speed BCH encoders.

Two design strategies for reversible D flip-flops with asynchronous set/reset are shown in the following study [5], which is optimised for quantum cost, delay, and garbage outputs. With the application of these flip-flops as LFSRs and their prospective usage as pseudo-random bit sequence generators, the creation of a 3-bit LFSR utilising these methods is also presented. The comparison of the suggested techniques based on performance indicators such trash output, delay, and quantum cost is the final section of the paper.

In a different research publication [6], three distinct automated methods for LFSRs and D flip-flops are presented to minimize layout area and power consumption. The paper highlights the importance of LFSRs in providing self-test capabilities for Integrated Circuits (ICs). By implementing LFSRs up to the layout level, the paper emphasizes their significance as key components for low-power applications. Furthermore, the research explores various architectures for LFSRs and D flip-flops in a 0.18μm CMOS technology, aiming to reduce layout area while optimizing power consumption.

Overall, these studies contribute valuable insights into the design and optimization of LFSRs, D flip-flops, and reversible logic-based systems. The research findings underscore the significance of efficient and low-power implementations in advancing modern integrated circuit technology.

III. ARCHITECTURE OF TRUE RANDOM NUMBER GENERATOR

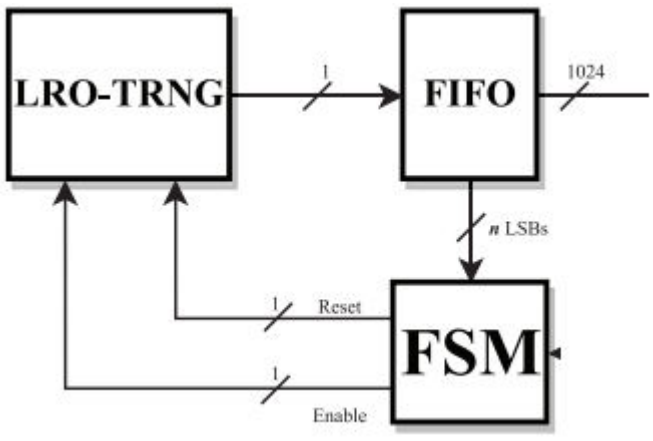

Fig. 1. Block scheme of the TRNG validation testbed.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209040 |

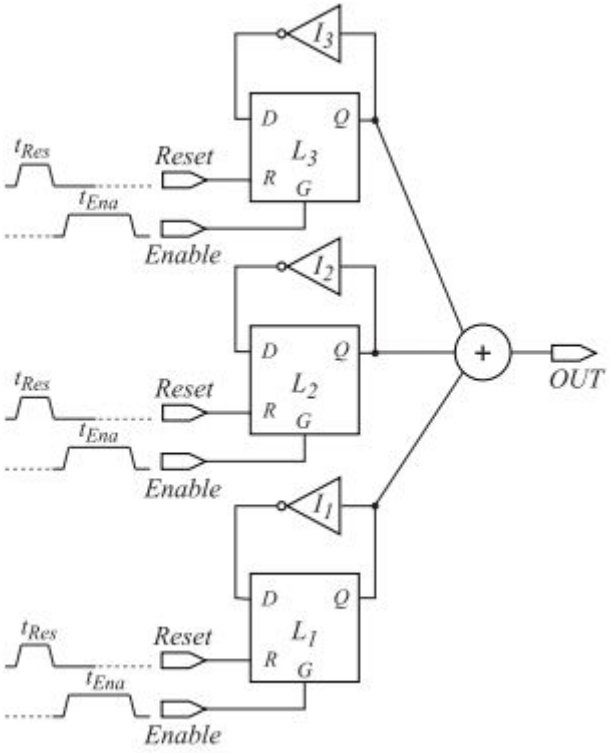

Fig. 2 Existing TRNG Architecture

Fig. 1 shows the proposed True Random Number Generator (TRNG) architecture. The TRNG cell has three latches (L1, L2, and L3) that are grouped in a ring oscillator structure. An inverter (I1, I2, or I3) controls each latch individually. The condition of the Gate inputs (G) determines how the latches behave. The latches are in the hold state when a logic '0' is applied to the Gate inputs, making them unresponsive to changes in the D inputs. In contrast, turning the G inputs to logic '1' makes the latches transparent and causes their Q outputs to follow changes in the D inputs. As a result, a free-running oscillation is produced when the latches are transparent, while in the hold state, the logic value of the output bit is sampled.

The propagation delays of the inverters I1, I2, and I3 and the D-Latches L1, L2, and L3 from the D inputs to the Q outputs (tDQi, i = 1, 2, 3) together determine the oscillation period (TROi) of each Ring Oscillator (RO). The three latches' routing path and physical implementation both have an impact on these delays.

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

The excitation sequence used by the proposed True Random Number Generator (TRNG) is as follows:

To start, reset the three D-Latches' outputs to logic '0' by setting the Reset signals to logic '1' for the duration of tRes.

The three Ring Oscillators (ROs) should then be enabled by setting a logic '0' on the Reset inputs and a logic '1' on the Enable signals for a time period tEna.

To sample the output random bit, set a logic '0' on the Enable input after a period of time tEna. The provided Reset and Enable sequence is used to generate each bit.

The bit-sequence throughput is governed by the formula: TP = 1 / (tRes + tEna) bits (Eq. 2). The total throughput (TP) of the TRNG is constrained by the sum of the time periods tRes and tEna.

The cumulative jitter, which is determined by the excitation time tEna of the ROs, is directly related to the entropy of the output random sequence. Increasing tEna results in higher entropy but reduces the throughput. Thus, optimizing the trade-off between these two factors is essential for the TRNG's performance.

It is significant to notice that the proposed LRO-TRNG behaves differently from traditional RO-TRNGs. When the gates are closed in the LRO-TRNG (G inputs are logic '0' and data is sampled), it is feasible to capture a metastable state, which increases the entropy since D-Latches are metastable. However, XORing the output of the three D-

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209040 |

Latches (L1, L2, and L3) considerably increases the TRNG's resistance to process, supply voltage, and temperature (PVT) fluctuations. This XOR operation acts as a common mode variation, ensuring good statistical performance despite variations in working conditions.

To avoid locking phenomena and potential degradation of statistical performance, During the implementation phase, the three LROs' oscillation frequencies should be correctly imbalanced. This can be accomplished by utilising the various delays offered by the FPGA blocks and routing resources. Accordingly, design flow and routing strategies have been researched.

Utilising four LUTs and three Latches, the LRO-TRNG has been successfully built in a single FPGA slice. Various experiments and analyses have been conducted to validate its performance, confirming its suitability as a reliable and efficient True Random Number Generator.

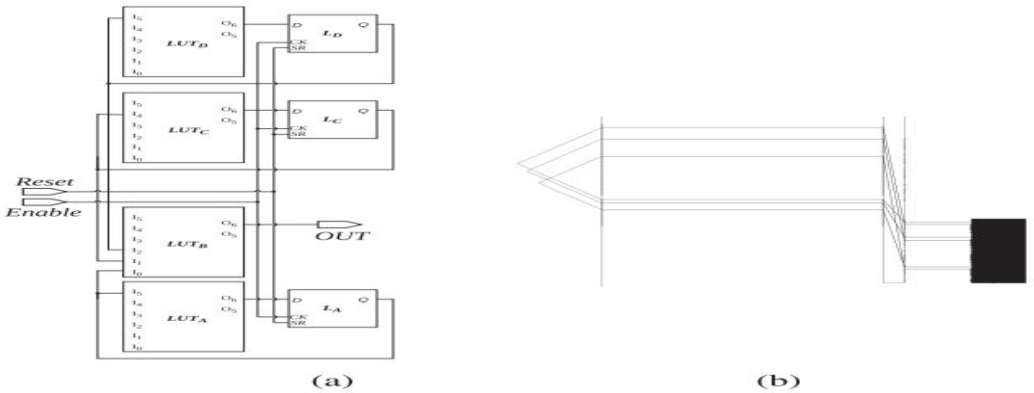

Fig. 2. Slice implementation of the suggested TRNG (a); view of the Slice's intra-connections from an FPGA editor (b)

After a thorough analysis of numerous routing configurations, the best design in terms of unpredictability and entropy was chosen and is shown in Fig. 2(a), which is also the most effective arrangement overall. In this architecture, the inverters shown in Fig. 1 have been implemented using LUTA, LUTC, and LUTD, while the three flip-flops serving as latches are designated as FFA, FFC, and FFD. The three D-Latches outputs are then XORed through LUTB to create a single output.

Fig. 2(b) depicts the floorplan view of the feedback connections for the LRO-TRNG macro-cell in the FPGA Editor. The switch matrix block and the Placement Constraints were thoroughly examined in accordance with the Xilinx Guide [21], and the intra-connections that optimise randomization performance were found.

The LUTA and LUTC routed pathways' delays, and LUTD are represented by tQI5A, tQI5C, and tQI5D, respectively. According to [2], the nominal delay between the inputs of the LUTs and the D-Latches' outputs is approximately 950ps. The frequencies of the three oscillators are observed to fall within the range of [300, 400] MHz, considering the fan-in effect of LUTB in the estimation.

The ability of the three D-Latches to share the same Reset and Enable signals, which improves the synchronism of the excitation sequence, is another remarkable feature of the proposed solution. The TRNG's overall performance and dependability are aided by this synchronisation.

In summary, the chosen routing configuration, careful consideration of constraints on placement and the switch matrix, and the shared Reset and Enable signals in the D-Latches collectively optimize the performance of the LRO-TRNG, ensuring superior randomness and entropy for reliable random number generation.

IV. MEMORY ARCHITECTURE

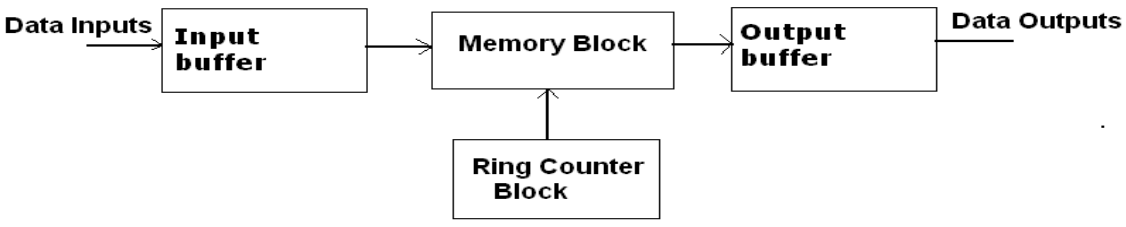

Fig3: Memory Organisation

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209040 |

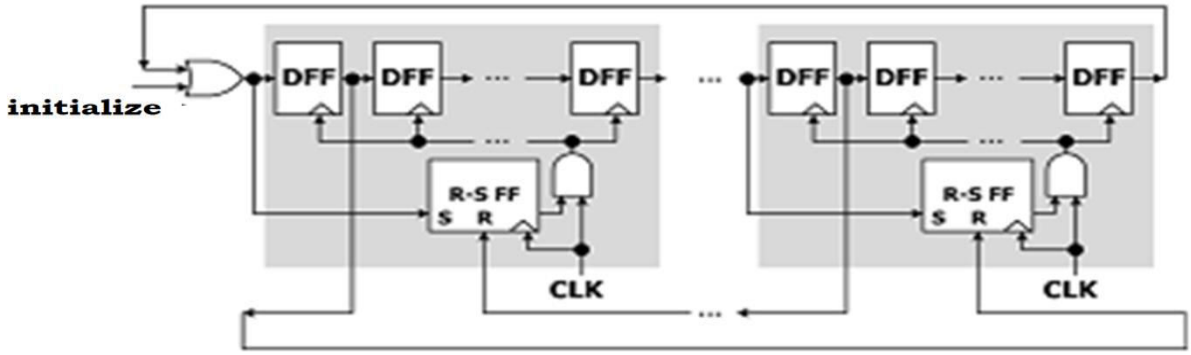

Fig4 : Ring Counter With SR Flip-Flops

The power-controlled Ring counter is depicted in the block diagram above, divided into two blocks, each featuring an SR FLIPFLOP controller to minimize constrained parameters.

V. RESULT

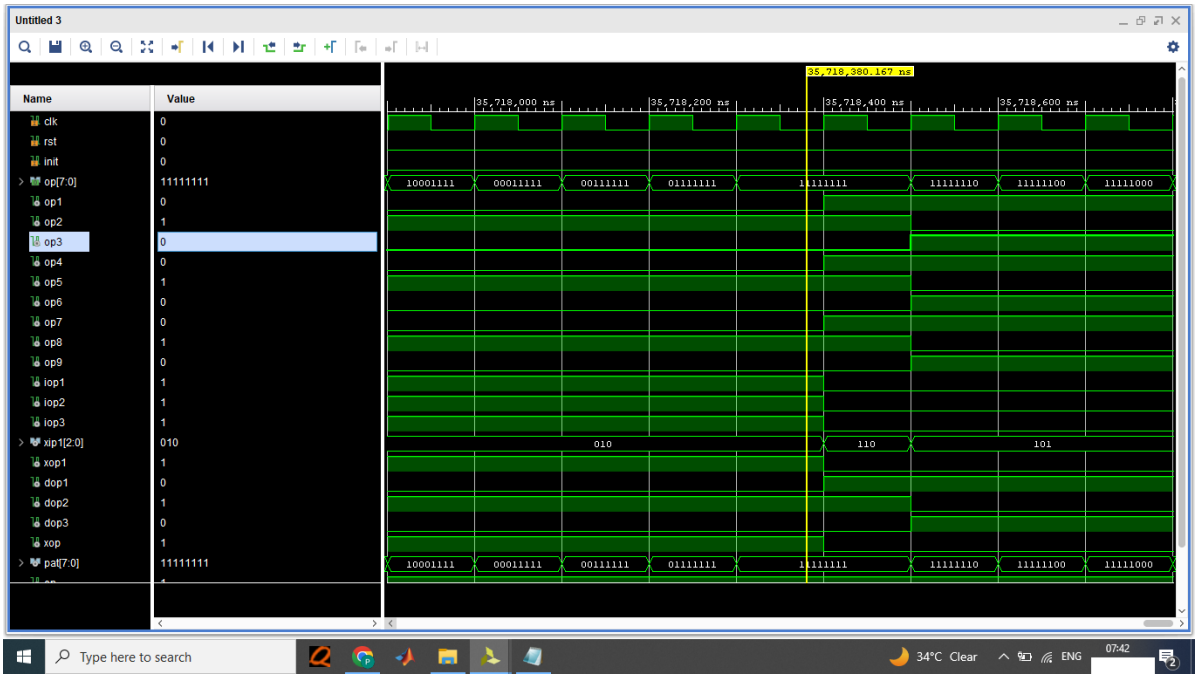

Fig. Proposed simulation result

The simulation results displayed above illustrate 8-bit patterns generated using the proposed clock gating method in XILINX Vivado 2018, with a modified structured memory organization. The power supply is directed to the corresponding block, which is accessed to store patterns in an organized memory (RAM). In each simulation, the input signal 'clk' is clocked with a rising edge as '1' and a falling edge as '0'.

VI. CONCLUSION AND FUTURE SCOPE

A novel True Random Number Generator (TRNG) architecture that combines the advantages of ring oscillator jitter and D-Latches' metastability has been proposed. The randomness is enhanced by employing a feedback technique to set the control word's four low-frequency bits at random, thereby increasing entropy. The TRNG fulfils test requirements even under supply voltage variations. Additionally, a bit-swapping Linear Feedback Shift Register (LFSR) generates By applying combinational logic to reduce the hamming distance between adjacent patterns, a random test sequence with minimal switching power can be created. To further reduce average power consumption,

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209040 |

dual threshold voltages are assigned, with a low threshold for critical paths and a high threshold for non-critical paths, effectively reducing total power, particularly leakage power.

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 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 Generation 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.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details