Fault-Tolerant Reversible-Logic Based Ro-Puf For Secure Device Authentication

S.Gayathri[1], P.Sridevi[2]
[1]Dept of ECE
[2]Assistant Professor, Dept of ECE
[1, 2] TAGORE INSTITUTE OF ENGINEERING AND TECHNOLOGY(TAMILNADU)

Abstract- *Protecting data and hardware is vital, drivingthe adoption of Physically Unclonable Functions (PUFs) for generating unique circuit signatures. This paper introduces a fault-tolerant system featuring a ring-oscillator (RO) based PUF, utilizing a reversible logic (RL) design. The proposed system comprises various sub-systems such as Fault-Tolerant RL-based inverter design, Reversible-Logic designing, Fault-Detection module, Fault-free path selection module, and the Reversible RO-PUF module. The proposed design is implemented on a Basys-3 FPGA board for calculating various PUF parameters. It is observed that the uniqueness, uniformity, and bit-aliasing of the proposed design at 27◦C are 49.40%, 51.20%, and 48.30%, respectively. Further, bit-error-rate (BER), reliability, and key error rate (KER) are determined at three different temperatures, and the best results obtained are 0.003%, 99.7%, and 0.092 at 40◦C, respectively. Compared to conventional PUFs, the proposed design showcases higher reliability (0.002% to 0.11%) and significantly reduced BER and KER (1.67× to 22.67×, and 1.6× to 8.02× respectively). The proposed design also passed 15 NIST tests against conventional RO-PUF, which could pass only 11 NIST tests. We have also tested the resilience of different PUF designs against three machine-learning models with the best accuracy of 58.9% against the Logistic Regression model.*

Keywords- Reversible logic, double-Feynman gate, fault-tolerant gates.

I. INTRODUCTION

In the landscape of consumer electronics, Physically Unclonable Function (PUF) technology stands as a keystone, augmenting the security of devices like televisions, cameras, smartphones and tablets. Leveraging the intrinsic and distinctive traits of semiconductor chips, PUFs forge electronic fingerprints that are virtually impossible to replicate, ensuring secure identification and thwarting unauthorized access or counterfeiting attempts. Depicts the comprehensive lifecycle of PUF within consumer electronics, from the design phase, where specific security needs dictate PUF requirements through the integration into hardware architecture during semiconductor chip manufacturing, to its utilization during the device's configuration. The digital fingerprints generated by PUFs act as crucial authentication tools, safeguarding against tampering or counterfeit components. Manufacturers continually update PUF-related security features to enhance device security, employing PUFs in the secure boot process of smartphones and gaming consoles to guarantee the loading of authorized firmware or software. This integraltechnology not only fortifies the authenticity and security of consumer electronics but also shields user data and mitigates threats posed by counterfeit electronics, positioning PUFs as a pivotal element in meeting the escalating demand for secure and reliable consumer electronics.

Circuit and system resilience encompasses fault tolerance, which is crucial for systems to operate in the face of faults. High fault tolerance enables continued operation, partially or fully, after a failure, requiring comprehensive consideration of potential faults and their implications throughout the equipment's life cycle. Designing fault-tolerant systems involves aligning tolerance levels with fault criticality and optimizing costs and resources at every life cycle stage, from specification and design to validation, verification, maintenance, and operation. As technology progresses beyond the sub-10 nm node, accommodating billions of transistors within a single IC poses challenges. Moore's law initially drove improvements in performance, but there have been challenges to further transistor size reductions beyond the 10nm node. Reversible computing is an emerging field that seeks to reduce power consumption in digital logic circuits and systems, which will be especially advantageous for low-power design and quantum computing.

Quantum computing emerges as a promising alternative, challenging the conventional semiconductor fabrication era.

This shift not only fuels the evolution of reversible designs inthese methods into traditional digital IC design. These developments pose significant implications for the future of circuit design and semiconductor technology.Digital

logic gates operate by conveying binary logic signals among various functional blocks in digital design, facilitating arithmetic and logic operations in computing processors' ALUs through the exchange of logic 1s and 0s across combinational and sequential blocks. Despite their capability to execute extensive operations, digital circuits suffer from an inherent limitation of irreversible design, resulting in output signals that cannot deduce input signal information.

Landauer's principle highlights the energy dissipation incurred in irreversible bit operations, where each operation dissipates approximately $KTln_2$ (Joules), affecting lower technology nodes by generating excess heat that can impede overall performance. To address these challenges, reversible logic emerges as a potential solution, offering energy-efficient processing and minimizing information loss in advanced node computing and low-power VLSI circuits. Reversible circuits, necessary for reversible logic gates, feature bijective mappings between input and output vectors, preserving bits and reducing power dissipation. Various reversible gates, includingFeynman, Double-Feynman Gate (DFG) and Modified New Fault-Tolerant (MNFT) gates, boast differing input-output vectors and parity-preserving features, crucial for error detection. These fault-tolerant reversible gates hold promise for advancing reversible logic's role in reducing power requirements and enhancing the efficiency of digital designs.

The reversible gates offer a unique advantage in configurability, allowing any input signal to function as the gate's control signal, thereby enabling the attainment of desired functionalities from a single gate. This feature is exemplified in the Double-Feynman gate, which can operate as a configurable inverter or buffer based on different logic inputs applied to the input vectors. Depending on the specific application, this gate can serve as an inverter, XOR gate, or buffer, showcasing its adaptability within various contexts employing reversible gates. In presents a comparative analysis of different reversible gates, elucidating parameters such as the number of input-output vectors (M), parity-preserving capabilities, and the associated cost, measured in terms of the number of basic gates utilized. This table serves as a valuable tool for informed decision making in designing circuits, aiding in the selection of the most suitable reversible gate based on specific design requirements and constraints.

II. LITERATURE REVIEW

2.1 Self-Voting Dual-Modular-Redundancy Circuits for Single Event-Transient Mitigation

Dual-modular-redundancy (DMR) architectures use duplication and self-voting asynchronous circuits to mitigate single event transients (SETs). The area and performance of DMR circuitry is evaluated against conventional triple-modular-redundancy (TMR) logic. Benchmark ASIC circuits designed with DMR logic show a 10–24% area improvement for flip-flop designs, and a 33% improvement for latch designs.

2.2. Reliable On-Chip Systems in the Nano-Era: Lessons Learnt and Future Trends

Reliability concerns due to technology scaling have been a major focus of researchers and designers for several technology nodes. Therefore, many new techniques for enhancing and optimizing reliability have emerged particularly within the last five to ten years. This perspective paper introduces the most prominent reliability concerns from today's points of view and roughly recapitulates the progress in the community so far. The focus of this paper is on perspective trends from the industrial as well as academic points of view that suggest a way for coping with reliability challenges in upcoming technology nodes.

III. METHODOLOGY

FAULT TOLERANCE

A brief description about encoder anddecoder is given in this section used to data encoded usingDouble-Feynman Gate.

3.1 FEYNMAN DOUBLE GATE

The proposed technique may be easily extended to sequential logic, by extending the method proposed in for CED in FSMs based on parity check codes. To make the circuit fault tolerant, the original area-optimized FSM implementation and an output comparator are added to detect faults in the next state and output logic, as illustrated in figure 4. The parity checker and the comparator produce the same control signals of the previous section to diagnose and correct a fault.

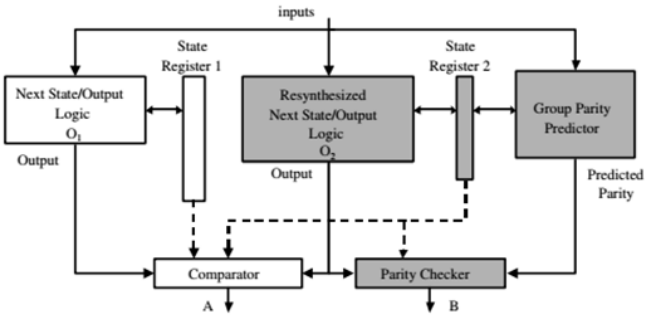

Figure 1: Methodology for Sequential Circuits

The parity check bits are stored in bistable elements to also detect faults in the state register in however, this is not possible in a fault tolerant implementation as the check is performed a cycle later, while the next state logic is evaluating the next state using an erroneous present state. Moreover, although the fault is detected it may not be corrected without performing a re-computation thatwill slow down the circuit operation. If the detection is performed before the next state is stored in the bistable elements then correction can be added in the same cycle, as shown in the left diagram of figure 1. Unfortunately, this will not allow us to correct any faults in the bistable elements. An alternative implementation that resolves this problem is illustrated in the left diagram of figure 4. In this case, we multiplex the correct state based on the value of the control signals A and B so that the correct previous state is used in the calculation of the next state. However, the clock cycle time must be increased to account for the delay it takes to compute A and B. In summary, the proposed method requires three additional hardware components in order to make a combinational or sequential circuit fault tolerant: a replica of the circuit resynthesized based on group parity, a comparator, and the small output selection hardware.

Input vector (IV) and output vector (OV) for 3 × 3 reversible Feynman double gate (F 2G) is defined as follows: IV = (a, b, c) and OV = (a, a ⊕ b, a ⊕ c). Block diagram of F 2G is shown in Fig. 2. Fig. represent the quantum equivalent realization of F 2G.From Fig. 2 we find that it is realized with two 2×2 Ex-OR gate, thus its quantum cost is two (Sec. II-B). According toour design procedure, twelve transistors are required to realizeF 2G reversibly as shown in.

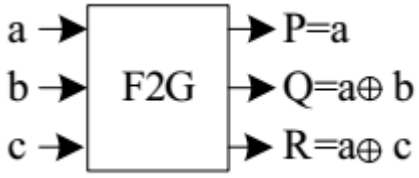

Figure 2:Block diagram of Reversible Feynman double gate

3.2 REVERSIBLE 4:2 ENCODER

The proposed 4:2 Reversible Encoder is shown in figure. It uses three Feynman gates(FG) and one Fredkin gate(FRG).It has four inputs A,B,C,D and two outputs Y1&Y2 and also has two garbage outputs g1&g2.The operation of circuit is given in Table. This proposed 4:2 Encoder has Quantum cost of 8. Reversible logic gates are very interesting topic for research due to less heat dissipation and low power consumption. Reversible logic gates are used in various applications such as CMOS design, Quantum computing, Nanotechnology, Cryptography, Optical computing, DNA computing, Digital signal processing (DSP), Communication computer graphics. Quantum computing is not realized without implementation of reversible logic .Main purposes of designing of reversible logic gates are to decrease quantum cost, garbage output, no. of gates. In this paper we present a proposed design of Encoder using Feynman and Fredkin reversible logic gates. Reversibility in computing implies that information about the computational states should never be lost. The information can be recovered for any earlier stage by computing backwards or uncomputing the results. This is termed as "logically reversibility". Physical reversibility is a process that dissipates no heat in terms of wastage of energy. Power dissipation of reversible circuit, under ideal physical circumstances, is zero. The loss of information is associated with laws of physics describing that one bit of information lost dissipates kTln2 of energy, where k is Boltzmann' constant and T is the temperature of the system.

Reversible computing will also lead to improvement in energy efficiency. Energy efficiency will fundamentally affect the speed of circuits. To increase the portability of devices again, reversible computing is required. Reversible are circuits or gates that have one to one mapping between vectors of inputs and outputs, thus the vector of input states can be always reconstructed from the vector of output states. In reversible logic gates the number of output bits always equals the number of input bits. The fan out of every signal including primary inputs in a reversible gate must be one.

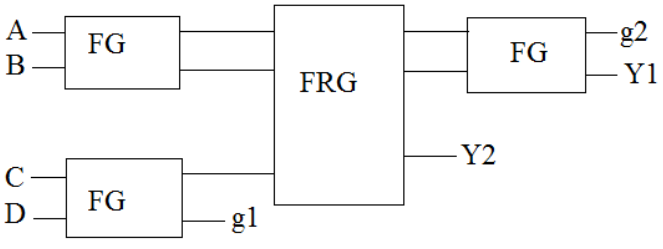

Figure 3: Reversible 4:2 Encoder

The presented different types of reversible Encoder using Feynman and Fredkin gates. In this paper we have calculate Quantum cost of different types of reversible encoders .Quantum cost of 4:2, reversible encoder is 8 respectively. They are used in various fields such low power VLSI design, optical computing, Nanotechnology, Quantum computer, Design of low power arithmetic and data path for digital signal processing (DSP).

3.2 REVERSIBLE DECODER

Decoder performs the reverse operation of encoder which consists 'n' input lines and 2n number of output lines. In decoder only one of the output lines will be 1 (high) and other output lines will be 0 (low) if it is active high and vice versa for active low.In this proposed work, the description of 2:4 decoder designed using 1 Feynman gate (FEYG) and 2 Fredkin gates (FG), also about the [21]Quantum Cost, Garbage Outputs and Constant Inputs of proposed design. The fig shows I0 and I1 are the encoded input given to FG1 at C and A terminals. The B input of FG1 and FG2 are '0', then P of FG1 is AC'=D2 and Q is AC=D3.The Feynman gate output Q will be I1' as the Q of FeyG will be (A⊕1) which is propagated to FG2 at A terminal. Then at P terminal of FG2 (A⊕1) C'=A'C'=D0 and at Q terminal (A⊕1) C=A'C=D1 are observed.

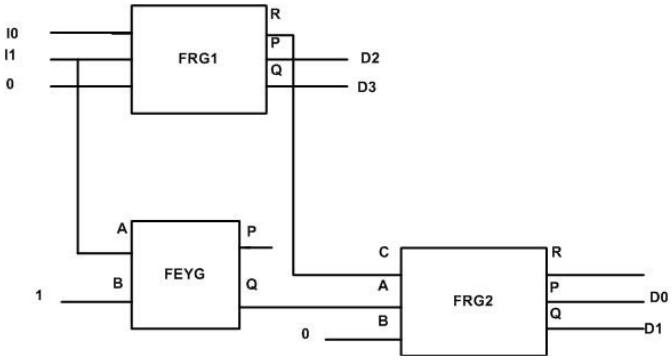

Figure 4: Reversible 2:4 decoder using Fredkin gate

1V. SIMULATION RESULTS

4.1 RTL SCHEMATIC OF 4:2 DECODER

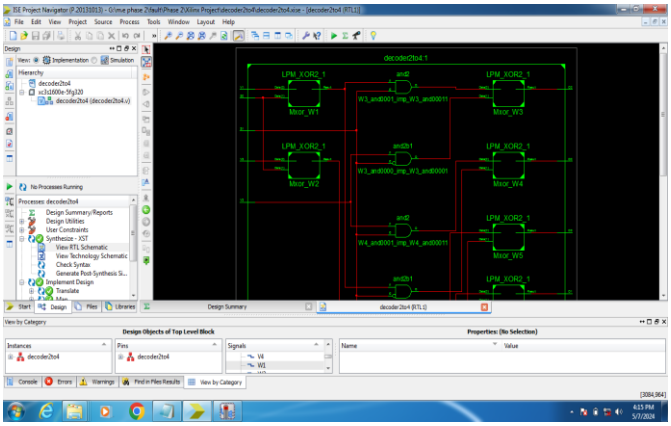

Figure 5: RTL View of 4:2 Decoder

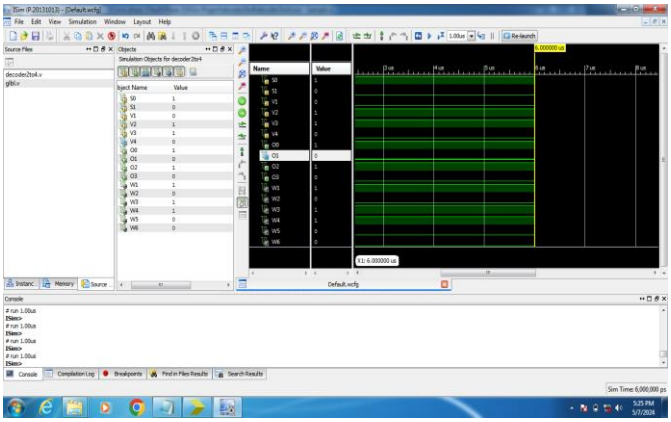

Figure 6: Xilinx Output of 4:2 Decoder

4.2 RTL SCHEMATIC 2:4 ENCODER

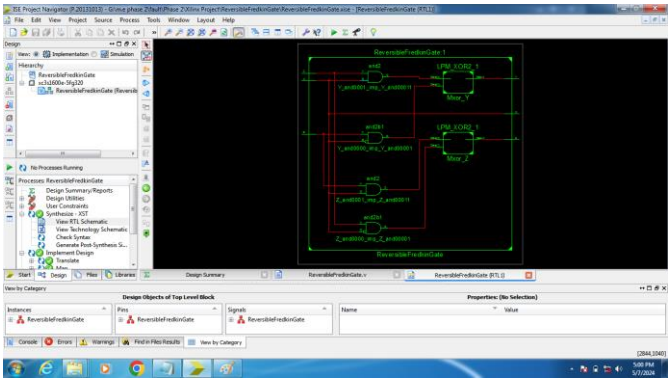

Figure 7: RTL view of 2:4 Encoder

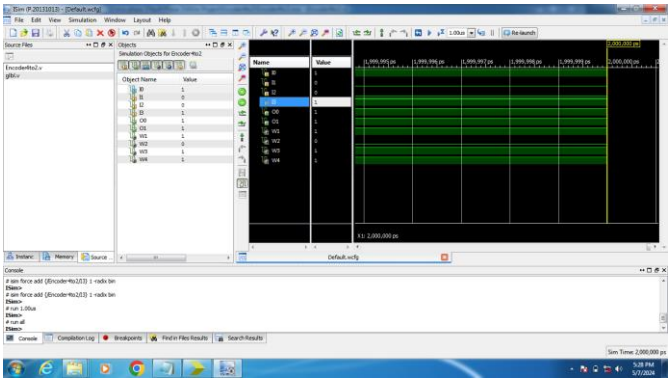

Figure: 6 Xilinx output of 2:4 Encoder

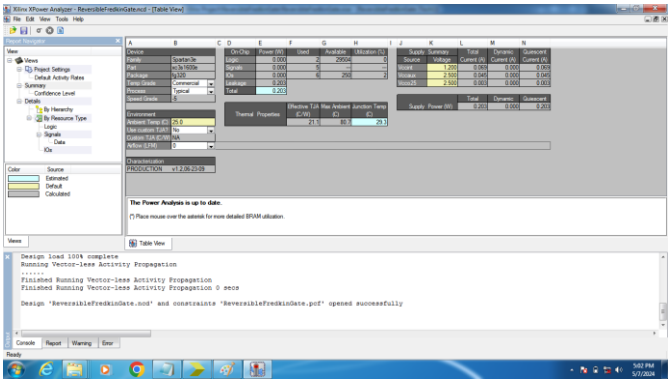

Figure 7: Power Analysis

V. CONCLUSION

This paper presents the design of a ring-oscillator (RO) based physically unclonable function (PUF), which is based on the reversible logic (RL) design and is fault-tolerant. Initially, a reversible gate is selected and checked for fault tolerant output. The fault-tolerant and configurable XOR gate can be used as an inverter and is then used to design the RO by cascading the odd number of these inverters. When compared to the traditional RO-PUF design and other taken into consideration RO-PUF architectures, the whole PUF system yields better results in terms of uniqueness, reliability, uniformity, bit-aliasing, BER, and KER. The proposed design leads to a significant increase in the number of CRPs, thus following up the characteristics of a strong PUF. The use of a modified comparator, which gives 32-bit output instead of the conventional comparator, which gives a 1-bit response, reduces the number of module instantiations. The proposed PUF design is also resistant to well-established ML attacks such as LR, ANN and Random Forest. Therefore, applications requiring strong PUF characteristics, enhanced PUF parameters, decreased hardware utilization, minimized faults, and chip authentication can employ the proposed architecture.

REFERENCES

[1] G. Burke and S. Taft, “Fault tolerant state machine,” in Proceedings of the Military and Aerospace Programmable Logic Devices Workshop, Jet Propulsion Laboratory, Pasadena, CA, 2004.

[2] M. Berg, “A Simplified Approach to Fault Tolerant Sate Machine Design for Single Event Upsets,” Mentor Graphics Users’ Group User2User Conference, 2004.

[3] A. Aviziens, "Fault-Tolerant Systems," in IEEE Transactions on Computers, vol. C-25, no. 12, pp. 1304-1312, Dec. 1976.

[4] L. Rui and K. Yan-jia, "A method of synchronous-feedback based state machine with triple modular redundancy," Proceedings of 2014 IEEE Chinese Guidance, Navigation and Control Conference, Yantai, 2014, pp. 136-139.

[5] S. Radhakrishnan, T. Nirmalraj, S. Ashwin, V. Elamaran and R. K. Karn, "Fault Tolerant Carry Save Adders - A NMR Configuration Approach," 2018 International Conference on Control, Power, Communication and Computing Technologies (ICCPCCT), Kannur, 2018, pp. 210-215.

[6] D. Shah, E. Hung, C. Wolf, S. Bazanski, D. Gisselquist and M. Milanovic, "Yosys+nextpnr: An Open Source Framework from Verilog to Bitstream for Commercial FPGAs," 2019 IEEE 27th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM), 2019, pp. 1-4, doi: 10.1109/FCCM.2019.00010.

[7] B. L. Synthesis, “ABC: A system for sequential synthesis and verification,” Berkeley Logic Synth. Verif.Group, 2011.

[8] A. Mishchenko, S. Chatterjee, R. Brayton, X. Wang, and T. Kam, “Technology mapping with boolean matching, supergates and choices,” Technical Report, UC Berkeley, 2005.

[9] E. M. Sentovich, K. J. Singh, C. Moon, H. Savoj, R. K. Brayton and A. Sangiovanni-Vincentelli, "Sequential circuit design using synthesis and optimization," Proceedings 1992 IEEE International Conference on Computer Design: VLSI in Computers & Processors, 1992, pp. 328-333, doi: 10.1109/ICCD.1992.276282.