An Off-chip Based PUF for Robust Security in FPGA Based IoT Systems

Chella Amala
Electronics & Commu. Engineering,
SRM University AP, India.
subbarao_burra@srmap.edu.in

Burra Subbarao
Electronics & Commu. Engineering
SRM University, AP, India.
amala_chella@srmap.edu.in

Tamoghna Ojha
Mathematics and Computing
IIT (ISM) Dhanbad, India
tamoghna.ojha@gmail.com

Banee Bandana Das
Computer Science and Engineering
SRM University AP, India.
banee.bandana@gmail.com

Saswat Kumar Ram
Electronics & Commu. Engineering
SRM University AP, India.
saswatram01@gmail.com

Saraju P. Mohanty
Computer Science and Engineering
University of North Texas, USA.
saraju.mohanty@unt.edu

***Abstract*—In this paper, a new promising hardware security primitive physically unclonable Function (PUF) is implemented to generate a unique secret key for each SOC Board. Especially FPGA-based, IoT is most widely used for different applications. Several types of PUFs are designed and implemented due to their remarkable performance for hardware security applications. In most of the PUFs ring oscillators are mostly preferred, but these are for limited input. In this context, we proposed a new PUF without increasing the size of the hardware implementation, and power. In this research, we used simple XNOR and XOR gates to increase the number of inputs. Even though it is a weak PUF, generally, weak PUFs is the most preferable for implementation, and by increasing CRPs, one can make a weak PUF as strong. This Arbitrary PUF is implemented on the Artix-7 AC701 Evaluation platform using Xilinx Vivado 2019.1.**

***Index Terms*—FPGA (Field programmable gate array), PUF (Physically Unclonable Function), Hardware security.**

I. Introduction

In general, hardware security is related to preserving systems, devices, and physical components from damage, misuse, and unauthorized access [1], [2]. It is essential for guaranteeing the availability, confidentiality, and integrity of data and services across a range of applications. Hardware devices are vulnerable to a wide range of threats, including malware and firmware exploits, as well as physical attacks including side-channel attacks, fault injections, and tampering [3]. The most crucial component in many application areas is security, which is achieved by providing a random and distinct key for encrypting and decrypting data arriving from sensors to IoT devices. In IoT applications, security and privacy pose the biggest concerns [1], [4].

Secret information forms the foundation of most workable security measures. This confidential data can be used as an input (key) to the encryption/decryption method in conventional cryptography-based solutions. While it is known that digitally stored secret keys in on/off-chip memory can be subject to physical attacks, cryptographic techniques are mathematically secure against attack. The secret key is kept in on-chip non-volatile memory as security tokens like smart cards, but FPGAs store the key in off-chip memory [1], [5]. A PUF is a hardware-based security primitive that leverages the inherent variations in the physical properties of hardware components to generate unique and unpredictable identifiers or keys. PUFs exploit microscopic manufacturing variations in hardware components, such as transistors or memory cells, to create a unique fingerprint for each device. The PUF offers an efficient alternative strong key in on/off-chip memory [6]. A PUF associates a collection of challenges as digital input vectors with an equivalent set of outcomes.

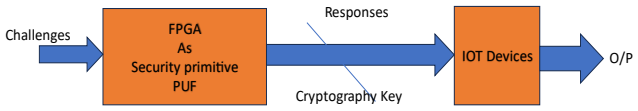

Fig. 1: Securing IoT Devices using FPGA as Security Primitive

The unique property of each PUF instance makes it resistant to cloning or replication attempts. Additionally, the unpredictable response makes it difficult for an attacker to derive the underlying secret key even if they have access to the challenge-response pairs. In cryptography, the secret key is usually kept in a volatile or non-volatile memory region, from which it is recovered through the encryption process. The entire system might collapse if the attackers use side-channel attacks to target the secret key [1]. Strong keys in memory are therefore useless. The output of the PUF system can be a random bit stream. An alternative to utilizing a standard dedicated key for cryptography is to employ this stream of random bits as a secret superstar key [3], [6]–[8]. The concept for securing IoT devices using FPGA as PUF is well depicted in Figure 1.

The PUF is used not only for cryptography, but there are numerous applications in various domains, especially in

hardware systems. The device authentication can be done by providing each unique PUF response that serves as its digital fingerprint [1], [3], [5]. The PUF can be integrated into semiconductor chips, RFID tags, or other physical products to provide anti-counterfeiting measures. The PUF can also be utilized for tamper detection in critical hardware components such as smart cards, secure modules, and IoT devices. PUFs are particularly useful in resource-constrained environments, such as IoT devices or embedded systems, where traditional cryptographic techniques may be impractical due to limited computational resources or memory constraints. PUF-based security solutions offer lightweight and efficient alternatives for ensuring device security and authenticity [1], [9]. A detailed discussion of various PUFs is discussed in subsequent sections of this research paper.

This paper is organized as follows, Section II presents the contribution of this research. Section III represents the Background of the PUF. Section IV analyzes the proposed work and its implementation. Section V is the final result and Section VI concludes the paper with future research directions.

II. Contribution of the Current Paper

A. Problem Addressed

The hardware security threats to modern integrated circuits are increasing day by day. To ensure the security of the devices in IoT, a security mechanism is a must. This paper focuses on the design of PUF as a security primitive and uses FPGA as a platform to secure IoT devices.

B. Proposed Solution

In this paper, we proposed and implemented a novel FPGA-based PUF as a CRO-PUF(configurable logic-based RO-PUF) that mainly increases the CRPs without significant changes in the required hardware resources. Based on a low-cost XRO reconfigurable ring oscillator, PUF is designed for IOT security applications.

C. Significance of the Proposed Solution

In this research, the main objective is to provide a robust PUF with less hardware. We proved the proposed methodology that states, that instead of using only one input, we can increase the size of input and CRPs without much power loss.

III. Related Work

Generally, different types of PUFs are used for cryptographic key generation based on their different physical properties [10]. The SRAM PUF is a memory-based PUF that employs the initial power-up values of SRAM memory cells as PUF responses. Unlike the Silicon PUFs, it does not receive any challenge. So, it could be used to generate the device's signature. PUF is built from two cross-coupled inverters that result in two stable states of the cell. Ideally, two feedback paths should be symmetrical. It should be pointed out that this PUF cannot be implemented in SRAM-based FPGAs because, during configuration, all unused configuration memory cells in FPGAs are initialized to certain values to identify accidental damage like short circuits. [6], [11].

Ring Oscillator PUFs utilize the inherent frequency variations in ring oscillator circuits to generate unique responses. Ring oscillators are made up of an odd number of loop-connected inverters and the propagation delay through the loop determines the oscillation frequency. Manufacturing variations in transistor sizes and parasitic capacitances cause each ring oscillator to have a slightly different frequency, resulting in every PUF instance receiving a different response. When triggered, the frequency at which the ring oscillator functions at rest depends on both the number of stages and the propagation delay between them [3].

The Arbiter PUF exploits race conditions in digital circuits to generate unique response patterns. As the delay difference between two symmetrically built parallel delay lines, this Arbiter PUF (APUF) is the first silicon PUF that extracts random noise in silicon. Although there should be no delay difference between two symmetrically laid-out pathways in theory, in reality, there is a delay difference because of random offset between the two delays caused by unreliable variation in the IC manufacturing process. They typically consist of a set of symmetric digital comparators (arbiter circuits) with slightly mismatched delay paths. Each challenge has a different output since the Arbiter PUF responds differently depending on whether the delay path wins in the race.

The optical PUF might be regarded as the initial PUF that was suggested. Even though its initial proposal was to represent a (cryptography) one-way function physically. The transparent tokens with randomly doped scattering particles are the primary building block of an optical PUF [6]. Optical PUFs produce responses by utilizing a material or structure's special optical qualities. Biometric PUFs use a biological organism's or structure's distinct physical properties to elicit responses [12]. For instance, DNA-based PUFs create unique IDs based on the inherent variances in DNA sequences, whereas biometric PUFs employ characteristics like vein, iris, or fingerprint patterns. Micro-electro-mechanical systems (MEM) PUFs produce distinct responses by exploiting the mechanical characteristics of MEMS components.

In the last decades, several types of PUF have been proposed and implemented. Based on the security of FPGA, ASIC, the PUF are preferred. In both FPGA and ASICs implementation one of the best designs is RO-PUF [1], [13]. In addition, compared to other PUF types, RO-PUF has the easiest implementation, the highest dependability, and interoperability with FPGA programmable blocks [14]. N-ROs, two N-to-1 multiplexers (MUXs), two counters, and one comparator circuit constitute the conventional RO-PUF architecture. An AND gate and an odd number of inverters linked to both MUXs make up each RO. Every counter is increased by the oscillation signal originating from the RO that the MUX has chosen, as each MUX's output serves as an input clock signal to one of the counters. The values of the two counters are compared by the comparator circuit. The RO-PUF challenge is represented by the MUXs' m-bit selection, and the RO-

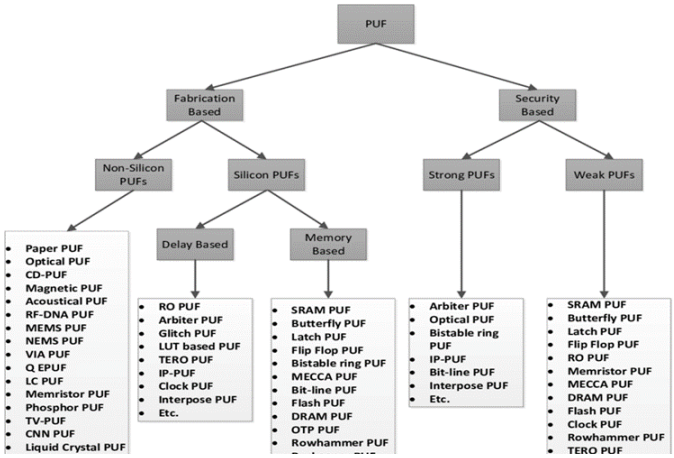

Fig. 2: Classification of PUFs [1], [2]

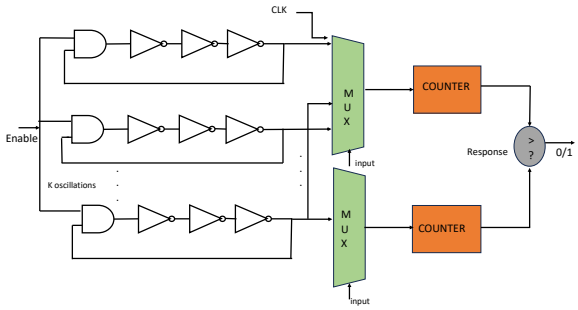

Fig. 3: Structure of a Traditional Ring Oscillator

PUF response is expressed by the comparison operation's output. Figure 3 depicts the conventional RO-PUF's working mechanism. The main disadvantage of the conventional RO-PUF is that it is regarded as a weak PUF since it only offers a few CRPs. Consequently, it would be fantastic if RO-PUF CRPs could be made larger without losing their excellent security features. This can be accomplished by creating a ring oscillator PUF that is programmable.

The classical RO-PUF design consists of n identically laid-out ring ROs. The challenge RO-PUF chooses two different ROs to say R_a and R_b and compare their frequencies to generate a response by equation 1.

$$R = \begin{cases} 1, if f_a > f_b \\ 0, otherwise \end{cases} \quad (1)$$

where f_a and f_b are frequencies of R_a and R_b, respectively. When comparing oscillators, the bias parameter does not show a significant systematic variance among the FPGAs, in contrast to the RO-PUF example. In this method, more independent bits than with the RO-PUF might be extracted.

IV. Proposed Work

The fundamental purpose of CRO-PUFs is to raise the number of CRPs (challenge Response pair) while maintaining a relatively minimum hardware resource need. The concept behind creating a CRO-PUF is to swap out or alter the fundamental inverters of an RO-PUF with a programmable logic part that can handle two or more delay variations. Examining earlier research reveals that there are two primary methods used in the design of a Configurable logic-based (CRO-PUF) and MUX-based RO-PUF.

MMaiti and Schalmont [18] addressed the CRO-PUF and utilized a MUX at each stage of each RO. Thus, each RO consists of two inverters and three 2 to 1 Mux connected to the inputs of each MUX. Thus, without significantly increasing hardware consumption, they were able to build a configurable RO with eight different configurations compared to the traditional RO's one. Several structures motivated by Maiti and Schalmont's MUX-based CRO-PUF have been introduced. A thorough analysis of the current state of the art in related work will be conducted because of the adjustable logic gates that form the foundation of the CRO-PUF presented in this study. The size of the CRPs is increased in the adjustable logic-based RO-PUF by using multiple LUT inputs. The low-cost reconfigurable ring oscillator PUF (XRRO-PUF) for IoT security applications was presented by the authors of [16]. In place of the inverter (oscillation stage) in the conventional architecture, the XRRO-PUF used a 2-input XOR gate as depicted in Figure 4.

Combinations of input values must equal one; ones with an even number of one cannot be used. According to the experimental work, the XRRO-PUF achieved uniqueness and reliability of 48.76%' and 97.72 %', respectively. Wei et al. [16] suggested another adjustable PUF called Transformer PUF, which combines XOR gates and MUXs to create a very adaptable CRO-PUF. The primary goal of the Transformer PUF is to be more resilient to machine learning Attacks. There are four distinct configurations for each inversion stage, however, not all of them can function as an inverter. As such, certain combinations of inputs will fail to produce an oscillation process; this is the same problem that occurs in [5], [8]. However, by making the CRP mapping relationship more

TABLE I: Summary of Related Research Works

Works	Techniques Applied	Important Features
Ding Deng et al. [15]	Configurable RO-PUF	⇒ Designed as Delay configurable unit (DCU) with combinational logic gates. ⇒ Less area and power. ⇒ Uniformity ratio of Response is 50.36% an averagely .
Weiqiang Liu et al. [16]	XRRO PUF	⇒ Designed by XOR-based reconfigurable PUF. ⇒ The Hardware resources requires only 12.5% compare to Ring PUF for 1-bit generation. ⇒ Mostly used for IOT security with uniqueness of 40.67%.
Liang Yao et al. [14]	Configurable XOR RO-PUF	⇒ More no.of challenge response pair(CRP) can be generated by using this PUF. ⇒ Consumes less Resource area 0.05% compare to other circuit .
Y.Cui,Z.wei et al. [17]	Transformer PUF	⇒ Designed by using XOR and Multiplexer. ⇒ It achieves highest hardware efficiency among CRO PUF's. ⇒ It is Resistant to two common machine learning attack Techniques.

complex, this CRO-PUF accomplished its primary objectives and strengthened PUF resilience against machine learning attacks.

XOR (Ring oscillator) based reconfigurable RO PUF is proposed to increase the CRPs as depicted in Figure 4. Generally, RO-PUF needs multiple input LUTs and is used to increase CRPs.This XRO-PUF used 2-input XOR gates instead of an inverter. Each XOR stages primary input connects to the previous gates output, and a configuration signal bit is linked to its second input. If the value of the configuration bit, that is when the S-bit equals 0 the XOR can act as a buffer otherwise it can act as an inverter. When the S-bit value is logic 1. For the XRRO-PUF to serve as a single RO it needs seven XORs and one AND gate. Thus, when the logic value of an odd number of configuration bits is 1, a ring oscillator structure is successfully generated. Otherwise, the configuration bits combination for a 7-stage RO must have 1, 3, 5, or 7 ones. Half of the input combinations are 1 [13]. In Yao et al. [14], a lightweight XOR-based CRO-PUF is

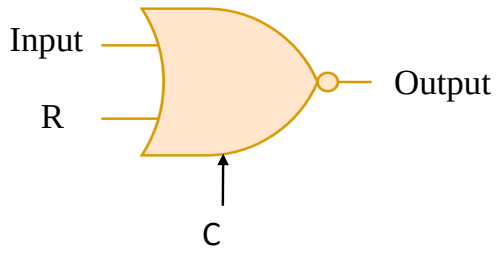

Fig. 4: Structure of the configurable logic PUF

introduced to outperform the conventional RO-PUF in terms of CRP count while utilizing less hardware. Three of the six LUTs' inputs (A_1 through A_6) were employed in the suggested design to create a programmable XOR that can be used in place of the one-input inverter that makes up the ring oscillator [**?**], [7].

Wei et al. [16] suggest another configurable PUF called Transformer PUF, which integrates XOR and MUX gates to present a highly adaptable CRO-PUF. The primary goal of the Transformer PUF is to be more resilient to machine learning assaults. By making the CRP mapping connection more complex, this CRO-PUF was able to achieve its primary objectives and strengthen PUF's durability to machine learning threats. [16], [19].

Figure 5 represents the structure of the proposed PUF. Based on the CLU or configuration input bit value, which can function as an inverter, the XOR-gate in this instance functions as an inverter. The two logic gates that make up the CLU are XNOR and XOR. Regardless of the value of the configuration input bit, it functions as an inverter. It can be constructed on both FPGA and ASICS. This serves as a useful source of entropy that can be realized as ASIC hardware or implemented on FPGA.

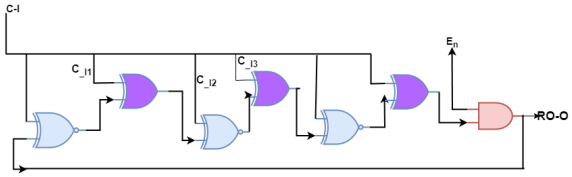

Fig. 5: Structure of Proposed Configurable Ring oscillator (CRO)

The CLU's internal functioning is configured by the value of the C_I input, which is connected to both the logic gates that make up the CLU. The XOR function serves as a buffer and the XNOR gate functions as an inverter when the C_I value is 0. The XOR does the inversion operation and the XNOR serves as a buffer when the C_I input is equal to 1. Only when the enable signal has a logic value (1) does an AND gate output the oscillation result and each RO chain is made up of three CLUs that carry out the oscillation operation. One of the RO's inputs is connected to the first CLU's input, and a configuration input (C_I) bit is attached to the second CLU's input. Each CLU's output is connected to one of the CLUs that follows it. The output of every CLU is linked to one of the CLUs that comes after it. One of the inputs of a two-to-one AND gate is linked to the output of the last CLU. The AND gate's secondary input is linked to the RO_En enable signal. One of the MUX's inputs is connected to the RO input, and

the AND gate's output, which is the output of RO (RO_O) is connected to the other input. The RO enable is low, and the output of the oscillator is zero. No oscillations will occur. To get oscillation, the enable must be active High. This CRO-PUF is connected to the input of the D-Flip flop. The structure of the modified CRO-PUF is shown in Figure 6.

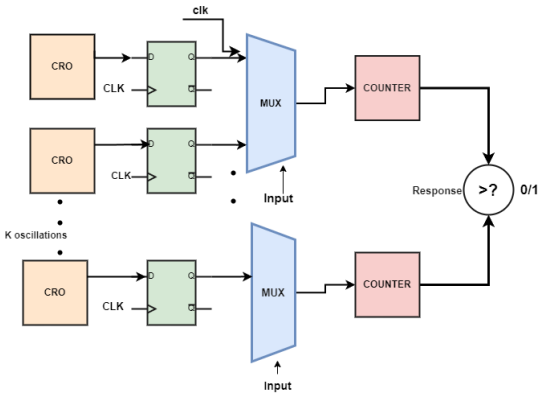

Fig. 6: Architecture of CRO-PUF

In basic terms, it is made up of an array of oscillators, each of which is sampled using a register to generate a binary sequence. It requires a few multiplexers to choose which oscillators to compare. A counter counts the ones in each sequence to determine the bias of each oscillator. Finally, the output is one, using a comparator block if the first oscillator's number of ones is more than the second oscillator's number of ones. The output is 0 else.

V. Experimental Results

To analyze the proposed structure shown in Figure 6. We prefer FPGA, as it is better in terms of reliability, reconfigurability, and high throughput. The FPGA boards have an attractive platform for cryptography applications. The design is implemented on the Artix-7 AC701 Evaluation platform using Xilinx Viv ado 2019.1. To design the proposed architecture in Fig. 6, four CRO-PUF with 4-LUT with 1000Hz clock frequency have been implemented on Artix-7 Ac701. Each PUF contains an array of 8 combinations. Each CRO is compared only to the next CRO (configurable Ring oscillator).

A total 32 comparisons are made for every single comparator. To calculate the precision for each comparison, $10,000$ bits are counted. It takes only 1 second to get results. Figure 7 represents the IP Block design of the proposed circuit in the Vivado environment. The simulation output of this design is represented in Figure 8. Figure 9 and Figure 10 represent the total on-chip power analysis of a single-ring oscillator and a configurable ring oscillator. Although the power consumed by CRO is a little bit greater than RO, at the point of security concern CRO generates more reliable PUF.

The goal of introducing the suggested CLU is to build an RO-PUF having low hardware costs. Apart from its cheap hardware cost, the CRO-PUF designed with the suggested

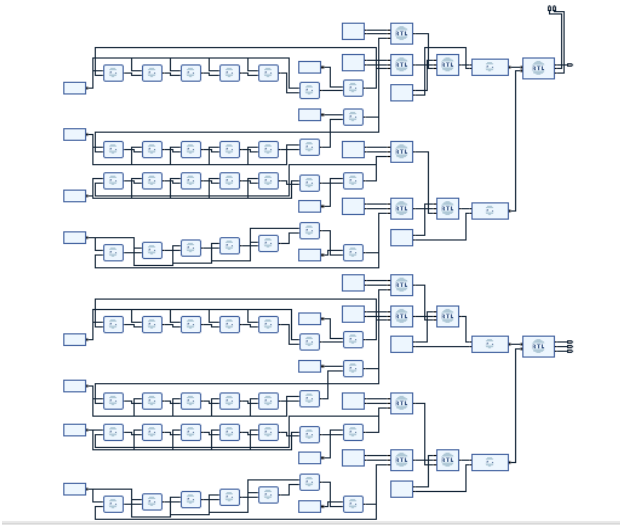

Fig. 7: Implemented Block design of CRO-PUF circuit

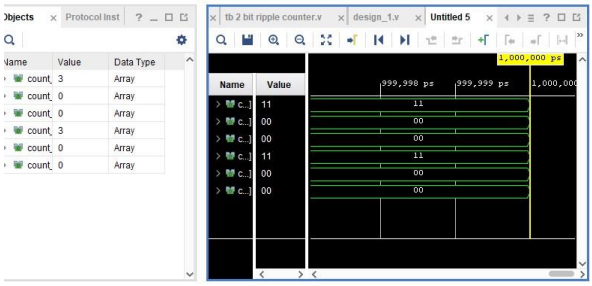

Fig. 8: Simulation Result of CRO-PUF

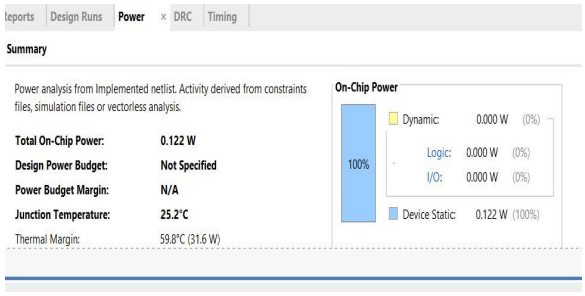

Fig. 9: Power analysis of Basic Ring Oscillator

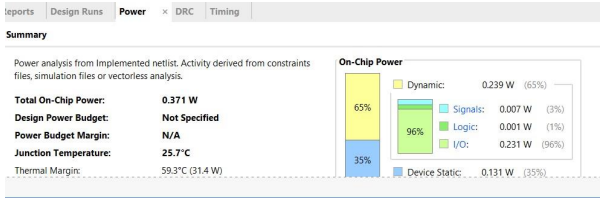

Fig. 10: Total on chip power usage of single CRO-PUF

TABLE II: Comparision with Existing Works

Design	components in a single RO	Design Uniqueness (50%)	Reliability (100%)	Uniformity (50%)	Resources for one CRP
CRO-PUF [15]	11LUTs	49.95%	95.7	49.61	22LUTs+ 2 MUXs
XRRO PUF [20]	8LUTs	48.76	97.72	-	16LUTs+ 2 MUXs
Configurable XOR RO-PUF [14]	8LUTs	48.438	98.24	-	16LUTs+ 2 MUXs
CRO-PUF [18]	7LUTs+ 3 MUXs	47.31	-	-	14LUTs+ 8 MUXs
RR0-PUF [21]	8LUTs+ 8 MUXs	49.97	98.41	-	8LUTs+ 8 MUXs
PRO-PUF [17]	-	44.79	98.01	-	-
This Work ($CRO - PUF_{en}$)	7LUTs	49.99	98.33	49.45	4LUTs+ 8 MUXs

TABLE III: Characterization Table

Parameters	RO PUF	CRO-PUF
Total On-chip Power	0.122W	0.371W
Junction Temperature	$25.2\ ^oC$	$25.7\ ^oC$
Thermal Margin	$59.8\ ^oC(31.6W)$	$59.3\ ^oC(31.4W)$
Dynamic Power	0.00 W	0.239 W
Static Power	0.122 W	0.131 W

CLU has the potential to be used in the development of hardware security applications that are lightweight and can be developed on FPGAs and ASICs. Furthermore, it can be applied in a variety of ways, such as hardware obfuscation approaches where configurable logic can replace an inverter gate with a more complicated defense against adversary attacks. Furthermore, bias resulting from delay differences in ASICs produced by asymmetric net routing can be adjusted and eliminated by using the inputs of the LUTs employed within budget. A comparative analysis with existing state-of-the-art works is presented in Table II. The characterization of the PUFs is presented in Table III.

VI. Conclusion and future research

In this research, we proposed a new PUF designed using a ring oscillator, a D flip-flop, a multiplexer, and counters. Here, a new ring oscillator was designed using two logic gates (XNOR, XOR). This CRO-PUF structure utilizes less hardware than a basic ring oscillator. Furthermore, the size of the challenge-response pair (CRP) size increased multiple times compared to the traditional RO-PUF. To analyze this design, Four PUF, and 4LUT were used, and simulation results were obtained using the Xilinx platform. For every 2 input bit, three combinations are generated with less power consumption. By increasing the number of PUFs, we can get more combinations of outputs. Due to this, the security key size will increase and reliability will also increase. PUF enhances hardware confidence. Developing energy-efficient techniques for the design PUF is a more significant subject for future research.

References

[1] S. K. Ram, S. R. Sahoo, B. B. Das, K. Mahapatra, and S. P. Mohanty, "Eternal-thing: A secure aging-aware solar-energy harvester thing for sustainable iot," *IEEE Transactions on Sustainable Computing*, vol. 6, no. 2, pp. 320–333, 2020.

[2] S. Joshi, S. P. Mohanty, and E. Kougianos, "Everything you wanted to know about pufs," *IEEE Potentials*, vol. 36, no. 6, pp. 38–46, 2017.

[3] S. K. Ram, S. R. Sahoo, B. B. Das, K. Mahapatra, and S. P. Mohanty, "Securing things: A novel cro applicable in puf and recycled ic detection," 2022.

[4] S. C. Moulee, S. Ramesh, and S. K. Ram, "A novel circuit-level method for hardware trojan detection in digital designs," in *2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, vol. 10. IEEE, 2023, pp. 1063–1068.

[5] S. K. Ram, S. R. Sahoo, B. B. Das, K. Mahapatra, and S. P. Mohanty, "Eternal-thing 2.0: Analog-trojan-resilient ripple-less solar harvesting system for sustainable iot," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 19, no. 2, pp. 1–25, 2023.

[6] D. Mukhopadhyay and R. S. Chakraborty, *Hardware security: design, threats, and safeguards*. CRC Press, 2014.

[7] J. R. Wallrabenstein, "Practical and secure iot device authentication using physical unclonable functions," in *2016 IEEE 4th international conference on future internet of things and cloud (FiCloud)*. IEEE, 2016, pp. 99–106.

[8] A. P. Johnson, R. S. Chakraborty, and D. Mukhopadhyay, "A puf-enabled secure architecture for fpga-based iot applications," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 110–122, 2015.

[9] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "Pmsec: Physical unclonable function-based robust and lightweight authentication in the internet of medical things," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 388–397, 2019.

[10] S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "Pufchain: A hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (ioe)," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 8–16, 2020.

[11] S. K. Ram, S. R. Prusty, P. K. Barik, K. Mahapatra, and B. Subudhi, "Fpga implementation of digital controller for active power line conditioner using srf theory," in *2011 10th International Conference on Environment and Electrical Engineering*. IEEE, 2011, pp. 1–5.

[12] B. B. Das, P. Kumar, D. Kar, S. K. Ram, K. S. Babu, and R. K. Mohapatra, "A spatio-temporal model for eeg-based person identification," *Multimedia Tools and Applications*, vol. 78, no. 19, pp. 28 157–28 177, 2019.

[13] S. Khan, A. P. Shah, N. Gupta, S. S. Chouhan, J. G. Pandey, and S. K. Vishvakarma, "An ultra-low power, reconfigurable, aging resilient ro puf for iot applications," *Microelectronics journal*, vol. 92, p. 104605, 2019.

[14] L. Yao, H. Liang, Z. Huang, C. Jiang, M. Yi, and Y. Lu, "A lightweight configurable xor ro-puf design based on xilinx fpga," in *2021 IEEE 4th International Conference on Electronics Technology (ICET)*. IEEE, 2021, pp. 83–88.

[15] D. Deng, S. Hou, Z. Wang, and Y. Guo, "Configurable ring oscillator puf using hybrid logic gates," *IEEE Access*, vol. 8, pp. 161 427–161 437, 2020.

[16] Z. Wei, Y. Cui, Y. Chen, C. Wang, C. Gu, and W. Liu, "Transformer puf: A highly flexible configurable ro puf based on fpga," in *2020 IEEE Workshop on Signal Processing Systems (SiPS)*. IEEE, 2020, pp. 1–6.

[17] Y. Cui, Y. Chen, C. Wang, C. Gu, M. O'Neill, and W. Liu, "Programmable ring oscillator puf based on switch matrix," in *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2020, pp. 1–4.

[18] A. Maiti and P. Schaumont, "Improved ring oscillator puf: An fpga-friendly secure primitive," *Journal of cryptology*, vol. 24, pp. 375–397, 2011.

[19] H. Kareem and D. Dunaev, "Towards performance optimization of ring oscillator puf using xilinx fpga," in *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE, 2022, pp. 1–6.

[20] W. Liu, L. Zhang, Z. Zhang, C. Gu, C. Wang, M. O'neill, and F. Lombardi, "Xor-based low-cost reconfigurable pufs for iot security," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 18, no. 3, pp. 1–21, 2019.

[21] Y. Cui, C. Wang, W. Liu, Y. Yu, M. O'Neill, and F. Lombardi, "Low-cost configurable ring oscillator puf with improved uniqueness," in *2016 IEEE International symposium on circuits and systems (ISCAS)*. IEEE, 2016, pp. 558–561.