Implementation and Analysis of PUF Architectures for Enhanced Security

Sangeeta Singh(✉), Azmath Noorain, G. Sanjeeva Reddy, and Srimanthula Manish Goud

Department of ECE, Vardhaman College of Engineering, Hyderabad, Telangana, India
sangeethasingh@vardhaman.org

Abstract. Physically Unclonable Functions (PUFs) [Coined in 2001 and 2002] are innovative physical security objects that produce unclonable measurements of physical objects. It acts as an equivalent to the biometrics of human being as it can securely generate and store secrets, PUFs allow advancements in the physical implementation of an information security system. To implement multiple applications, various PUFs were invented using different technologies. Thus, this paper compares and summarizes the characteristics of a set of PUFs using CMOS VLSI technology. The PUF architectures namely RO PUF, CRO PUF, and TERO PUF were designed using Cadence Virtuoso 45 nm technology. It was observed that, when all the constraint parameters were kept the same, according to the implemented sequence, there was a decrease in the usage of memory by 10%. While comparing CRO from RO there is a decrease of 82% in power and 51% in delay, for CRO to TERO there is a 19% decrease in power and a 49% increase in delay as there is a decrease in the number of used transistors.

Keywords: Physically unclonable functions (PUFs) · RO PUF · CRO PUF · TERO PUF

1 Introduction

In an increasingly interconnected world that relies heavily on electronics, security is paramount. Thus, to protect these large environmental data electronics rely on cryptography. But, not that secure. For this reason, physically unclonable functions (PUFs) [1–3] have emerged as hardware security techniques as they offer improved cryptography, anti-counterfeiting on ICs, and many more properties. Since the invention of PUFs, multiple applications, of various PUFs were invented using various technologies. But there was never a clear understanding and differentiation between those types. Their advantages and disadvantages have the same base technology.

This research focuses on examining the wide range of PUF designs [4, 5] to give readers a thorough grasp of their guiding ideas, practical applications, and implementation issues [6].

This research examines PUF designs, their implementation, and their effectiveness in enhancing security across a variety of applications [7]. The possible benefits and

X. Cheng (Ed): BROADNETS 2024, LNICST 601, pp. 231–240, 2025.
https://doi.org/10.1007/978-3-031-81168-5_21

deployment-related drawbacks of PUFs by comparing different PUF designs and their respective security features have been identified [8].

The objectives that are to be covered in this paper are as follows:

- Analyzing characteristics of a set of Delay PUFs.
- Implementing them on CMOS 45 nm technology.
- Doing their Performance and Comparative analysis.
- PUFs Included are:

1. Ring Oscillator PUF (RO PUF)
2. Configurable RO PUF (CRO PUF)
3. TERO PUF

The remainder of this work is organized as follows:

In literature survey, a review of PUF taxonomies is presented. The architectures of each implemented PUF along with their requirements, specifications, stages, and functionalities are discussed in design and implementation. The results of the implemented schematic diagrams are presented. Also, a comparison of power analysis of various PUFs and other parameters is done.

2 Literature Survey

A literature survey on PUF (Physical Unclonable Function) cells reveals a wide range of research and developments in this area. In the literature, the existing surveys have focused on presenting a taxonomy based on PUF architectures, their limitations, requirements, challenges, and different properties.

The article [9] presents a survey of the current state of threat in FPGA-based Physical Unclonable Function (PUF) designs and their performance. Then a detailed performance evaluation result for several FPGA-based PUF designs and their comparisons. It also covers four everyday application situations with real-world examples of FPGA-based implementations, known attacks on FPGA-based PUFs, and their defenses. Adapted PUF: Arbiter PUF, RO PUF, TERO PUF, Anderson PUF, Pseudo-LFSRPUF, HELP PUF, and Logically Reconfigurable PUF, SRAM PUF, Butterfly PUF, Flip-Flop PUF, and RS Latch-based PUF.

While surveying the paper [10] it was observed that it provides a complete organizational scheme for the suggested concepts for PUFs. The main aim of this paper is to form relationships between PUF technologies that previously had not been linked and look toward novel forms of PUF using physical principles that have yet to be exploited. To achieve this, they have considered the physical mechanisms and operations of different PUFs. As a result, they distinguished the different PUFs according to their respective properties and gave different schemas according to their respective functions.

The paper [11] describes the use of physically unclonable functions (PUFs) in low-cost authentication and key generation applications. At first, it advantages of using PUFs over the conventional secure nonvolatile memories. Then it defines the two primary PUF types which are the strong PUFs and the weak PUFs. It describes their implementations and their use for low-cost authentication. After this, the paper covers both attacks and protocols to address errors. Finally, this paper reviews several concepts in PUF technologies such as public model PUFs and new PUF implementation technologies.

3 Design and Implementation

The basic elements were implemented on the cadence virtuoso tool in the LINUX environment using 45 nm technology and were verified by their transient response.

3.1 RO PUF

A Ring Oscillator PUF is a security primitive and hardware-based method used to generate unique, random, and unpredictable identifiers or keys within integrated circuits [12]. A ring oscillator is a device composed of an odd number of NOT gates in a ring, whose output oscillates between two voltage levels, representing true and false. The NOT gates, or inverters are attached in a chain and the output of the last inverter is fed back into the first one.

RO PUF is an unstable PUF. A group of RO PUFs is connected to the multiplexer, followed by a counter then with a comparator. The RO PUF implemented has two inputs of the different pulse namely Enable and the selected line i.e. N-bit Challenge. The exact constraint values that are used in the making of PUF are provided in Table 1. RO consists of an odd number of inverters. Thus, we have taken a combination of 4 Ring Oscillators each having 5 stages of inverters. That implies a total of 20 inverters were taken. Along with inverters for each stage, one NAND gate is provided. Then we combined a combination of two ROs and attached them to the 2:1 Multiplexers which were provided with an N-bit challenge. Now two 4-bit counters using JK Flip Flop were taken and each MUX was attached to one counter respectively.

The output of the upper counter and the negation of the Lower counter were given to an AND gate. This block can act as a comparator. The comparator compares and gives the bit response. It has one output and the output response must be a clock response which changes its value after one cycle of the Enable input. These all were implemented on the cadence virtuoso tool in the LINUX environment using 45 nm technology.

Obstruction: Here, the main obstacle was the successive inverters. As there are successive inverters the output quality with the increasing of each stage was degrading. Resulting noise at the last stage of each ring oscillator. Thus, degrading the output performance.

Overcoming Obstacle: To overcome this obstacle, we adopted the concept of "Sizing in inverter chain" That is, we changed the size (increased to lambda times) of the transistors of the inverter at each stage. With the help of this concept, the drawback to the process was solved. Below Fig. 1 is the circuit diagram of the Ring Oscillator PUF. It is taken from the Internet.

Below Table 1 provides the constraint values that are used for designing RO PUF in Cadence Tool. The DC voltage was taken as Vdc = 5 volts.

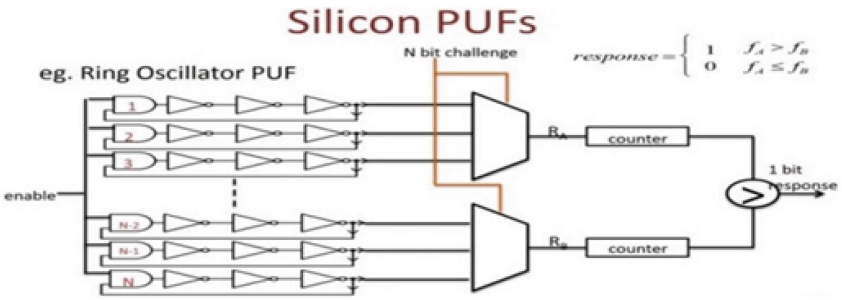

Fig. 1. Circuit Diagram of RO PUF

Table 1. Constraint values of RO PUF

Inputs	V1	V2	Period	Pulse Width	Pulse Type
Enable	1V	0V	40ns	20ns	vpulse
N-bit	1V	0V	20ns	10ns	vpulse

3.2 CRO PUF

A Configurable Ring Oscillator PUF is an advanced hardware security primitive that harnesses the inherent variations in manufacturing processes to generate unique and unpredictable identifiers or cryptographic keys [13]. It is a variation of the traditional ring oscillator PUF (ROPUF) concept. CRO-PUFs are versatile and allow for optimization in terms of performance, reliability, and security. The CRO PUF is more efficient in the matter of component usage and space when compared to the RO PUF.

The CRO is an alternative to the RO PUF. Here the multiple rings are replaced with two rings and each delay stage has two delay elements along with a multiplexer for selection in between them. When compared to RO PUF the CRO PUF uses less number of transistors. The CRO PUF implemented has four inputs of which one is Enable. The other 3 are externally selected lines for the Multiplexers of different periods namely C1, C2, and C3.

Here, we have taken 3 stages of inverters. That implies a total of 6 inverters were taken. As before each stage a multiplexer is required, a total of three 2:1 Multiplexers were used. Along with inverters and MUXs one AND gate was taken. Here, we have given the largest period for C1 and then C2 and the least for C3. The exact constraint values that are used in the making of PUF are provided in Table 2.

It has one output and the output response must be a clock response which changes its value after one cycle of the largest period input. Thus, at the output, the pulse was changing after completion of 1 total cycle of C1. To check functionality, at first, we provided enable as "LOW" and removed feedback then gave random inputs for AND gate to get the output pulse as "LOW". And it was verified. After verifying, we again gave the feedback to proceed further. These all were implemented on the cadence virtuoso tool in the LINUX environment using 45 nm technology. Below Fig. 2 is the circuit

Table 2. Constraint values of CRO PUF

Inputs	V1	V2	Period	Pulse Width	Pulse Type
Enable	1V	0V	20ns	10ns	vpulse
C1	1V	0V	40ns	20ns	vpulse
C2	1V	0V	20ns	10ns	vpulse
C3	1V	0V	10ns	5ns	vpulse

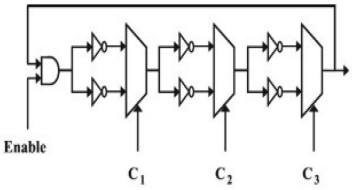

Fig. 2. Circuit Diagram of CRO PUF from existing technique [13]

diagram of the Configurable Ring Oscillator PUF. It is taken from [1]. Table 2 provides the constraint values that are used for designing CRO PUF in Cadence Tool. The DC voltage was taken as Vdc = 5 volts.

3.3 TERO PUF

A True Random Number Generator PUF (TRNG) is based on Twin Electron Ring Oscillators (TERO-PUF) and is an innovative approach for generating random numbers using the inherent quantum mechanical properties of electronic ring oscillators [14, 15]. The TERO PUF is alike the RO PUF, but it uses TERO cells. They have two states: "a transient oscillating state" and "a stable state". The transient stage is also known as an unstable state.

The TERO PUF implemented has two inputs of the same pulse and other parameters. The exact constraint values that are used in the making of PUF are provided in Table 3. This PUF consists of two cross-linked bi-stable ring oscillator chains as shown in Fig. 3.

Here, we have taken three stages of inverters. That implies a total of 6 inverters were taken. Along with inverters one NAND and one AND gate was taken. The top 3 inverters are considered as feed-forward inverters. Whereas, the bottom 3 inverters act as feedback inverters.

It has one output and the output response must be a clock response which changes its value after one cycle of input. These all were implemented on the cadence virtuoso tool in the LINUX environment using 45 nm technology. The Fig. 3 is the circuit diagram of the Transient Effect Ring Oscillator PUF. Table 3 provides the constraint values that are used for designing TERO PUF in Cadence Tool. The DC voltage was taken as Vdc = 5 volts.

Table 3. Constraint values of TERO PUF

Inputs	V1	V2	Period	Pulse Width	Pulse Type
A	1V	0V	40ns	20ns	vpulse
B	1V	0V	40ns	20ns	vpulse

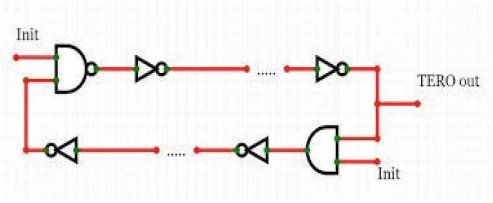

Fig. 3. Circuit Diagram of TERO PUF

4 Results and Discussions

The transient response of RO PUF, CRO PUF and TERO PUF is depicted in Figures 4, 5 and 6 respectively.

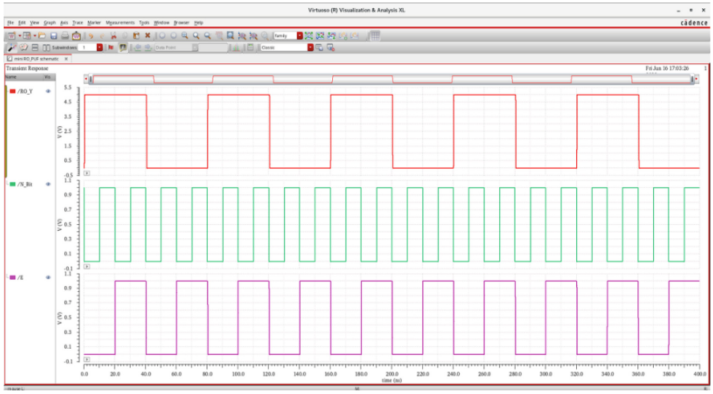

Fig. 4. Transient Response of RO PUF

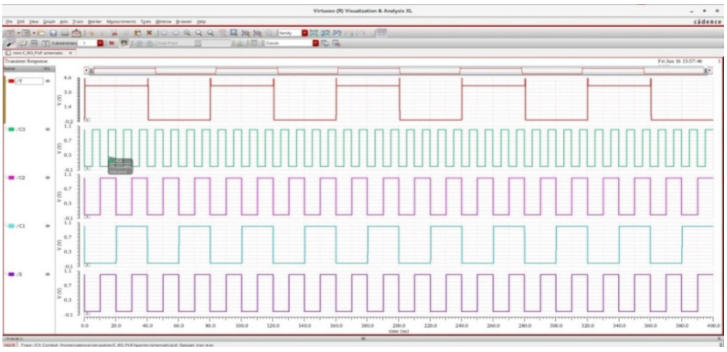

Fig. 5. Transient Response of CRO PUF

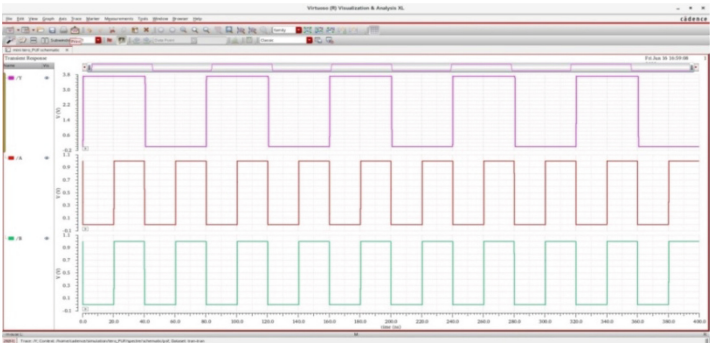

Fig. 6. Transient Response of TERO PUF

4.1 Power Calculations of RO PUF

In Table 4, the power analysis of RO PUF is presented. The parameter Y is the total power accumulated at the end of the PUF. The inverter in the last column and the last row has the highest power among others as it is the inverter just before the output.

Table 4. RO-PUF Power Calculations

INSTANCE	POWER(W)	INSTANCE(W)	POWER	INSTANCE	POWER(W)
Y	104.2 x 10^ -3	Inverter	340.7 x 10^ -6	Inverter	358.7 x 10^ -6
NAND	610.9 x 10^ -6	Inverter	391.4 x 10^ -6	Inverter	340.7 x 10^ -6
NAND	610.9 x 10^ -6	Inverter	340.0 x 10^ -6	Inverter	340.0 x 10^ -6
2X1 MUX	4.385 x 10^ -3	Inverter	391.5 x 10^ -6	Inverter	391.4 x 10^ -6
NAND	610.9 x 10^ -6	Inverter	358.7 x 10^ -6	Inverter	358.7 x 10^ -6
NAND	610.9 x 10^ -6	Inverter	358.7 x 10^ -6	Inverter	340.7 x 10^ -6
2X1 MUX	4.385 x 10^ -3	Inverter	340.7 x 10^ -6	Inverter	391.4 x 10^ -6
4B counter	41.96 x 10^ -3	Inverter	391.4 x 10^ -6	Inverter	340.0 x 10^ -6
4B counter	41.99 x 10^ -3	Inverter	340.0 x 10^ -6	Inverter	391.5 x 10^ -6
AND	1.303 x 10^ -3	Inverter	391.5 x 10^ -6	Inverter	411.1 x 10^ -6

4.2 Power Calculations of CRO PUF

In Table 5, the power analysis of CRO PUF is depicted. The parameter Y, is the total power accumulated at the end of the PUF.TOP-Inverter-1 corresponds to the first inverter from the left and the above one.DOWN-Inverter-1 corresponds to the first inverter from the left and the below one. When compared to RO PUF it gives less power consumption.

Table 5. CRO-PUF Power Calculations

INSTANCE	POWER	INSTANCE	POWER
Y	19.25 x 10^-3	TOP-Inverter-2	385.1 x 10^ -6
2X1 MUX	5.174 x 10^ -3	TOP-Inverter-3	385.1 x 10^ -6
2X1 MUX	5.174 x 10^ -3	DOWN-Inverter-1	388.5 x 10^ -6
2X1 MUX	5.156 x 10^ -3	DOWN-Inverter-2	388.6 x 10^ -6
AND	1.42 x 10^ -3	DOWN-Inverter-3	388.6 x 10^ -6
TOP-Inverter-1	385.1 x 10^ -6		

4.3 Power Calculation of TERO PUF

Table 6 presents the power analysis of TERO PUF where Y is the total power accumulated at the end of the PUF. Inverters 1, 2, and 3 are the top forward inverters whereas Inverters 4, 5, 6 are below feedback inverters. When compared to the other two PUFs, TERO PUF gives less power dissipation overall as well as individual.

Table 6. TERO-PUF Power Calculations

INSTANCE	POWER	INSTANCE	POWER
Y	15.7 x10^-3	2-AND	3.858 x 10^-3
1-AND	3.858 x 10^-3	Inverter-4	1.772 x 10^-3
Inverter-1	1.772 x 10^-3	Inverter-5	1.772 x 10^-3
Inverter-2	1.772 x 10^-3	Inverter-6	446.4 x10^-6
Inverter-3	446.4 x 10^-3		

4.4 Comparison of Parameters

Table 7 presents the comparative analysis of various parameters of implemented PUFs.

Table 7. Comparison of Parameters

PARAMETERS	RO-PUF	CRO-PUF	TERO-PUF
Technology used	45nm	45nm	45nm
Time/Duration of signal	0 – 400 ns	0 – 400 ns	0 – 400 ns
Max. value of Current (I)	5.004 V	5.003 V	5 V
Max. value of Voltage (V)	42.43 mA	8.607 mA	4.126 mA
Total no. of transient steps	2237	2655	785
Memory used	103 Mbytes	93 Mbytes	84.9 Mbytes
No. of Inverters used	21	6	6
Delay of o/p w.r.t i/p	20.0 x 10^-9	9.992 x 10^ -9	20.19 x 10^ -9
Power of o/p w.r.t i/p	104.2 x 10^ -3	19.25 x 10^-3	15.7 x10^-3
No. of stages used	4-(5)	3	3

5 Conclusions

This paper analyzes the characteristics of a set of Delay PUFs. Three PUFs were chosen: RO PUF, CRO PUF, and TERO PUF. The implementation of these PUFs on CMOS 45 nanometer technology has been observed with all the same constraint parameters. According to the implemented sequence, there is a decrease in the usage of memory upto 10%. For CRO from RO there is a decrease of 82% in power and 51% in delay. The CRO With respect to TERO there is a 19% decrease in power. Therefore, this paper presented a comprehensive survey of the selected silicon PUF designs and their corresponding performances.

References

1. Anchana, U.K., Singh, S., Mogireddy, M., Kadavergu, E.: Design and analysis of physical unclonable function. In: 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India (2023)
2. Anchana, U.K., Mogireddy, M., Kadavergu, E., Singh, S.: Design of PUF based chaotic random number generator. In: 2023 Second International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), Tiruchirappalli, India (2023)
3. Ning, H., Farha, F., Ullah, A., Mao, L.: Physical unclonable function: architectures applications and challenges for dependable security. IET Circuits Devices Syst. **14**(4), 407–424 (2020)
4. El-Hajj, M., Fadlallah, A., Chamoun, M., Serhrouchni, A.: A taxonomy of PUF Schemes with a novel Arbiter-based PUF resisting machine learning attacks. Comput. Netw. **194**, 108133 (2021). ISSN 1389-1286
5. Gebali, F., Mamun, M.: Review of physically unclonable functions (PUFs): structures, models, and algorithms. Sens. Netw. **2** (2021)

6. Suh, G.E., Devadas, S.: Physical unclonable functions for device authentication and secret key generation. In: Proceedings of the 44th ACM/IEEE Design Automation Conference (DAC), pp. 9–14 (2007)
7. Wei, L., Song, C., Liu, Y., Zhang, J., Yuan, F., Xu, Q.: BoardPUF: physical unclonable functions for printed circuit board authentication. In: Proceedings of IEEE/ACM International Conference on Computer-Aided Design (ICCAD), pp. 152–158 (2015)
8. Zhou, K., Liang, H., Jiang, Y., Huang, Z., Jiang, C., Lu, Y.: FPGA-based RO PUF with low overhead and high stability. **55**(9) (2019)
9. Anandakumar, N.N., Hashmi, M.S., Tehranipoor, M.: FPGA-based physical unclonable functions: a comprehensive overview of theory and architectures. Integration **81**, 175–194 (2021). ISSN 0167-9260
10. McGrath, T., Bagci, I.E., Wang, Z.M., Roedig, U., Young, R.J.: A PUF taxonomy. Appl. Phys. Rev. **6**, 11303 (2019). 011303. Bibcode:2019ApPRv...6a1303M
11. Herder, C., Yu, M.-D., Koushanfar, F., Devadas, S.: Physical unclonable functions and applications: a tutorial. Proc. IEEE **102**(8), 1126–1141 (2014)
12. Maiti, A., Casarona, J., McHale, L., Schaumont, P.: A large scale characterization of RO-PUF. In: 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Anaheim, CA, USA, pp. 94–99 (2010)
13. Miskelly, J., Gu, C., Ma, Q., Cui, Y., Liu, W., O'Neill, M.: Modelling attack analysis of configurable ring oscillator (CRO) PUF designs. In: 2018 IEEE 23rd International Conference on Digital Signal Processing (DSP), Shanghai, China, pp. 1–5 (2018)
14. Marchand, C., Bossuet, L., Cherkaoui, A.: Design and characterization of the TERO-PUF on SRAM FPGAs. In: 2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Pittsburgh, PA, USA, pp. 134–139 (2016)
15. Pratihar, K., Chatterjee, U., Alam, M., Chakraborty, R.S., Mukhopadhyay, D.: Birds of the same feather flock together: a dual-mode circuit candidate for strong PUF-TRNG functionalities. IEEE Trans. Comput. **72**(6), 1636–1651 (2023)