A Dissertation

entitled

A Comprehensive Analysis of the Environmental Impact on ROPUFs employed in Hardware Security, and Techniques for Trojan Detection

by

Faris Nafea Alsulami

Submitted to the Graduate Faculty as partial fulfillment of the requirements for the

Doctor of Philosophy Degree in Engineering

Dr. Mohammed Niamat, Committee Chair

Dr. Richard Molyet, Committee Member

Dr. Weiqing Sun, Committee Member

Dr. Ahmad Javaid, Committee Member

Dr. Noor Ahmad Hazari, Committee Member

Dr. Scott Molitor, Interim Dean
College of Graduate Studies

The University of Toledo
December 2022

An Abstract of

A Comprehensive Analysis of the Environmental Impact on ROPUFs employed in Hardware Security, and Techniques for Trojan Detection

by

Faris Nafea Alsulami

Submitted to the Graduate Faculty as partial fulfillment of the requirements for the Doctor of Philosophy Degree in Engineering

The University of Toledo
December 2022

Ever-increasing hardware fabrication costs have compelled the semiconductor industry to utilize the global supply chain by shifting integrated circuit manufacturing overseas. This approach has resulted in several challenges and concerns such as intellectual property (IP) infringement, counterfeiting, reverse engineering, and the introduction of Trojans. Because of the increased demand for integrated circuits (ICs) in different applications, counterfeit circuits and devices can infiltrate crucial infrastructures such as smart grids, military installations, and other critical cyber infrastructures. The usage of counterfeit and compromised devices and chips can cause severe monetary losses and make the security and reliability of the ICs suspect. Physical Unclonable Function (PUF) can ensure the security of ICs by utilizing process manufacturing variations to establish a unique signature and key for the IC chip. These keys have potential use in the generation of secret keys and unique IDs for device authentication.

This research presents a comprehensive analysis of the environmental impact on Ring Oscillator PUFs (ROPUFs) design using ten different Xilinx Artix-7 FPGAs. For a comparative study of their performance metrics; three, five, and seven stage configurations of AND-Inverter ROPUFs are implemented. The performance is evaluated in terms of

uniformity, reliability, bit-aliasing, uniqueness, and randomness. The impacts of temperature variations, voltage variations, and aging are analyzed in depth for these metrics. The results demonstrate that using a lower number of stages in the Ring Oscillator (RO) promises a better security feature. ROs with a lower number of stages generate higher Challenge and Response Pairs (CRPs). The higher number of CRPs leads to enhanced security. Additionally, this work includes an analysis of two simultaneous environmental variation factors; namely, aging and voltage variations, and temperature variations with voltage variations. The results demonstrate that ROPUF performance is sensitive to operating temperature and voltage changes. The impact of aging appears to be minimal at normal operating voltages. However, aging has a considerable impact on ROPUF performance when the operating voltage is low.

In this work, a novel authentication scheme for the Advanced Metering Infrastructure (AMI) of the smart grid is also proposed. The scheme utilizes a combination of ROPUFs for authentication, and blockchain technology for traceability in a Zero Trust Architecture (ZTA) design to maximize the security of the AMI. The proposed design provides security for communications between the utility company and the bi-directional advanced smart meters. The use of ROPUFs rather than typical cryptography limits the effectiveness of physical attacks and the use of Hamming code parity bits over the response bits limits the effectiveness of machine learning attacks. In addition, due to the scheme's use of FPGAs, new design and technology can be retroactively fitted into current smart meters making them future proof. Furthermore, through the implementation of blockchain technology, communications are fully traceable, allowing for ease in investigation and establishing the trustworthiness of the AMI network. Not only the proposed scheme satisfy

the requirements of ZTA, but by making the transaction data on the blockchain available to all nodes, the data becomes immutable and secure.

This research also proposes power consumption and ROPUF frequency-based Trojan detection techniques. For each technique, three different design configurations are analyzed. These configurations include the Trojan-free design (or the golden design), the design with inactive Trojan, and the design with active Trojan. This approach monitors the channel parameters of RO delay paths through power side-channel analysis, and ROPUF frequency-based detection. The proposed technique not only detects the Trojan but also facilitates in determining its location.

This dissertation is dedicated to my loving parents, Nafea Alsulami and Haya Aljlsy

Acknowledgements

First and foremost, I thank God for His never-ending grace, mercy, and provision throughout this Ph.D. journey and for giving me the strength and perseverance to complete the dissertation. I owe a special thanks to my leader and guide, Prof. Mohammed Niamat. His advice had a reflective influence on my professional and intellectual growth during my years in graduate school. Our long conversations with Prof. Niamat were especially rewarding, and his gentleness and liberality have made my years in Toledo particularly pleasant. I would like to thank my committee members Dr. Richard Molyet, Dr. Weiqing Sun, Dr. Ahmad Javaid, and Dr. Noor Ahmad Hazari for being a part of my dissertation committee. I thank all my group members, for their contributions to my research effort.

Many thanks to my brothers Tariq, Prof. Abdulrahman, Abdullah, Hani, and Muath, and my sisters Asma, Saafyh, Dr. Rabah, Dr. Salmah, Dr. Bashayir, Dr. Raghad, and Nada for their everlasting love, undying faith, trust, support, patience, and encouragement. Also, I will not forget my brother-in-law Dr. Nawaf Alsulami for his understanding, endless patience, and encouragement when most required throughout life.

Finally, I am also grateful to my wife Afnan Alharbi, my lovely daughter Aljawharah Alsulami, and my son Battal Alsulami who walked with me step by step to achieve this dream, and we will be together for the entirety of our lives, God willing.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

AMI	Advanced Metering Infrastructure
APUF	Arbiter Physical Unclonable Function
ASIC	Application Specific Integrated Circuits
BPUFs	Butterfly Physical Unclonable Functions
CLB	Configurable Logic Blocks
CLK	Clock
CMOS	Complementary Metal Oxide Semiconductor
CPBPi	Challenges and Parity Bit Pairs
CROPUF	Configurable Ring Oscillator PUF
CRP	Challenge-Response Pair
FPGA	Field Programmable Gate Array
HD	Hamming Distance
HW	Hamming Weight
ICs	Integrated Circuits
I/O	Input/ Output
IP	Intellectual Property
LUT	Look-Up Table
MOSFET	Metal Oxide Semiconductor Field Effect Transistor
MUX	Multiplexer
NAND	NOT AND Logic Gate
NIST	National Institute of Standards and Technology
NOT	Simple Inverter Gate
PUF	Physical Unclonable Function
RO	Ring Oscillator
ROPUF	Ring Oscillator Physical Unclonable Function
sPUFs	Silicon Physical Unclonable Functions
SRAM	Static Random Access Memory

Chapter 1

Introduction

1.1 Hardware-oriented Security in PUF

Hardware Oriented Security and Trust (HOST) is bringing research interests and studies in cybersecurity. HOST played a vital role to bring back trust in integrated circuits and chips with enhanced security in various applications. Hardware based security has enabled protection of sensitive information from hackers and hardware Trojans. Advances and progress in semiconducting devices and chips have eased the electronic computations and communications. Hardware used for various applications has sensitive data and information. Vulnerabilities in system can cause the leaking of data for malicious purposes. Hardware Trojans have affected organizations and government departments such as USA department of military and defense and NSF. Research studies are focusing on hardware security and early detection of Trojans. Moreover, hardware design layout and implementation of various hardware security primitives such as PUFs, are part of the most advance research in hardware security. HOST has been facilitating the security of integrated circuits and chip through hardware architecture and protection from side channel attacks. The research in hardware security involves protection, detection and countermeasures for malicious attacks and Trojans. Hardware testing and characterizations, hardware cyber security and IoTs (Internet of things) are also part of HOST. Similarly, HOST is comprised of some emerging fields of hardware security such as Field Programmable Gate Arrays (FPGAs), System on chip (SoC), hardware obfuscation, IP trust, hardware manufacturing, split manufacturing, integration of 2d and 3d manufacturing technologies, supply chain hardware security, sensor-based hardware, embedded hardware security, hardware architectures, cryptography, and data science security. Supply chain hardware and operations are complicated and require high hardware security to rectify vulnerabilities in operations. FPGA based chips are extensively used in supply chain hardware. It is important to significantly enhance the security of FPGA chips to avoid Trojan attacks that can disrupt the operations. FPGA, with reconfigurable platforms (RCs), are extensively used in various operations and industries. Similarly, the security for such hardware devices and systems is of utmost importance. Applications of FPGA and RCs include defense sector, industrial processes, medical devices, automobiles, aviation, smart grids and IoTs. Remote upgradations of these hardware systems pose extreme threats for the hardware security. Trojan attacks can enable hackers to access these systems remotely by cloning FPGA systems. Cloning FPGA systems can allow access to sensitive information, data, and design layouts for digital systems. This highlights the need of these systems to have high level of cyber security for IP protection. Usually, remote access of cloned FPGA is carried out through upgradation protocols. Cloning is much cheaper than to physically alter the devices and systems. Latest research studies are focusing on the upgradation of security protocols against Trojans [1].

Research studies were able to pinpoint two malicious hardware Trojans in ARM and IBM processors in 2018. These Trojans were used to gain access to secret memory [2,3]. As these adversaries were based on the architecture of chips, they severely affected the performance by patching or unpatching. The following Trojans exposed the vulnerabilities of the system and these Trojans were able to abuse hardware characteristics such as energy management, DRAM density and power distributing networks for these chips and systems [4]. Moreover, with the progress in technologies and economics of chips and integrated circuits, various chip manufacturing is outsourced to third parties that can be unreliable and may introduce Trojans by compromising the security. Currently, components such as commercial off shelf (COTs) and 3PIP are introduced in chips through untrusted third parties. In addition to manufacturing, final characterization and testing for chips and integrated circuits are done offshore as well. It is anticipated that Trojans can easily penetrate during the untrusted manufacturing and testing that can leak some of very sensitive information and important data to hackers [5]. In 2011, Boeing alerted US navy regarding a possible Trojan in a FPGA chip being used in various sensitive hardware in military installations. The specific chip was being used in P-8A aircraft. It was concluded that a third party that was responsible for these chips, made it possible for Trojans to penetrate the hardware and chips. As FPGA are becoming viral for various industrial and military applications, it is important to enhance the security of these systems to avoid any such attacks in future.

The security of chips and integrated circuits is more important than ever. Protecting sensitive systems from malicious attacks is the need of an hour. The security of these devices must be kept in mind during manufacturing, testing, characterization, maintenance, and remote upgradations. New security features are being introduced to effectively integrate the design layout and manufacturing to protect these systems and chips from Trojan attacks [5]. The main goals for HOST are as follows:

- Collaboration of researchers around the world for security of electronics, microarchitecture and systems.
- To work on cutting edge technologies to enhance the hardware security for various important applications.
- To integrate the findings of various public, government, and private organizations with the goal to enhance the existing security measures and shape the future of hardware security to overcome the issues related to Trojans and malicious attacks.
- To train the workforce regarding the system security to counter the potential attacks that can leak sensitive data and information.

Physical unclonable functions (PUFs) are known as the most promising hardware security systems to provide powerful and cost-effective security solutions. Silicon based PUFs are the most implemented systems in HOST research studies. PUFs provide high level of security solutions to various semiconductor integrated circuits and chips including FPGA and ASIC chips. PUFs offer high security and protection against cloning, counterfeiting, and reverse engineering of chips to insert Trojan. Memory based devices are more vulnerable to these malicious attacks. PUFs are memoryless, cost effective and faster to offer great protection against attacks on authentication of devices. PUFs generate a random and unique signature for secret key in authentication process making it impossible for Trojan to penetrate the device. The hardware system security provides a safe and secure environment for the output unit, including the operations of the cryptographic unit, memory, encryption keys and storage of sensitive data, data communication, and planning and control unit. PUFs are being studied for verification, traceability, and certification of hardware systems. Several studies have proposed comprehensive solutions to the attacks that involve common side channels such as energy, electromagnetic radiation, and photon radiation [6]. All silicon-based devices and integrated circuits are sensitive to passive and active physical attack. Attackers can clone a device to mimic the original key. PUFs can resolve these security problems by using a basic manufacturing modification and variation in device to create a hardware-based fingerprint that offers enhanced security [7].

Due to high performance and basic design layout, ring oscillator PUFs (ROPUFs) are considered as one of the most important PUFs to enhance the security for AGIC and FPGA systems. Ring oscillator PUF (ROPUF) creates a unique device fingerprint by relying on delay deviations and variability. These delays are produced by the variability in manufacturing that results in minor differences between two similar pathways, causing one path to be quicker in propagating the signal. The output of a digital delay line is sent back to the input of a RO circuit to form an asynchronous oscillating loop. The delay on multiple similar circuits is random due to variability in manufacturing, that affects the resulting random frequency of the oscillation. The frequency is determined using an edge detector and a digital counter coupled with circuit to the output of ring oscillator [8,9].

1.2 Research Objectives

ROPUF is one of the most researched subjects in hardware security, particularly when it comes to FPGA security. The mass acceptance of ROPUFs as a security feature will only be possible when there is absolutely no distinction between the performance metrics of any two chips at any given time under any environmental conditions. The purpose of this research is to enhance the performance metrics such as uniqueness, reliability, randomness, bit-aliasing, and uniformity so that there is no, or negligible error left between similar designs on similar ICs. Furthermore, this performance variation is subjected to environmental conditions like temperature, supply voltage, and aging. Therefore, it is an additional goal to achieve a uniform response from a single IC under various conditions. In addition to that, a novel technique is proposed in which the collective response of voltage variation and aging, as well as temperature and voltage variations, will be examined. The final objective of this research is to investigate a Trojan detection technique through the use of side-channel power analysis. Time and frequency domain analysis will be performed on the drawn power to extract meaningful information regarding hardware Trojans in FPGAs.

This dissertation is organized into eight main chapters as follows:

Chapter 1: The current chapter presents an introduction, motivation and objective of the proposed research.

Chapter 2: This chapter provides a background and literature review about hardware security and PUFs. It also briefly discusses the application of PUFs, different types of PUFs, PUF security metrics, and classification of hardware Trojans.

Chapter 3: This chapter introduces the design and implementation of the proposed AND inverter ring oscillator PUF (ROPUF). Later in the chapter, we compare the data obtained by the proposed ROPUF to examine the outcomes and compare its performance to the other PUFs.

Chapter 4: This chapter discusses a comparative study of the environmental impact on ring oscillator PUFs, including temperatures, supply voltages as well as aging. A unique analysis combines two simultaneous environmental variation factors, namely; aging and voltage variations, and temperature variations with voltage variations.

Chapter 5: This chapter presents the impact of temperature and voltage variations on different stages of the ROPUF.

Chapter 6: This chapter explains the applications of ROPUF for the proposed novel authentication scheme for the Advanced Metering Infrastructure (AMI) layer of the smart grid. The scheme utilizes a combination of ROPUFs for authentication and blockchain for traceability in a Zero Trust Architecture design to maximize the security of the AMI.

Chapter 7: This chapter analyzes the power consumption and ROPUF frequency-based Trojan detection for three different design configurations. This approach monitors the channel parameters of RO delay paths through power (such as current and voltage) side-channel analysis and ROPUF frequency-based Trojan detection.

Chapter 8: Conclusion the dissertation and suggests the future work.

Chapter 2

Background and Literature Review

2.1 Hardware Security

Trust and hardware securities are emerging fields in modern technology that can provide a secure and safe environment for various embodied devices and systems. Hardware devices such as computer to smart phones are used to transfer important and sensitive data regarding financial and other important details. These devices are prone to different cyber-attacks when information is transferred through untrusted means. Smart devices and high computational power are being employed in a number of fields such as energy, power, industrial, financial, and sensitive government sectors. The security breach of computer devices can severely disrupt these sectors and cause financial losses. Different tools are used to get into, breach and attack these hardware devices. Various research studies with industrial and academic collaboration are trying to overcome these issues of attacks by presenting robust solutions. With each passing day, these hardware devices are becoming more and more complicated and complex. Latest manufacturing units fabricate these devices and ICs offshore for cost reduction. The manufacturing parties and fabrication facilities can be responsible for deliberate introduction of modifications that are known as hardware Trojans [10].

Hardware Trojans are threat to hardware devices such as embodied systems, microprocessors, ASICs, FPGA and other embedded systems. These hardware Trojans have the ability to change the functionality of various physical systems that are working based on silicon chips. Hardware Trojans can leak confidential and sensitive information by penetrating devices through silicon chips. The vulnerabilities and possibility of Trojan attacks during the fabrication of ICs are the possible threats to military infrastructure, security, financial setup and household systems. Trojans can be introduced during hardware modifications to microprocessors, networking systems, micro-controllers, modern digital signal processing systems and ASICs. These Trojans are implemented and integrated in these systems through various modifications of firmware as explained and documented by various government bodies such as senate committee in US, USA taskforce for Defense Science and safety, IEEE, and organization related to semiconductor materials [11].

Trojans can be incorporated into systems through the following means and methods.

- Through third party that is responsible for reverse engineering of components.
- Through design layouts, and different firmware to provide control for system hardware.
- Through cloning of systems where the hackers clone the design layout of systems and sale them for such malicious purposes.
- Through third parties that fabricate different components of original systems may use the designs and layout to incorporate Trojans into the systems.

- Hackers maybe able to gain unauthorized access to these systems bypassing the security measures and firmware.

Hardware Trojans can be inserted into main systems through various supplementary hardware equipment such as keyboards, network cards and mouse. High security defense institutes and government departments must be vigilant to overcome the issue of leaking sensitive information through these Trojans. The stealth nature of these hardware Trojans make it difficult to detect through standard post fabrication tests for fabricated chips and systems [12]. Figure 2-1 shows the simplified form of hardware Trojans that cause various malfunctions in systems [13].

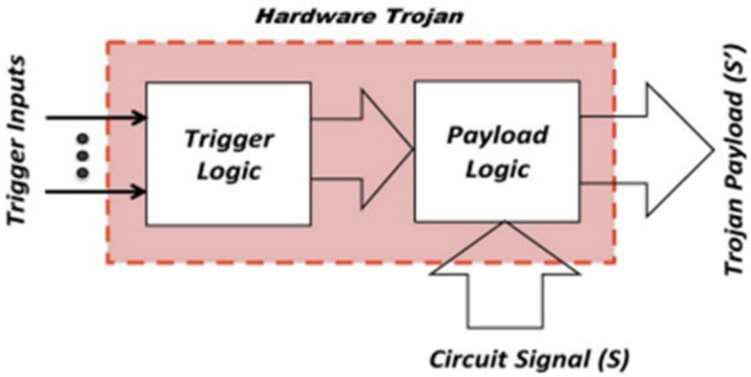


Figure 2-1: Simplified form for Hardware Trojan.

Hardware Trojans are activated and inserted into integrated circuits by trigger mechanisms and the malfunction is caused by payload logic. Such mechanisms effectively act as intruders in the chip and are powerful enough to disrupt the system by leaking information. The two main characteristics for hardware Trojans are malicious nature and difficulty in detection. Latest economic feasibly for fabrication of chips and integrated circuits play a vital role to increase the vulnerability for hardware Trojans. Most of designing for chips and integrated circuits rely on third party manufacturing units. These chips are fabricated in untrusted facilities making it easier for hardware Trojans to penetrate. Latest fabrication of integrated chips involves intellectual properties (IPs) cores that are mostly outsourced through various third parties. Similarly, different design layouts, electronic design tools and testing services are outsourced to third parties. This loosens the grip for design control and make these chips more prone to attacks of hardware Trojans. Figure 2-2 explains the design life cycle for the integrated circuits and possible vulnerabilities for hardware Trojans [13].

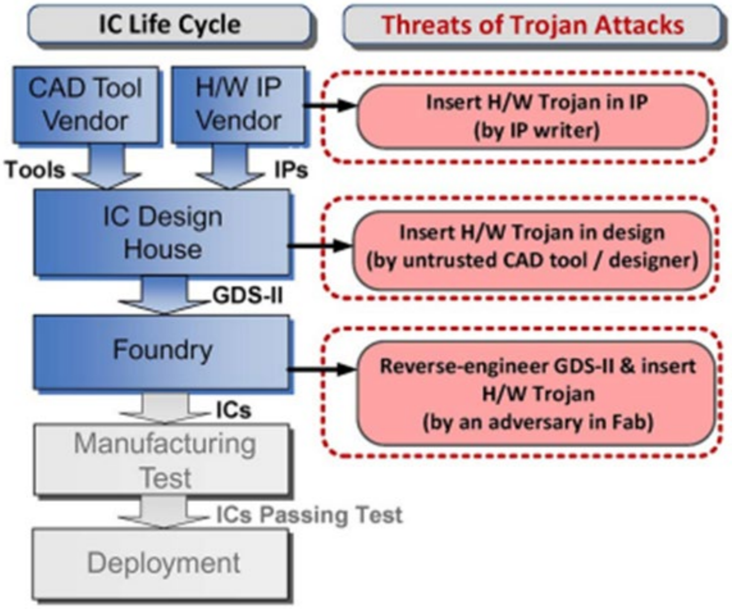

IC Life Cycle
Threats of Trojan Attacks
CAD Tool Vendor
H/W IP Vendor
Insert H/W Trojan in IP (by IP writer)
Tools
IPs
IC Design House
Insert H/W Trojan in design (by untrusted CAD tool / designer)
GDS-II
Foundry
Reverse-engineer GDS-II & insert H/W Trojan (by an adversary in Fab)
ICs
Manufacturing Test
ICs Passing Test
Deployment

Figure 2-2: Life cycle of designing IC and possible intrusion of Hardware Trojans.

Scientists from different countries are analyzing a special kind of hardware Trojans that are certainly impossible to detect through detailed testing. Becker et al. investigated the consequences of deliberately disrupting and disturbing the doping process and introducing slight changes in the structure of dopants for inclusion of hardware Trojan

[14,15]. Alteration of doping mask without changing the concentration of impurities can be used for hardware Trojans. It is believed that such slight alterations cannot even be detected by sophisticated instruments such as scanning and tunnelling electron microscopes. Figure 2-3 shows the difference between design layout of original and Trojan infected device.

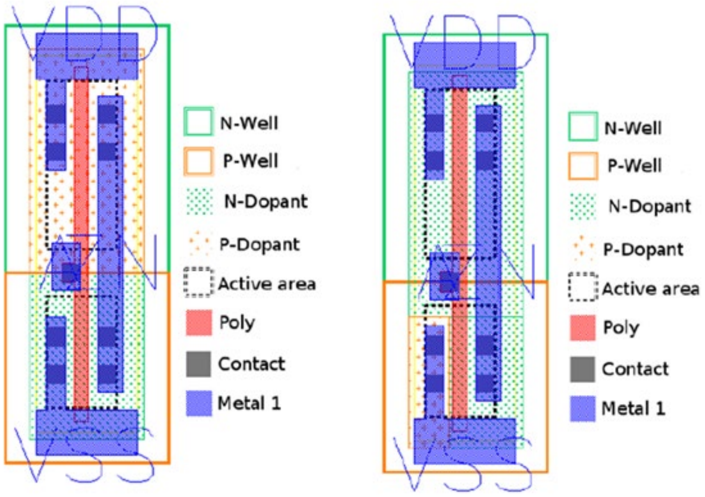


Figure 2-3: Difference between design layout of original and Trojan infected device.

US Department of Defense fears the inclusion of hardware Trojans with the excessive use of Chinese based chips and integrated circuits in US army equipment. It is anticipated that the influx of compromised and Trojan infected chips will increase in future. The attack mechanism on any hardware must be fully understood to overcome these issues. Modification of the random number generator (RNG) module in Intel Ivy Bridge processors is an example of Trojans [16]. The RNG in the Intel Ivy Bridge processor generates 128-bit pseudo-random numbers that consists of two parts: an entropy source and a digital post-processing system. One of the post-processing modules produces a result based on unknown 128-bit random numbers from the entropy source and unknown 128-bit numbers K, that are calculated during processing. The hacker will try to change a certain number of 128 K registers to constant values to reduce the probability of guessing a random number from 1/2128 to 1/2n, where n is the number of unmodified K registers [17]. Figure 2-4 shows Trojan infected area in a digital device.

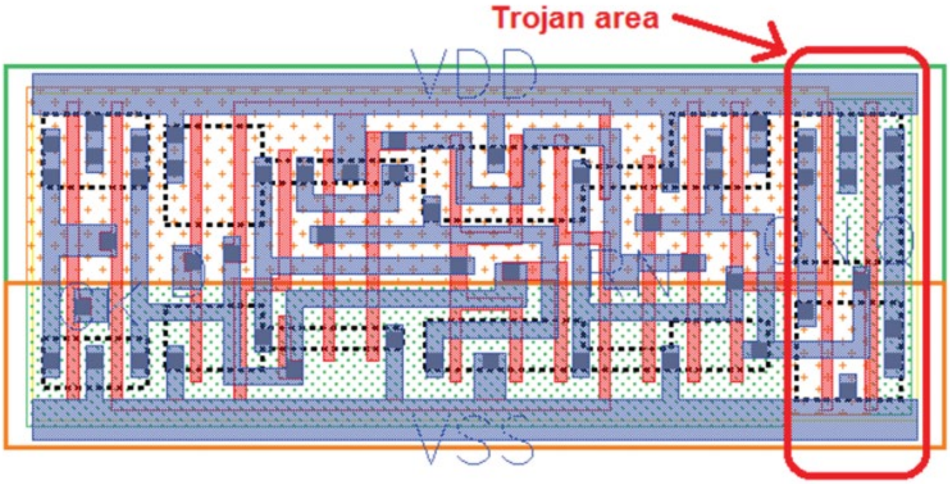


Figure 2-4: The infected area in the integrated circuit device.

It is important to understand the difference between software and hardware based Trojans. Software Trojan is a malware software that gains the access to the code of operating system and can steal the sensitive data once activated. The software Trojan can corrupt data and has ability to even erase it altogether. Software Trojans are comparatively easier to detect and erase with the use anti-Trojan software. Anti-Trojan software effectively monitors new Trojans and remove all existing Trojans in operating systems. While hardware Trojans are inserted into the integrated chips during the fabrication process but these Trojans are very difficult to detect let alone removing them [18]. The difference between hardware and software Trojans is explained in Table 2.1 [13].

Table 2.1: Difference between Hardware and Software Trojan.

Trojan Type	Activation Mechanism	Infection Method	Solution
Hardware	Inserted during manufacturing and is activated as the device starts to operate	Inserted by means of untrusted third-party manufacturing facilities	Impossible to remove after the fabrication of integrated circuit. Circuit replacement is required
Software	Software malware or Trojan is inserted into the code and activated during the execution of code.	Software Trojan can spread through user interaction with infected files and running untrusted file from internet.	Software Trojans can be removed with anti-Trojan software.

It is also important to know the difference between fault and hardware Trojans. Various post fabrication tests are designed to access the functionality and defects of integrated circuits and chips. Physical defects such as path delay and stuck-at-faults are the faults that can arise in these testing methods. Faults can occur due to issues with fabrication process and are of functional state. The imperfections and faults in the manufacturing process are rectified after the detection. Usually, these faults are activated at a specific functional state for a circuit such as stuck-at-fault. It activates once the input values are sensitized to 0. Hardware Trojan activation processes are complex and are dependent on the sequence for internal nodes of integrated circuits. Assembly layout and manufacturing processes can be changed to overcome the fault for future chips while it is almost impossible to detect hardware Trojan [13].

2.2 Physical Unclonable Functions (PUFs)

PUFs are known as devices that are used in the exploitation of randomness for integrated circuits. The randomness in these circuit is inserted during the manufacturing process. PUFs are used in number of applications such as authentication, identification, key generation and anito-counterfeiting [8]. PUFs are used in a different security application due to some of very promising characteristics regarding temper evidence and physical unclonability. PUFs have low implementation cost, simplicity in supply chain and high security than other similar systems such as key storage in NVM, storage in NVM and other secured systems. PUF provides the alternative solution to storage of random secret or encrypted bits in different volatile and non-volatile memories that are prone to attacks by Trojans. PUF works by generation of random bit at the time of evaluation in real time. PUF is considered as robust solution against the hacking attacks. High level of protection is provided by PUF for physical hardware Trojan attacks with the implementation of read proof hardware. Physical attacks can be divided into two categories: non-invasive and invasive attacks. Invasive attacks mean the intrusion of attacker or hacker by physically altering the structure of an integrated circuit or chip or device while non-invasive attack involves no modification of device structure [19]. Both attacks have ability to significantly change the behavior and functioning of device. Change of response is observed after the attack for the same challenge. Authenticity for any product is checked through PUF by measuring a physical property that is converted into a string of bits to verify. To keep PUF safe, the responses are kept inside the device for protection against different attacks [20]. When a PUF system is queried with a specific input (challenge), a quantifiable output (response) is created based on the intrinsic unique physical features of the devices or circuits that comprise the PUF system. As illustrated in Figure 2-5, a PUF can have one or more challenges and responses, which are referred to as challenge-response pair(s) or CRP(s). Ideally, CRP has the robust advantage that each response provides little information about responses from different calls to the same PUF, or even identical calls to dissimilar PUFs [8]. True physical randomness may assure that the relationship between the challenges and replies, or the CRP behavior, is not easily realizable using mathematical functions. As a result, a PUF is more than just a mathematical function; it is a method with input–output functionality. Furthermore, a PUF is not only an abstract idea, but must always be implemented as a tangible object, which is typically a silicon-based material [9].

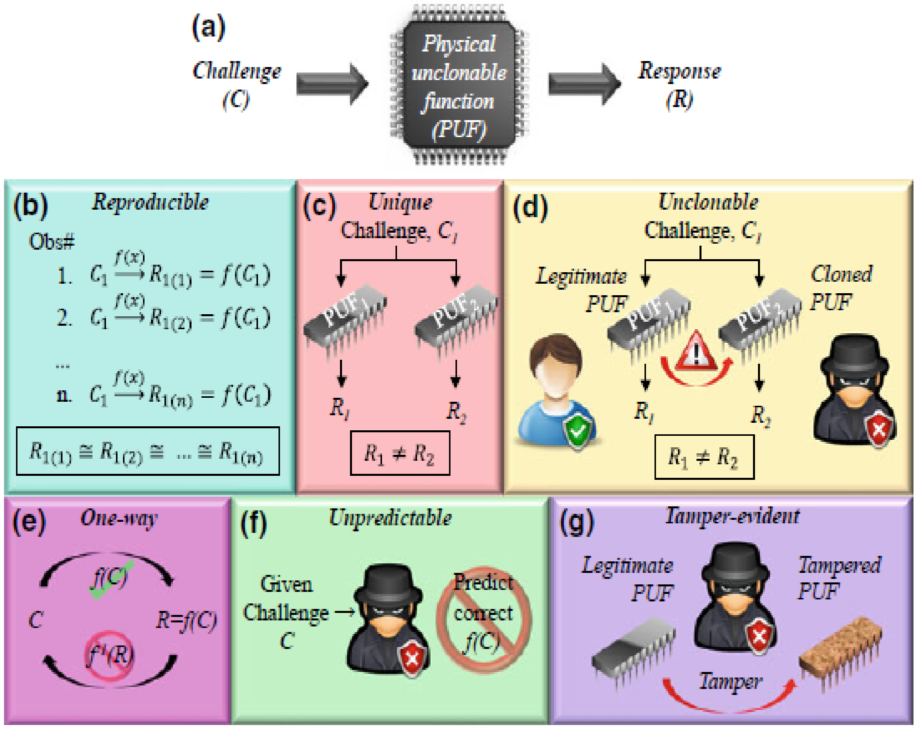


Figure 2-5: Framework of a PUF.

2.2.1 Ring Oscillator PUF

ROPUF is used to measure and quantify smaller random delays based on deviations caused by the variability in manufacturing of these devices. Inverted delay line for outputs and feedback into the input create an asynchronously oscillating loop known as ring oscillator. The frequency in this oscillator is directly proportional to precise delay for delay line and on the randomness variations during manufacturing. The frequency is measured through digital instrumentation such edge detector [21].

The edge detector is known to use the rising edges in ring oscillations while a digital counter measures total edges over a set period. The counter digital component has all the desired measurements and is known as PUF response. The design layout containing the basic blocks for ring oscillator is shown in Figure 2-6 [22].

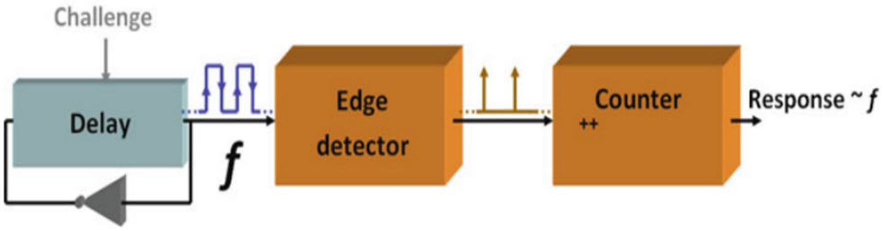


Figure 2-6: Basic blocks in design layout for Ring Oscillator.

The responses in ring oscillators are delayed by different environmental factors that are die temperature during manufacturing and voltage supply. Counter measures are needed to overcome the effect of these factors in ring oscillator. One technique is division of two oscillations leading to a robust and effective response as shown in Figure 2-7 [23].

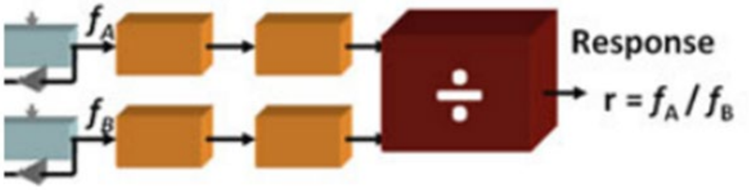


Figure 2-7: Layout of Ring Oscillator with division counter measure and compensation mechanism.

Figure 2-8 shows a typical design of a ROPUF includes a set of ring generators (RO), two multiplexers (MUX), two counters, and comparators. Connection and inverter delay in all ROs are not controllable due to the variations un manufacturing, often resulting in different RO outputs. By choosing two ROs based on PUF input, pulses can be measured over the time range determined by the sensor. For example, if the first shelf has a value greater than the second, the emptying of the pouf will be ‘1’, otherwise, the pouf output is '0'. Ideally, the pouf RO will always produce the same bit value for a given input, but there are bit errors and distortion in the output. Fluctuations in regular processes and ambient noises occur due to voltage and temperature variations that affect the stability of output signal [24]. FPGA-based PUF bit errors arise directly from a specific, frequency-narrowed ROS pair, resulting in unstable measurements in the meters and the inverted output in the comparison.

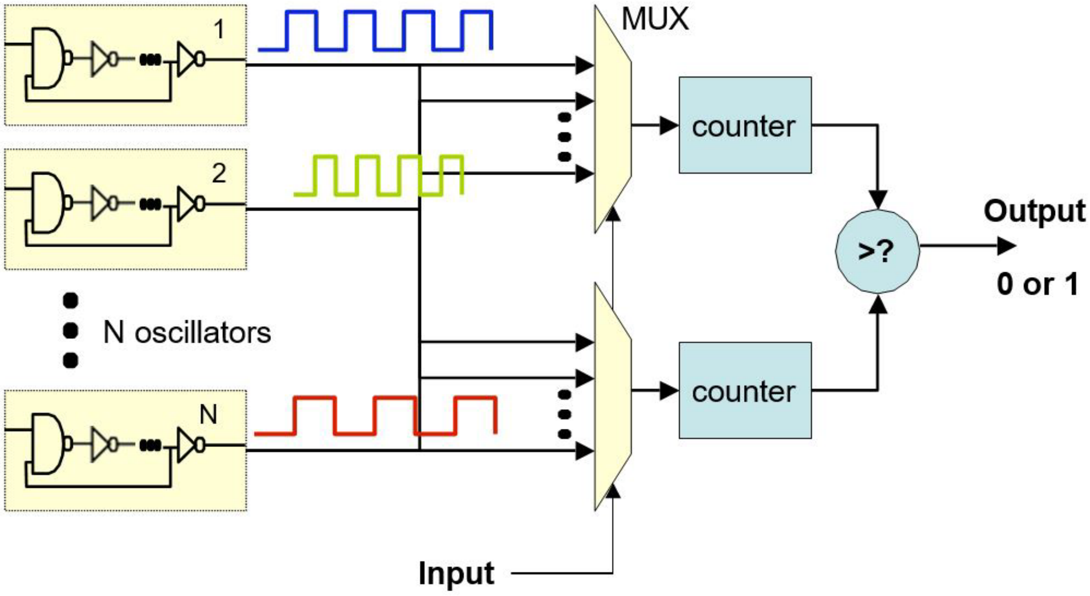


Figure 2-8: Structure of ring oscillator PUF.

2.2.2 Advantage of PUFs

PUFs provide simple, secure and innovative solutions for secret key/code storage and authentication without the implementation of expensive systems such as EEPROM (Electrically erasable programmable read-only memory) [25,26]. PUFs do not store secret keys in digital memory but secret keys are derived from physical characteristics that are linked with integrated circuits. PUFs are various advantages over digital and secure storage systems. These advantages are as follows:

- PUF systems are less energy intensive and do not require state of art cryptographic systems. PUF systems use simple hardware and digital circuits that can be fabricated with ease. These systems are found to consume much less energy than

EEPROM. Moreover, various PUF applications do not require sophisticated cryptographic systems such as key encryption and secure hash algorithms [27].

- PUF systems store secret keys physically into the chips. These chips require being turned on to access those keys that is why any form of Trojan, or hacker attack can only be proceed once the chip is turned on. This property adds another layer of security for PUFs.
- PUF systems do not require continuous, powered-on anti-tamper mechanisms for security. Invasive Trojan attacks and hacking are hard to execute without any modification in physical characteristics of chip that are associated with secret key storage. Therefore, it adds another advantage to PUF systems.
- PUF systems do not require such complex systems for security. Nonvolatile memory-based systems are much expensive to fabricate. EEPROMs need additional masking layers, and RAMs require an external and continuous power source with power back up [28].
- Two PUF chips can never be similar in architecture. A PUF based system and relative integrated circuits are dependent on masking during fabrication. These PUF based circuits have advantage in fabrication variability and are unique in storing secret keys. No two PUF chips can be exactly similar even though the fabrication process is same. It is impossible to fabricate two similar chips even after having all technical design specifications [29].

2.2.3 Important Properties of PUFs

PUFs are based on randomly generated numbers and PUFs need to satisfy various properties depending on the applications and other requirements. The important properties for PUFs are as follows:

- The generated response must be random and unique, no two challenges can have same random number.
- Challenge Response Pair (CRPs) must always be generated in a fraction of time.
- CRPs should be exclusive of PUFs models and should not give information regarding them.
- Implementation of PUF based models should be secure and must have lower attack multiplicity. Low attack multiplicity means if by any means the hackers get to know the challenge response pair at a specific time, they should not be able to do the same with other response pairs.
- The highest security level of challenge response pairs and PUF based model can be achieved through the implementation of strict avalanche conditions (SAC). Bit-flip probability for output should be 0.5 as single bit of input is flipped [6].

2.3 Performance Assessment of PUFs

The performance and quality of PUF systems are assessed through various parameters depending upon the nature of application. PUFs generate challenge-response pairs (CRP) through spatial random variations. Resultant random responses are produced in PUF systems. Systematic spatial variations are caused by the imperfections in fabrication processes that decrease the randomness of PUF systems. Temporal variations are activated during operation phase of PUF, which may be reversible or irreversible. The reversible variations are caused by variations in operating temperature, making challenge response pairs unreliable and noisy in PUF systems. The irreversible variations, also known as aging, impact the reliability of PUF systems [30]. Various types of variabilities and their sub-types are shown in Figure 2-9 [31].

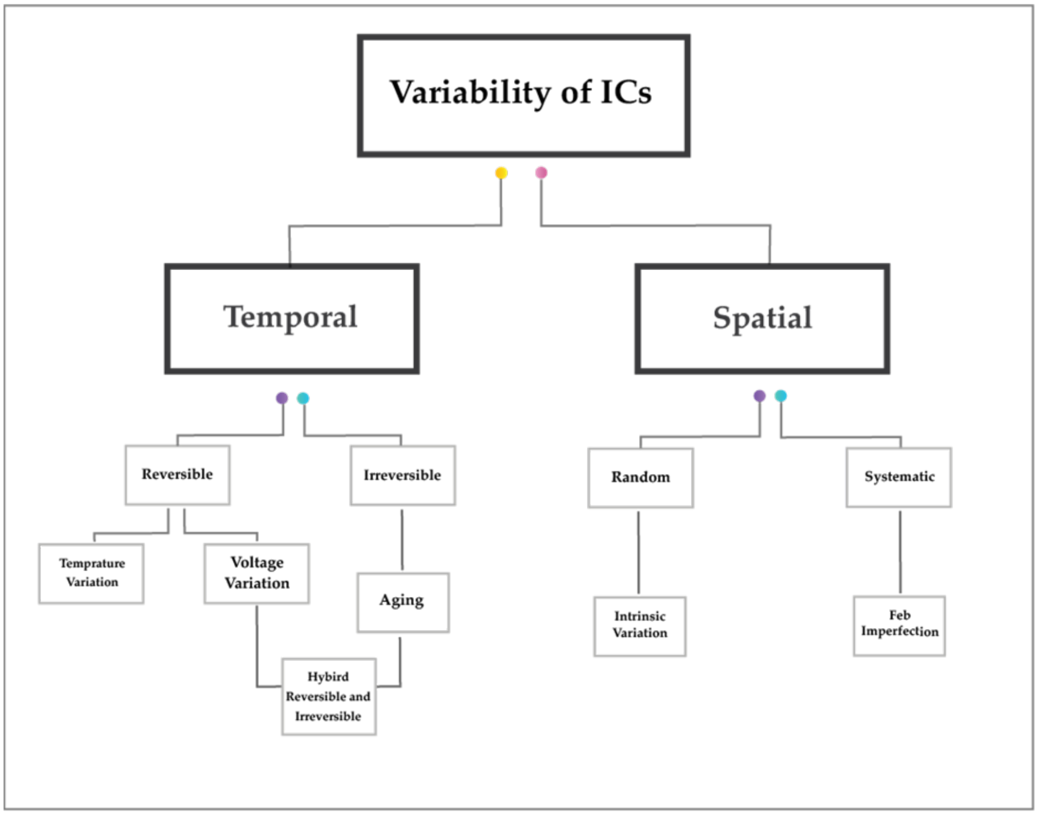


Figure 2-9: Temporal and spatial variability in integrated circuits.

The performance of PUFs is assessed through factors such as uniqueness, steadiness, reliability, randomness, bit-aliasing, uniformity, and correctness as shown in Figure 2-10.

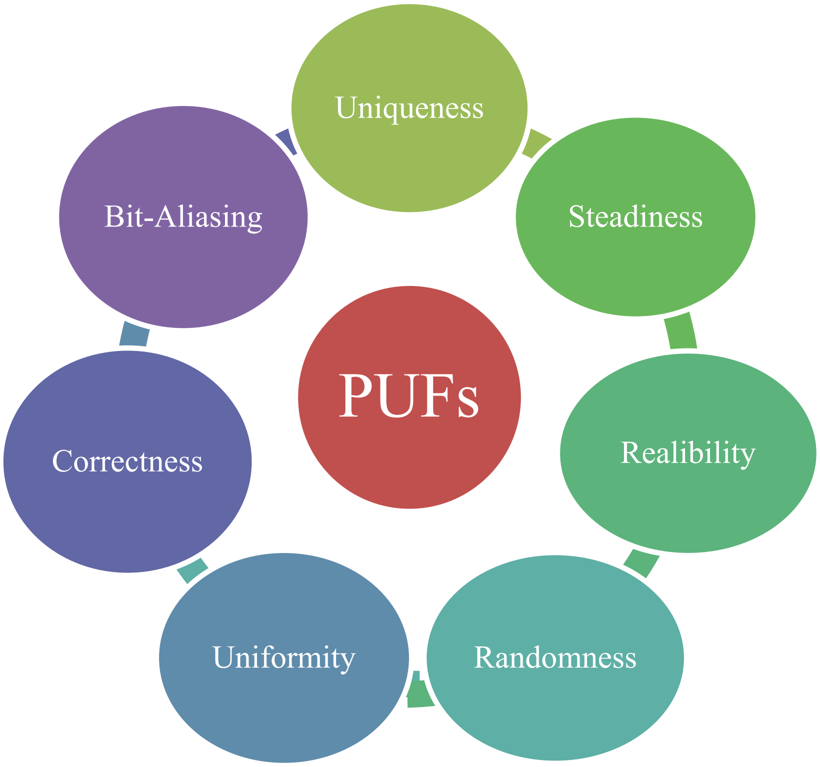


Figure 2-10: Assessment parameters of PUFs.

2.3.1 Uniqueness

Uniqueness quantifies differences for each chip. It shows the process variability in fabrication of integrated chips. Each FPGA chip generates the response vector $R = [r_1, r_2, \cdots, r_n]$ for a challenge vector $C = [C_1, C_2, \cdots, C_m]$. The response matrix for a chip is thus written as follows:

$$\mathrm{R_i} = \begin{bmatrix} \mathrm{R_1} \\ \mathrm{R_2} \\ \vdots \\ \mathrm{R_k} \end{bmatrix} \tag{2-1}$$

The following formula is used to determine the inter-chip uniqueness:

$$Uniqueness = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(R_i, R_j)}{N} \times 100 \qquad (2\text{-}2)$$

Where *i* and *j* are two chips being compared and *N* is the number of response bits generated. R_i and R_j are the response bits from the same challenge *C* for chip *i* and *j*. *HD* is the hamming distance between response bits generated from chip *i* and *j*.

2.3.2 Reliability

PUF reliability assesses the strength of a PUF to replicate the response bit under a variety of settings, and this relates to how efficient a PUF is at reproducing the response bits. The ideal value is 100%, and anything close to that value is considered good. It is a test between different environmental or any other conditions.

$$Reliability = 1 - \frac{1}{K.T.L} \sum_{k=1}^{K} \sum_{t=1}^{T} \sum_{l=1}^{L} r_{n,k,l} \otimes r_{n.k.t.l} \qquad (2\text{-}3)$$

Where $r_{n,k,l}$ is the *l-th* binary bit of the *t-th* sample of the *k-th* FPGA (tested under specific condition). Further, *k* is the index of the ID in the chip, *t* is the index of the sample, *l* is the index of the response bits, and *n* is the index of the chip.

2.3.3 Randomness

The randomness of a PUF is based on the ratio of 1s and 0s in the response bits. The ideal value is 100% and anything close to that value is considered good. The device randomness H_n of a PUF is given by

$$H_n = -log_{2^{max}}(p_n, 1 - p_n) \qquad (2\text{-}4)$$

Where *p_k* is the frequency of 1's in the output results, whose expression is shown in the equation below, where *k* is device number and *$b_{k,t,l}$* is the *i-th* bit response of challenge set on *k-th* device.

$$P_k = \frac{2}{k(k-1)} \sum_{k=1}^{K} \sum_{t=1}^{T} \sum_{i=1}^{L} \frac{HD(R_i, R_j)}{N} \times 100\% \qquad (2\text{-}5)$$

2.3.4 Bit-Aliasing

Bit-aliasing estimates the bias of a response bit across *K* different devices. Bit aliasing estimates the bias of a response bit across different devices. The ideal uniqueness value is 50%, therefore; any uniqueness value near 50% is considered a good value. It can be explained using:

$$(bit - aliasing)_l = \frac{1}{K} \sum_{i=1}^{K} r_{i,l} \ X\ 100\% \qquad (2\text{-}6)$$

Where $r_{i,l}$ is the lth binary bit of *n* bit response

2.3.5 Uniformity

PUF uniformity is the amount of 0s and 1s in a *p*-bit response from a chip *k*. The ideal value for uniformity is 50%; this means that any value around 50% is considered a good value; the closer the value to the 50%, the better the uniformity. This is measured by calculating the intra-chip hamming weight (HW) where *$r_{i,l}$* is the *l*th binary bit.

$$(Uniformity)_k = \frac{1}{p} \sum_{i=1}^{p} r_{i,l} \ X\ 100\% \qquad (2\text{-}7)$$

Where $r_{i,l}$ is the lth binary bit of *n* bit response from a device *n*.

2.3.6 Correctness

Correctness is the measure of accuracy under challenge response pair for various operating conditions. The ideal value for correctness is 100%. The correctness parameter is defined as follows:

$$Correctness = 1 - \frac{2}{K.T.L} \sum_{k=1}^{K} \sum_{t=1}^{T} \sum_{l=1}^{L} \left(r_{n,k,l}\ r_{n,k,l,t}\right) \qquad (2\text{-}8)$$

2.3.7 Other Assessment Factors

Apart from all these performance assessment factors, some other important factors such as cost analysis, design, and power consumption have impact on the performance of the devices. Moreover, false negative and positive rate are used to identify various chips, for performance assessment of PUFs [32].

2.4 Inter and Intra-Hamming Distance

The most important parameter to estimate PUF performance is Hamming distance (HD), that is the total number of different bits in between two outputs. The intra-HD exhibits reproducibility for each chip while the inter-HD shows the uniqueness in between various chips. Inter and intra HD for specific PUF designs are explained as follows:

- Distance between two separate PUFs for any applied problem is known as distance between two responses that results from the challenge that is applied to both PUFs.
- For any problem, the internal distance between two PUF is the distance of two generated responses from any challenge to be applied in a PUF at once.

It is important that both the inter and intra-distance are measured across each pair of response because of the same challenge. Distance measurements may vary depending on the nature and type of PUF. The bit value depends on both the inter and intra distance and is based on the applications and involvement of PUF properties and characteristics. Gaussian distribution can be used through histograms for the calculation and representation of both inter and intra-distance. The mean of inter and intra distance are represented by μ_{inter} and μ_{intra} respectively [33].

2.4.1 Inter-chip Hamming Distance (HD$_{inter}$)

Humming distance between chips measures the uniqueness of PUF. HD$_{inter}$ is used to estimate the difference in responses between two PUF with the identical challenge. The standard HD$_{inter}$ value is 50%. The average values of different PUFs can change significantly from 20% to 50% and the presence of bias depends on these values [34].

2.4.2 Intra-chip Hamming Distance (HD$_{intra}$)

The Intra-chip Hamming Distance is used to measure the difference of particular PUF response when same input is applied. The resilience of a PUF to fluctuating environmental conditions can be measured using Intra-chip Hamming Distance. The generated bits have two phases. The generation process of bit is dependent on normal supply voltage and happens at around 25°C. Bits reproduction is carried out through regeneration with supply voltage (-5% to 5%) and done at 0°C, 25°C and 85°C [35].

During one or more successful regeneration of the bits, the differences can be represented by intra-chip hamming distance and the differences between the bits are the Hamming distances. The average noise in the responses is also represented by HD$_{intra}$. For the intra-chip hamming distance, the ideal value is zero.

2.5 Classification and Types of PUFs

PUFs can be divided based on security analysis as well as fabrication route as shown in Figure 2.11. Security is utmost requirement during the fabrication of integrated chips. PUFs are required to bear various attacks including semi-invasive and invasive based Trojan attacks. PUFs are classified based on security and fabrication processes as explained in the Figure 2.11.

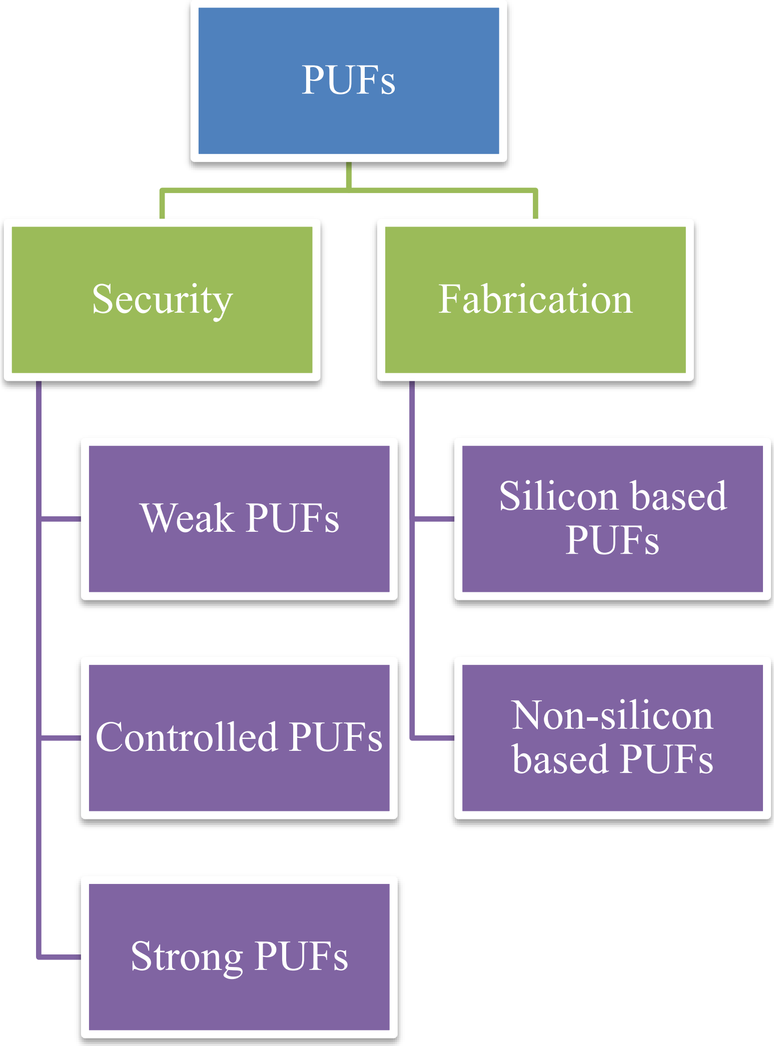


Figure 2-11: Classification of PUFs.

The primary functions of PUFs are low-cost authentication and generation of secure key. The low cost of PUFs can be achieved through the fabrication processes while secure key generation is achievable through strong PUFs. The PUFs are categorized into two models i.e., strong PUF and weak PUF models. These classifications are based on the number of Challenge Response Pairs. Strong PUFs are employed for authentication while weak PUFs are used for key storage. PUFs have ability to be modelled for response systems such as black box challenge response system where an input is given to PUF system as challenge c, and the returned response is as given in equation below:

$$r = f(c) \tag{2-9}$$

f(.) is defined as the relationship between output and input of PUF. Black box challenge response system is useful in these conditions as it can effectively hide from the users and can show the internal variability of manufacturing. Black box model can generate a unique challenge and response sets. The black box model is shown in Figure 2.12 [36]. The response of the system is usually determined by some of very complex physical functions of PUF systems. These complex functions are unique for each device as well as the generated responses. The basic difference between strong and weak PUFs is the use of domain such as *f(.)* and the total number of unique challenges that can be processed through PUF system. Weak PUF systems can support very few challenges even at some instances only a single challenge can be processed. While strong PUFs can support large number of challenges along with the respective challenge response pairs in a given time frame [20].

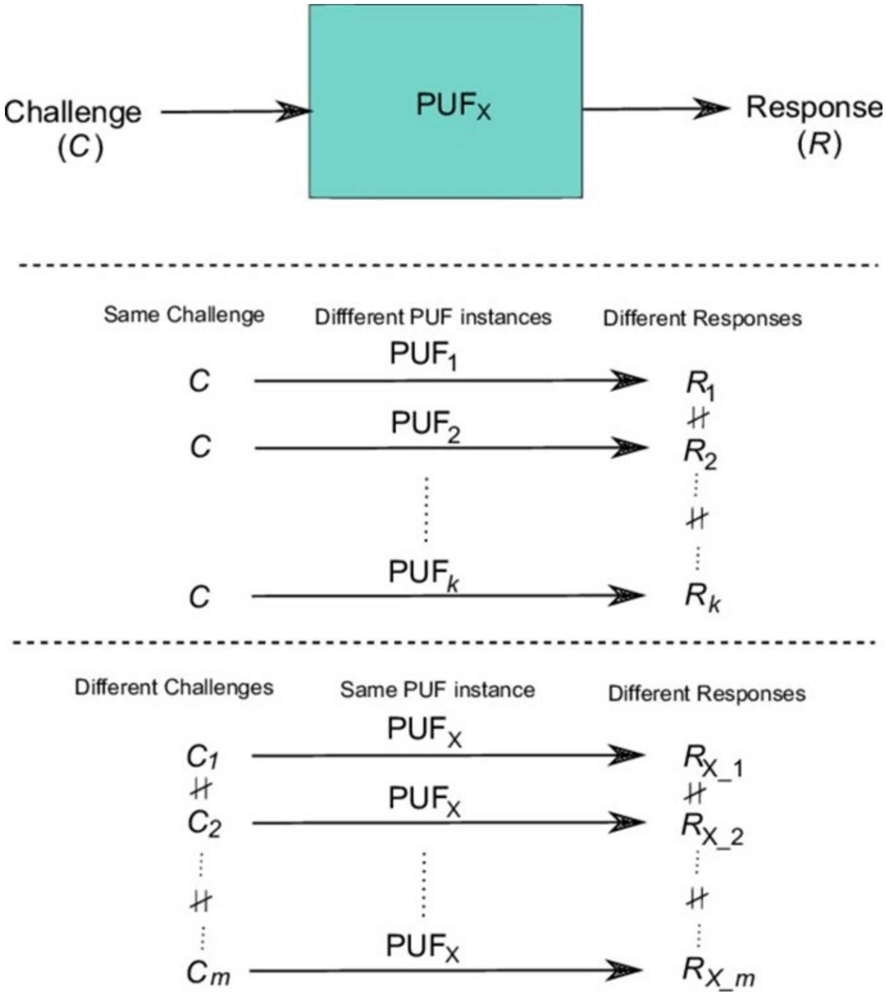


Figure 2-12: A PUF based system that can be treated like black box model.

2.5.1 Strong PUFs

Strong PUFs support large number of challenge response pairs. Authentication in strong PUF can be carried out without using any cryptographic technique or hardware. The difference between weak and strong PUFs are shown graphically in Figure 2.13. Strong PUF based systems have the following requirements.

- Challenge response pairs have large enough responses to not give any time for Trojan or attacker to copy these responses in a certain fixed time.

- A stable response environment with the ability of multiple readings.
- The responses are generated randomly, not to give any indication to the attacker for the possibility to predict the response. The response will always be random and unique to over such attacking issues.
- Two PUFs cannot be fabricated having same challenge response.
- Hacker will be unable to get the underlaying information of any response to know about the internal functionality of PUFs.

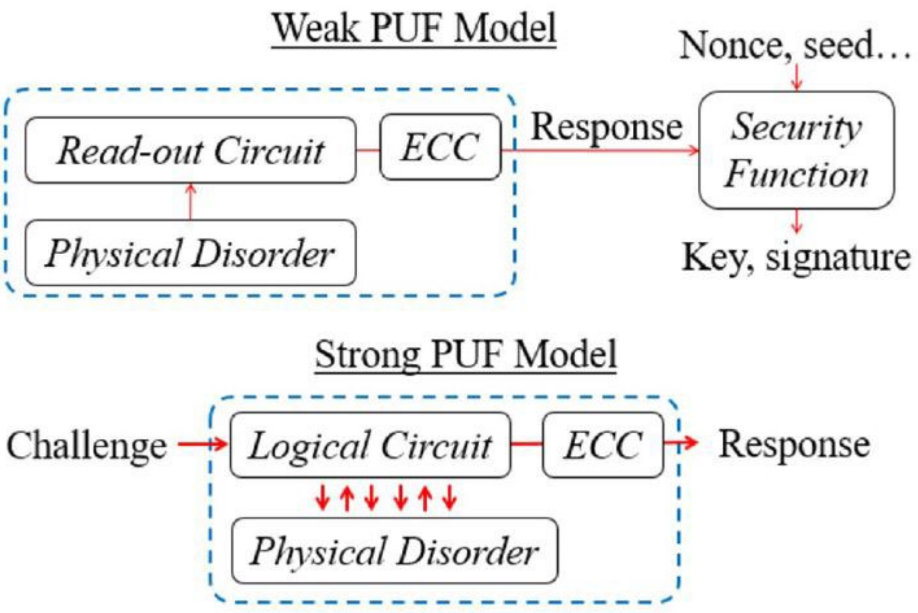


Figure 2-13: Difference between strong and weak PUFs [37].

It is worth noting that a weak PUF can perform the authentication if it is attached with cryptographic hardware that supports HMAC or some other authentication techniques. These techniques can support challenge response pairs that grow exponentially but require response stability must be 100% along with error correction in responses [38].

Similarly, the security difference between strong and weak PUFs must be kept it mind before implementation of these systems. The response of weak PUFs must be kept private to protect from possible attacks. Moreover, strong PUFs have read out restriction on responses due to the implementation of various system model. Strong PUFs provide fast enumeration of challenge response pairs while weak PUFs are protected through a secret key that uses cryptographic technique and relevant hardware to limit the outside access to outputs for protection. The strong PUF system can protect itself from such unauthorized access to the internal functionalities [20]. A typical strong PUFs model is shown in Figure 2.14 [39].

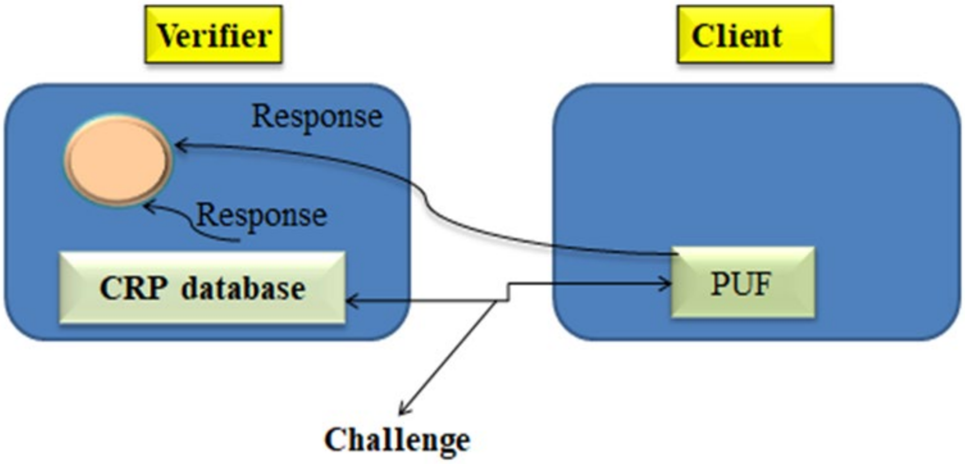


Figure 2-14: Strong PUF system-based model.

2.5.2 Weak PUFs

First class PUFs that use the production variability are known as weak-PUFs or Physically Obfuscated Key (POKs). Such PUFs can be used to directly digitize some of “fingerprints” in the circuit. This type of direct measuring produces a digital signature that can be used employed for the cryptography. The fingerprint signatures are mostly invariable which means PUF can only be used and assessed by single or few challenges. The black box model as explained earlier corresponds to a function with domain having small numbers of or only one input(s). Moreover, the domain has limited range with any challenge giving the same response ignoring noise [20]. The same black box model can be used in support of more challenge response pairs. Even after the use of black box model, this is still a weaker PUF model based on the number of responses generated that are linearly proportional to the components in fabrication variation. A weak PUFs system have following characteristics and properties.

- Weak PUFs generate a few numbers of challenge response pairs and these responses are directly related to the manufacturing variations.
- The generated response has high stability and unique with the environment conditions so that every challenge may have the same response.
- Responses are generally dependent on the fabrication variability of the devices. These responses are somehow unpredictable.

An example for weak PUFs is a SRAM, which has symmetrical structure. Variations and variability in fabrication of devices can bring the tendency of logical "1" or "0" during power-on mode. This variation is purely random across the SRAM, it gives a unique identifiable fingerprint for power-on systems. In the following example, if the "response" contains the whole SRAM state as power-on, the concept of "challenge" is not that useful as there is only one potential "challenge" to power-on the SRAM system. The output signature remains the same with the exclusion of noise. Increase in size of SRAM structure can provide more output bits but the space related to responses is still dependent linearly on the number of components. Total components are based on manufacturing variability for each SRAM system. SRAMs are known as weak PUFs as most of these have only one challenge response pair. As weak PUFs have limited number of challenge response pairs, the security of these response pairs must be taken seriously by keeping them secret. PUFs with only one challenge response pair can comprise the security of whole system if leaked or revealed. Weak PUFs can generate randomness for the secure storage, and this secure storage generates a secret key. PUF response bits are responsible for this secret key. The key is recovered in PUFs using error corrections and cryptographic techniques. For weaker PUFs, the output is employed as a secret key for key hashed authentication coding system (HMAC) challenge response pairs or sequences. Additionally, the output can also be used and employed for secret keys in encryption and decryption of data in various devices. The example of HMAC is shown in Figure 2.15 [40].

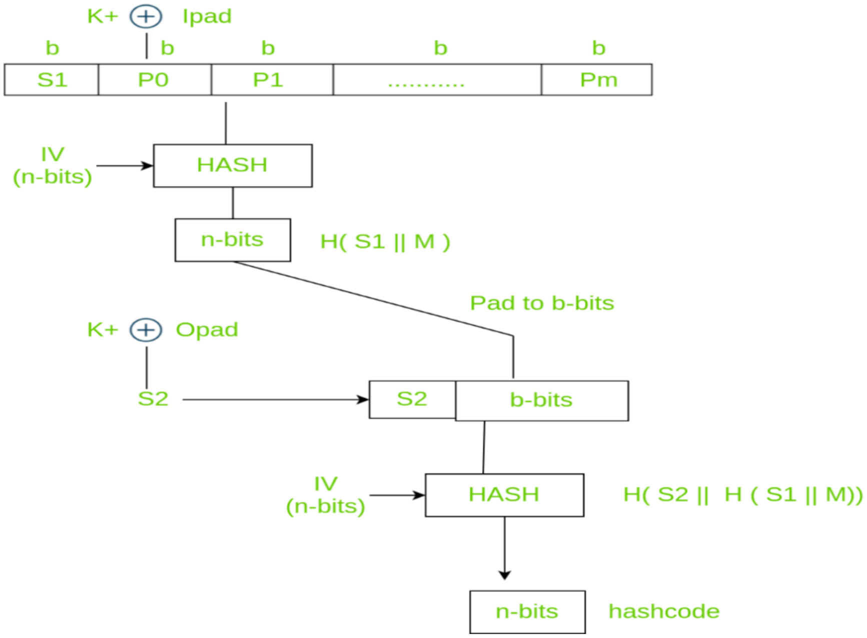


Figure 2-15: Challenge response pair or sequence for authentication of hash key codes (HMAC).

2.5.3 Silicon PUFs

Silicon based PUFs and other integrated circuits form interfaces. Silicon PUFs are manufactured on the same die being part of integrated circuit. The process variations during manufacturing are considered as challenges. Delay in information and timing produce a unique response for any given challenge [6]. Various research studies are focusing to control the variation in manufacturing of silicon based PUFs. Control on process variations can be used in cryptography, device authentication, and other application related to security. Silicon PUFs are used in generation of unique signature in different integrated circuits. Table 2.2 shows various types of silicon and non-silicon PUFs [21].

Table 2.2: Various types of Silicon and non-Silicon PUFs.

Silicon PUFs	**Non-Silicon PUFs**
Memory based PUF	Magnetic PUF
Glitch PUF	RF-DNA PUF
Butterfly PUF	Acoustical PUF
Bistable PUF	Paper PUF
Delay based PUF	CD PUF
Power grid PUF	Optical PUF
Latch PUF	Phosphor PUF
Coating PUF	
Analog electronic PUF	

2.5.3.1 Memory based PUFs

One of the most used silicon PUFs include memory based PUFs. Memory based PUFs are represented by butterfly and SRAM PUFs. SRAM PUFs usually contain a great number of memory-based units. SRAM PUF is shown in Figure 2.16 [21].

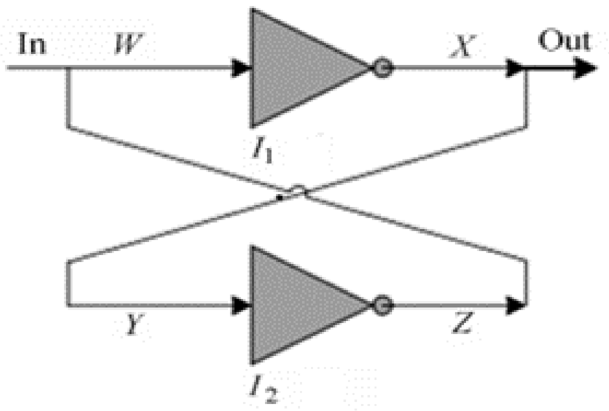


Figure 2-16: Cross coupling of two inverter units for SRAM PUF.

A memory unit for SRAM PUF is formed with the cross coupling of two inverter units. Stable states in these units are represented with 0 and 1. Even a minor difference or fluctuation in voltage due to intrinsic variations is the resultant of the amplifying effects of inverter on to the outputs. Generated challenge is referred to memory units of inverter and can be read after they are powered on. SRAM PUFs are not recommended for all type of FPGAs [41]. To overcome the issues and complexities of SRAM PUFs, butterfly PUFs are recommended. The idea of butterfly PUFs was proposed by Kumar et al.[42] Butterfly PUFs are based on circuits that are unstable and cross coupled. Such circuits replace the inverters through flip-flop or latch as shown in Figure 2.17 [21].

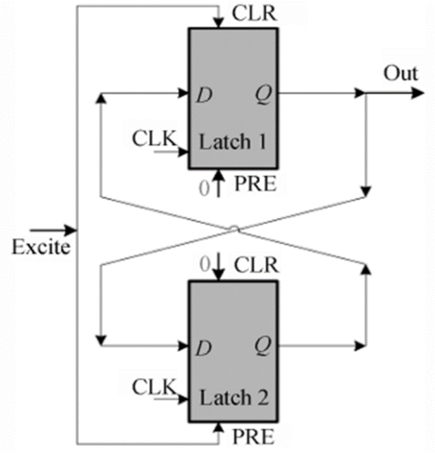


Figure 2-17: Butterfly PUF layout with cross coupling of latches.

Latches in butterfly PUFs are used to store data and information and these PUFs are not required to be powered on for output generation.

2.5.3.2 Delay based PUFs

Various PUFs such ring oscillator PUF, intrinsic personal PUFs and arbiter PUFs are part of delay based PUFs. Arbiter PUF is shown in Figure 2.18 [7].

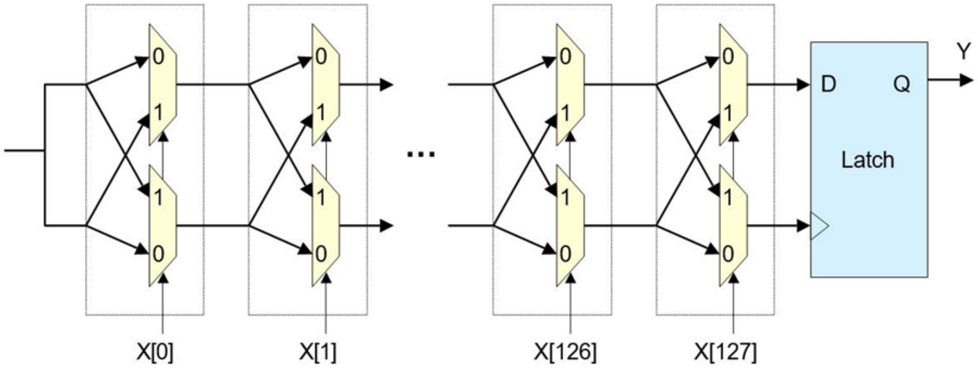


Figure 2-18: Basic Structure of Arbiter PUF.

Two multiplexer chains that are parallel are sharing the input port and the output ports are connected with input port labelled as D. Step input signals are used by input ports. The response of delay based PUFs can be shown as linear function for the challenge. The attackers can predict responses by knowing delay of all units. Attackers usually employ customized software to calculate the sum of delays in all units. Methods such as artificial intelligence and machine learning are employed by these attackers for such purposes [21].

2.5.4 Non-Silicon PUFs

PUFs other than silicon are known as non-silicon PUFs. They are fabricated in the same process as silicon but with some modifications in fabrication process. Complementary metallic oxides semiconductor (CMOS) fabrication methods are not used for the fabrication of non-silicon PUFs. Similar in the case with silicon PUFs, the response is usually generated through challenges via random physical variations from the physical system in place of integrated circuit [6]. Types of non-silicon PUFs are mentioned in Table 2-2. Types of non-silicon PUFs are explained below.

2.5.4.1 Optical PUF

Physically one- or single-way functioning PUF (POWF) was introduced by Pappu et al. A two-dimension speckle pattern was formed with the use of epoxy wafer that was transparent. A laser beam was employed for patterning of such structure. The same structural pattern is then used in production and generation of fix length bit keys. Major challenge for optical PUF is the precision required for laser beam in patterning [43]. Tuyls et al. theoretically analyzed optical PUFs. Slow or weak PUFs were employed to overcome the issues related to the Trojan attacks and hacking [44,45]. Similarly, Ignatenko et al. used different coding algorithms that are based on universal sources to maintain the secrecy of PUFs. The universal coding source is known as context tree-based weighting technique [46].

2.5.4.2 Acoustical PUF

Vrijaldenhoven introduced the concept of acoustical PUFs that was made possible due to variability and innovation in manufacturing [47]. Acoustical PUF is made through materials like glass and used to transform and convert electrical signals into the mechanical vibrations. This conversion is usually carried out through transducer. The signal produced in the process is unique for every acoustical PUF.

2.5.4.3 Paper PUFs

The intrinsic roughness on the surface can be used in the generation of physical randomness across PUFs. This randomness can give strong and built-in security features in various applications for paper PUFs. Buchanan et al. analyzed the use of focused laser beams for specific angles and the reflected intensities to enhance the security of branded products and documents against attackers and frauds. The verifications of fingerprints in paper PUFs require the use of laser-based microscope that can contribute to increase the overall cost [48].

2.5.4.4 RF-DNA PUFs

An RF-DNA technology was proposed by DeJean et al. for the generation of PUF fingerprints for various interactions of a device under electromagnetic waves. A cryptographic certificate is generated and produced to check authentication and verification to prevent any unauthorized access to the device. The same PUF model can be used for checking and distinguishing counterfeit and fake products [49].

2.5.4.5 Magnetic PUFs

Magnetic PUFs are employed through the patterning of magnetic media for the generation of unique fingerprints [21].

2.5.4.6 Phosphor PUFs

Phosphor PUFs are used mainly to counter fake counterfeit products in systems and devices. Random patterns are generated by the scattering of phosphor for unique identification that act as physical identifiers [50].

2.6 Attacks against PUFs

2.6.1 Active Attack

An active attack can be invasive or non-invasive. Invasive attacks are on the chip delays of modern devices and equipment such as Focus Ion Beam (FIB) and other important processes. PUF secret keys should not disclosed and must be protected from unauthorized access. Due to these preventive measures, many attacks can be avoided on PUF. The non-invasive attacks can disrupt operating condition of a PUFs and making it unstable [51]. Non-invasive attacks are mainly side channel attacks that are designed to penetrate weaker channels. These attacks leak and reveal information in a physical phenomenon such as power consumption, photon emission, electromagnetic emissions etc.

2.6.2 Passive Attack

Through side-channels, the PUF may be attacked passively such as power consumption or electromagnetic radiation emitted from a chip containing a PUF [52].

2.6.3 Replay Attack

During the authentication process, an attacker can create copies of CRPs and apply these continuously to fake the original PUF. Using a unique and secure CRP, this sort of attack can be avoided [53].

2.6.4 Cloning Attack

In this attack, hackers or attackers attempt to make a physical copy of the original PUF with duplicate challenge-response behavior. No successful cloning attacks on PUFs have been reported so far.

2.7 Advantages and disadvantages of PUFs

The main disadvantage of PUFs is the noisy output and unstable responses that are sensitive to environmental factors leading to generation of random errors. The advantages of PUFs are cost reduction and security. Encryption keys protect data for Internet of Things (IoT). These keys are provided by the manufacturer or chip supplier. Encryption keys increase the complexity and cost for the chip fabrication. Random Number Generator (RNG) can be used to decrease the fabrication cost for PUF. The key cannot be stored in non-volatile memory (NVM). Therefore, alternative secure key storage is required. one option is to add a safety element to the device. However, adding hardware increases complexity and cost. Silicon PUFs can store encryption keys securely without adding any other hardware. The level of security used to set up and store encryption keys, supply chain overhead, and the cost of technical options must be considered while designing security for PUFs.

2.8 Applications of Physical Unclonable Functions (PUFs)

PUFs provide unique and essential security features for devices and integrated devices to avoid the attacks of hackers and Trojans. PUFs are used to store sensitive data in non-volatile memory and to generate unique PUF responses to provide higher physical security [41]. PUFs have been extensively studied in last decade for authenticating integrated circuits and electronic components to enhance data security [54]. PUFs are employed for various security applications that include identification, authentication, and verification. They are used in a variety of industries, including telecommunications, banking, and medical devices. PUFs are used to create secure cryptographic keys to provide unique identities and protect against counterfeiting and attacks. PUF circuits are applied to application-specific integrated circuits (ASICs), or to FPGA, primarily on memory chips using a variety of CMOS technologies.

2.8.1 Applications in Internet of Things (IoT)

With the growing number of smart devices being deployed across several industries and home applications, the concept of IoT is becoming imperative. IoT encompasses smart devices that are connected to the internet and interconnected to for various applications. These include devices in smart homes, buildings, and personal equipment, from alarming systems to control systems in industries and more complicated systems as well. IoT ensures communication, but with this comes the mandatory requirement of security to ensure access control, confidentiality, integration and protection against active and passive attacks. Smart devices store secret keys and identifications as texts, and these are vulnerable to attacks. PUFs offer an opportunity to solve these issues and some applications are discussed below.

2.8.2 Supply Chain Management Applications

To store product information, products are usually tagged by RFID or other electronic tagging methods which store important information as texts. As mentioned above, this information is vulnerable to attacks, both internal and external. PUFs can enhance the security of this information in the form of PUF-RFIDs. The manufacturers can maintain a database of PUF-IDs after they are introduced in the products, and these can be used to store important information which can be verified by the consumers using long distance RFID readers. The disadvantage of this technique is the high cost associated with introducing PUFs and the use of long distance RFID readers.

2.8.3 Pay Television Applications

Cyphered video streams can be accessed by smart cards. However, to secure these cards with a higher level of security, PUFs can be introduced which generate private keys that can be used to decrypt the video stream encrypted by a public key on the server side.

2.8.4 Applications for Manufacturing Contracts

Large manufacturing companies often outsource production to smaller companies. They do not have effective methods to ensure that these smaller companies do not manufacture low grade products of the same nature and sell it off to other companies during night shifts. This is a clear violation of contract and can be avoided if PUF based chips are mandated to be installed in each product, and their database to be maintained. These chips can then have their PUF-IDs monitored to ensure no violation of contract occurs.

2.8.5 Dynamic Identity Allocation Applications

Another application of PUFs for unique ID allocation to devices associated in IoT is that instead of storing the ID in some dedicated memory, the unique ID is generated dynamically using PUFs. Existing components in the smart devices can be used as PUFs. An example of this is the Unclonable RFID tag.

2.8.6 ICs Activation and Deactivation (IRAD) Remotely

PUFs have also found applications for IRAD in smart devices associated with IoT. To validate the ICs' PUF-based embedded intellectual property a few methods have been researched. The IC activation and user authentication can be achieved by contacting the intellectual property owner.

2.8.7 Software Attestation for Smart Devices in IoT

Another application of PUFs in a completely new dimension is by introducing lightweight remote attestation for distant devices in IoT. The software attestation process can be linked with the remote PUF-based hardware.

2.8.7.1 PUF based applications in Wireless Sensor Networks

To structure IoT in innovative application scenarios, wireless sensor networks form a key component. Sensing devices from these networks contribute to a massive number of things. The key mechanism is to share sensing data in IoT. Data such as temperature, humidity, wind speed, and light are common examples of data types. In some sensitive applications the data from sensors is crucial to deliver effective applications and service and requires protection. PUFs find potential applications in this regard for increasing the security of sensing information and authenticating the sensors. Some examples of this application are as follows:

- An impedance mismatch PUF circuit to generate a private key to be used in authenticating IoT objects.
- A public PUF (PPUF) for use in building trusted sensing systems. These are used for encrypting the wireless sensor data and authenticating the sensor by adding extra information like the timestamp and location data.
- Secure key generations in wireless sensor networks to avoid the data breach and Trojans.

2.8.7.2 PUF based applications in Wireless Body Area Networks

A healthcare application of IoT is wireless body area networks. These represent wearable sensors including medical sensors to sense data about temperatures, heartbeats and blood pressure. Some of the sensors in these applications are usually placed inside the body, making them hard to replace and remove. This has generated an application for PUFs, wherein low power and simple equipment is used to transmit data in these body area networks, and due to their simplicity, PUFs offer an attractive security and authentication method.

2.8.8 Signature Generation

PUFs have the application of identifying physical objects in the same capacity as biometrics have the capacity to identify people. A group of individual PUF structures can be used to generate a unique signature for authentication of a device. The signature is generated dynamically from physical properties unique to the device, it cannot be duplicated and is tamper resistant. This makes application in intellectual property protection very attractive as each device now has a unique signature. Some examples of its uses in this domain are as follows in sections 2.8.8.1-3.

2.8.8.1 Anti-counterfeiting

To manage anti-counterfeiting, PUF based data can be stored off-line and these databases are used for cross verification of products. However, this method is relatively new and require more research as it has some drawbacks such as lack of methods to deliver the database to customers for cross verifications and lack of methods to update the offline database incase new PUFs are added as identifiers. It also requires additional overhead to synchronize the offline database with the latest upgrades.

2.8.8.2 Intellectual Property and Design Protection

The ability of signature generation by PUFs can be used for design protection by manufacturing industries. A database of the unique IDs of each manufactured product can be maintained by the manufacturer, so that if the design is copied and illegally reproduced, the new products will not have IDs matching the original database. This ensures design protection.

2.8.8.3 Enhancement of the Security of RFID Authentication

As established in IoT applications of PUFs, the ability to enhance the security of RFIDs. This can be applied in the RFID-based book ID in libraries, electronic door keys in hospitals, IDs for workstations in offices and industries. PUFs have been integrated well with RFID to bring high security. It is a low-cost option as no on-chip memory is needed to store the ID value. Some other signature generation applications are as follows:

- Symmetric-key authentication protocol
- Authentication of mobile sensor network nodes

2.8.9 Cryptography

PUFs can be used to generate dynamic secrets for cryptography. These secrets are not stored in volatile or non-volatile memory that are vulnerable to attacks. These secrets are needed for cryptographic decrypting operations and need to be stored in a very secure way. For example, a mobile phone whose firmware must be decrypted on each startup needs a cryptographic key that must be stored securely. Physically disassembling such a circuit will destroy its delay characteristics and consequently change its output, therefore PUFs can reduce these vulnerabilities to a great extent.

2.8.10 Random Number Generator Applications

A PUF can be used as a cryptographically secure random number generator. Several types of PUFs have been successfully deployed as true random number generators. Similarly, deterministic random bit generators can also be generated and paired with PUFs. The numbers may be predictable but the pairing with PUFs makes it unique if the PUF seed is hidden.

Chapter 3

Performance Study of FPGA Based AND-Inverter Ring Oscillator PUFs

3.1 Introduction

The demand for Field Programmable Gate Arrays (FPGAs) is ever increasing because of their attributes such as low time to market (rapid prototyping), parallelism, and low engineering cost. These attributes have made the FPGA a favorable platform in signal processing, aerospace, high-speed communication and defense applications [55]. But with this progress, the issues of IP theft, hardware metering, hardware Trojans, etc., are also on the rise [56, 57, 58]. Researchers have suggested a number of security mechanisms for FPGA based systems, among which the Physical Unclonable Function (PUF) is one [59, 60]. PUFs exploit manufacturing process variations in IC fabrication and come in numerous designs; some of them are more suitable for ASICs while others like the Ring Oscillator PUFs (ROPUFs) are best suited for FPGAs [61, 62]. PUFs are considered one of the promising solutions when it comes to hardware security. However, with every solution there are some drawbacks. For example, considerable research has been done and is still underway to resolve the issue of bit-flip occurrences, which is due to bit aliasing of the outcome [63, 64]. The major accomplishment of this chapter is the implementation of the ROPUF which consists of a single AND gate cascaded with an odd number of inverters.

3.2 Background

The stages of ROPUF are defined by the number of inverters added into the design and it remains unchanged with the number of buffers added into it. For example, a 3 stage ROPUF will have 3 inverter gates in it while 5 stage and 7 stage ROPUFs will have 5 and 7 inverter gates, respectively. The performance parameters or metrics used to measure the efficiency of PUFs are uniformity, bit-aliasing, standard deviation frequency, uniqueness, correctness, steadiness, reliability, and randomness. In the current scenario of a ROPUF based design, the evaluated metrics are reliability, uniqueness, uniformity, bit-aliasing, randomness, and standard deviation frequency [65-69].

A brief description of PUF performance parameters is given next to the notations used, which are:

- K = total number of devices used
- k = index of device being used
- p = bit response from chip k
- C = challenge vector
- R = response vector
- L = length of stages implemented
- T = number of tests generated

3.2.1 Reliability

PUF reliability assesses the strength of a PUF to replicate the response bit under a variety of settings, and this relates to how efficient a PUF is at reproducing the response bits. The ideal value is 100%, and anything close to that value is considered good. It is a test between different environmental or any other conditions.

$$Reliability = 1 - \frac{1}{K.T.L}\sum_{k=1}^{K}\sum_{t=1}^{T}\sum_{l=1}^{L} r_{n,k,l} \otimes r_{n.k.t.l} \qquad (3\text{-}1)$$

where $r_{n,k,l}$ is the *l-th* binary bit of the *t-th* sample of the *k-th* FPGA (tested under specific condition). Further, *k* is the index of the ID in the chip*, t* is the index of the sample, *l* is the index of the response bits, and *n* is the index of the chip.

3.2.2 Uniqueness

Uniqueness refers to a PUF's ability to provide identifiable outcomes in multiple de-vices despite using the same design and having the same set of challenges applied. This is critical because PUFs rely on the inherited delay variation of the device and replicating similar results from two different devices under the same set of challenges is quite a challenge. For various ROPUFs, the inter-chip uniqueness was determined by calculating the hamming distance of the response bits associated to the challenges throughout all of the chips. The ideal uniqueness value is 50%; therefore, any uniqueness value near 50% is considered a good value. What this value means is that at least 50% of the responses generated from chip u and v differ from each other. Each FPGA chip generates the response vector $R = [r_1, r_2, \cdots, r_n]$ for a challenge vector $C = [C_1, C_2, \cdots, C_m]$. The response matrix for k FPGA chips is thus supplied as follows:

$$\mathrm{R_i} = \begin{bmatrix} \mathrm{R_1} \\ \mathrm{R_2} \\ \vdots \\ \mathrm{R_k} \end{bmatrix} \tag{3-2}$$

The following formula is used to determine the inter-chip uniqueness:

$$Uniqueness = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(R_i, R_j)}{N} \times 100 \tag{3-3}$$

where *i* and *j* are two chips being compared and *N* is the number of response bits generated. R_i and R_j are the response bits from the same challenge *C* for chip *i* and *j*. *HD* is the hamming distance between response bits generated from chip *i* and *j*.

3.2.3 Uniformity

The PUF uniformity is the amount of 0s and 1s in a *p*-bit response from a chip *k*. The ideal value for uniformity is 50%; this means that any value around 50% is considered a good value; the closer the value to the 50%, the better the uniformity. This is measured by calculating the intra-chip hamming weight (HW) where $r_{i,l}$ is the *l*th binary bit.

$$(Uniformity)_k = \frac{1}{p} \sum_{i=1}^{p} r_{i,l}\ X\ 100\% \tag{3-4}$$

where $r_{i,l}$ is the lth binary bit of *n* bit response from a device *n*.

3.2.4 Randomness

The randomness of a PUF is based on the ratio of 1s and 0s in the response bits. The ideal value is 100% and anything close to that value is considered good. The device randomness H_n of a PUF is given by

$$H_n \ = \ -log_{2^{max}}(p_n, 1 \ - p_n) \tag{3-5}$$

Where p_k is the frequency of 1’s in the output results, whose expression is shown in the equation below, where *k* is device number and $b_{k,t,l}$ is the *i-th* bit response of challenge set on *k-th* device.

$$P_k = \frac{2}{k(k-1)} \sum_{k=1}^{K} \sum_{t=1}^{T} \sum_{i=1}^{L} \frac{HD(R_i, R_j)}{N} \times 100\% \tag{3-1}$$

3.2.5 Bit Aliasing

Bit aliasing estimates the bias of a response bit across *K* different devices. Bit aliasing estimates the bias of a response bit across different devices. The ideal uniqueness value is 50%, therefore; any uniqueness value near 50% is considered a good value. It can be explained using:

$$(bit - aliasing)_l = \frac{1}{K} \sum_{i=1}^{K} r_{i,l} \ X \ 100\% \tag{3-2}$$

where $r_{i,l}$ is the lth binary bit of *n* bit response

3.3 Implementation of AND-Inverter ROPUF

For a given challenge, a ring oscillator generates a one-bit response by comparing the frequencies received from two oscillators. The proposed design consists of a single AND gate and an odd number of inverter gates. A three stage ROPUF consists of one AND gate and three inverter gates. The five stage implementation has one AND gate and five inverter gates. And the seven stage, one AND gate and seven inverter gates. The layouts of ROPUFs for each of the three different stages used in our study are shown in Figure 3-1. The stage of the ROPUF is defined by the number of inverters inherent in its circuitry.

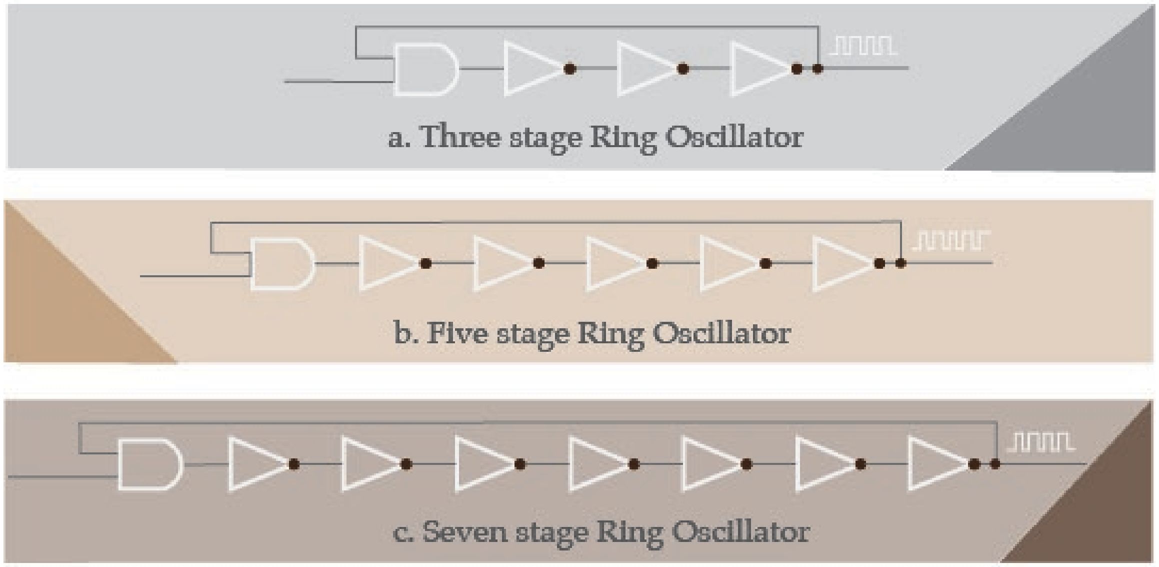

a. Three stage Ring Oscillator
b. Five stage Ring Oscillator
c. Seven stage Ring Oscillator

Figure 3-1: Three, Five and Seven stage AND-Inverter based ROPUFs.

Figure 3-2 shows the component level layout of the ROPUF mapped on an Artix-7 FPGA. The 3-stage ROPUF utilizes 4 LUTs, the 5-stage utilizes 6 LUTs, and the 7-stage utilizes 8 LUTs. A total of 256 oscillators are used in this design. Each RO is manually mapped using the FPGA Editor tool in order to have identical ROs placed at different spatial locations of the FPGA. Figure 3-3 shows the floorplan layout of the RO hard macros on four different CLBs taken from Xilinx FPGA Editor. In the figure, the four ROs are shown in yellow, blue, orange, and green color with small circles inscribed on them. It is important to note that the correct placement of the ROs within the FPGA is of critical importance for obtaining accurate results. In our design, challenges for choosing the ROs are produced through a 10-bit challenge generator. After the challenge is applied, the frequency counter is switched on for 0.4 ms to measure the frequency response. A 0.1 ms delay is used between challenges to select the next RO.

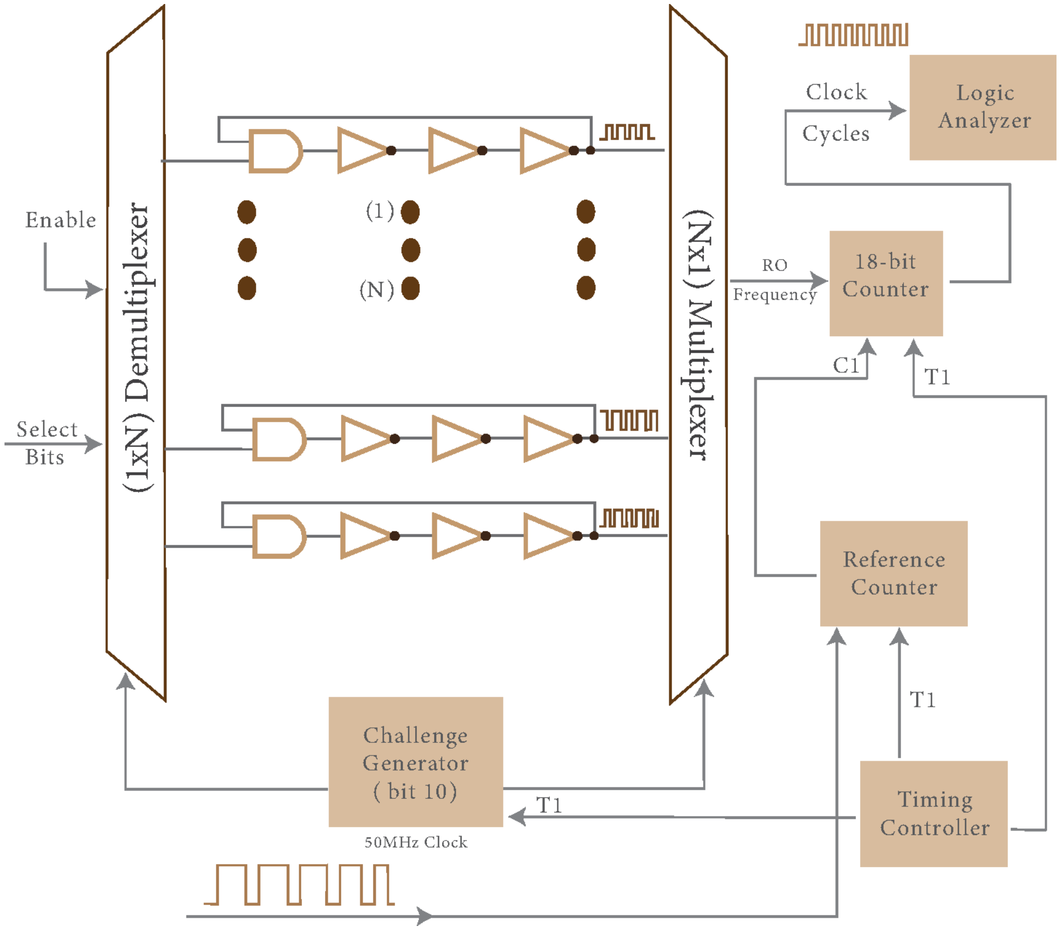


Figure 3-2: Implementation of AND-Inverter ROPUF.

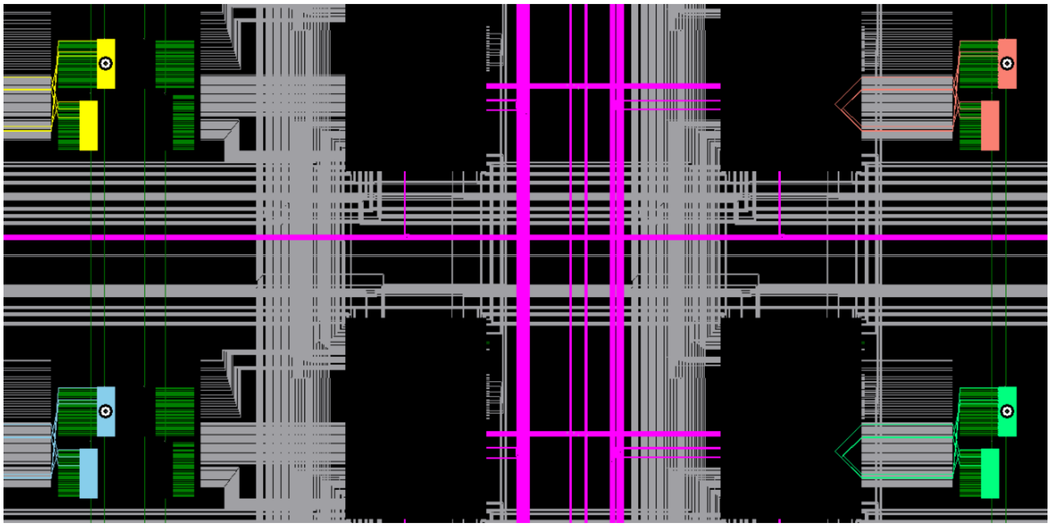


Figure 3-3: Floorplan layout of the RO hard macros on four different CLBs from Xilinx FPGA Editor.

3.4 Results from AND-Inverter based ROPUF

The results obtained from the AND-Inverter based ROPUF are shown and compared with existing models. The frequency distribution of data obtained from Agilent 16801 A Logic Analyzer is shown in Figure 3-4, 3-5, and 3-6. It is observed that the frequencies are evenly distributed for the three stage oscillator. For the five stage and seven stage, the distribution is not uniform.

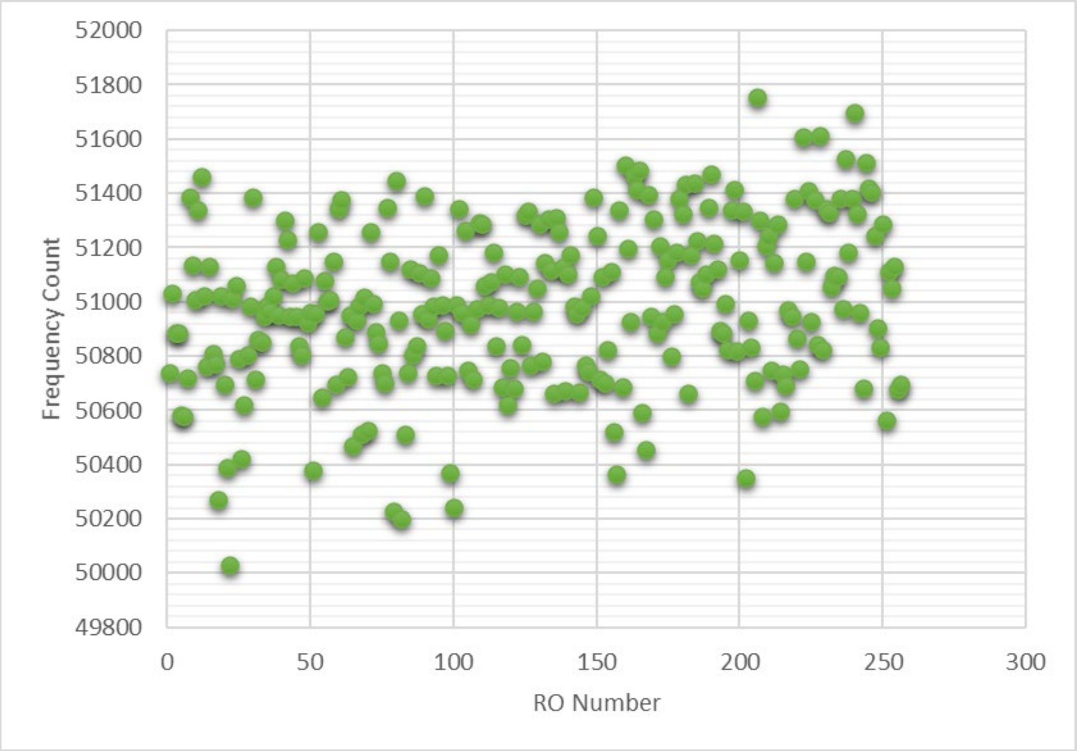


Figure 3-4: RO frequency count distribution for three stage ROPUF.

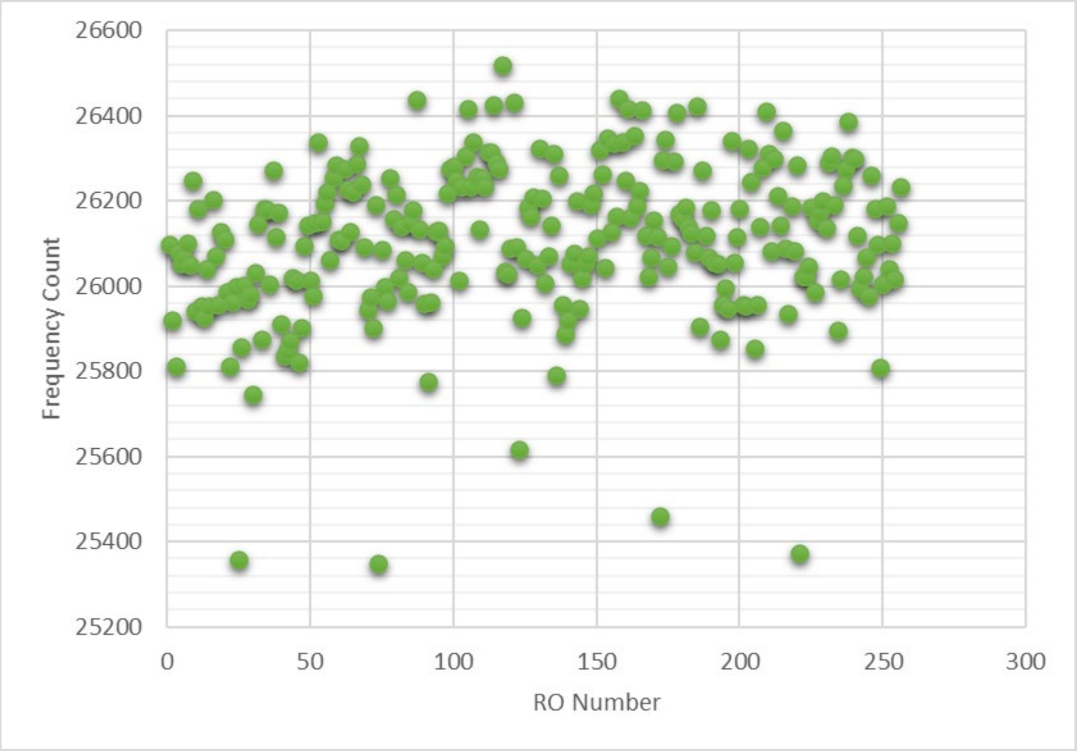


Figure 3-5: RO frequency count distribution for five stage ROPUF.

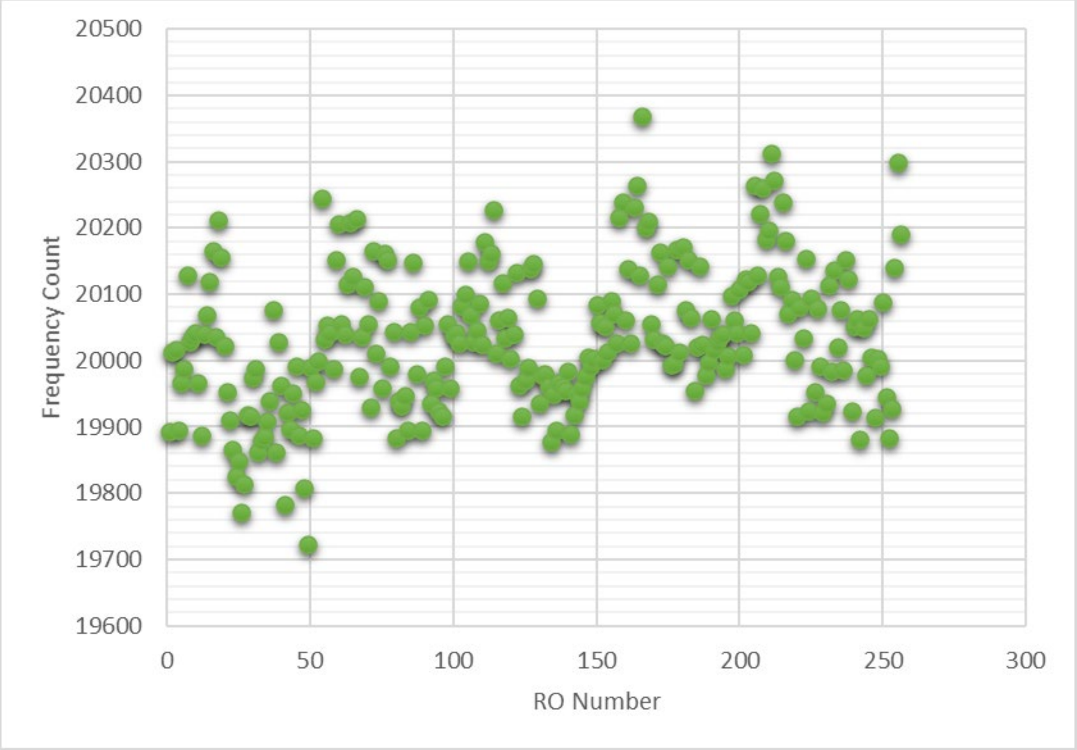


Figure 3-6: RO frequency count distribution for seven stage ROPUF.

Pareto analysis is used here to obtain rich data for all possible cases depending upon actual results. The performance parameters require relatively a huge dataset to provide clearer results. The pareto analysis is performed on the obtained frequencies and it is deduced that the frequency distribution in three stage RO is much better than five and seven stage ROs. The frequency distributions from three, five and seven stage ROs are shown in Figure 3-7, 3-8 and 3-9, respectively.

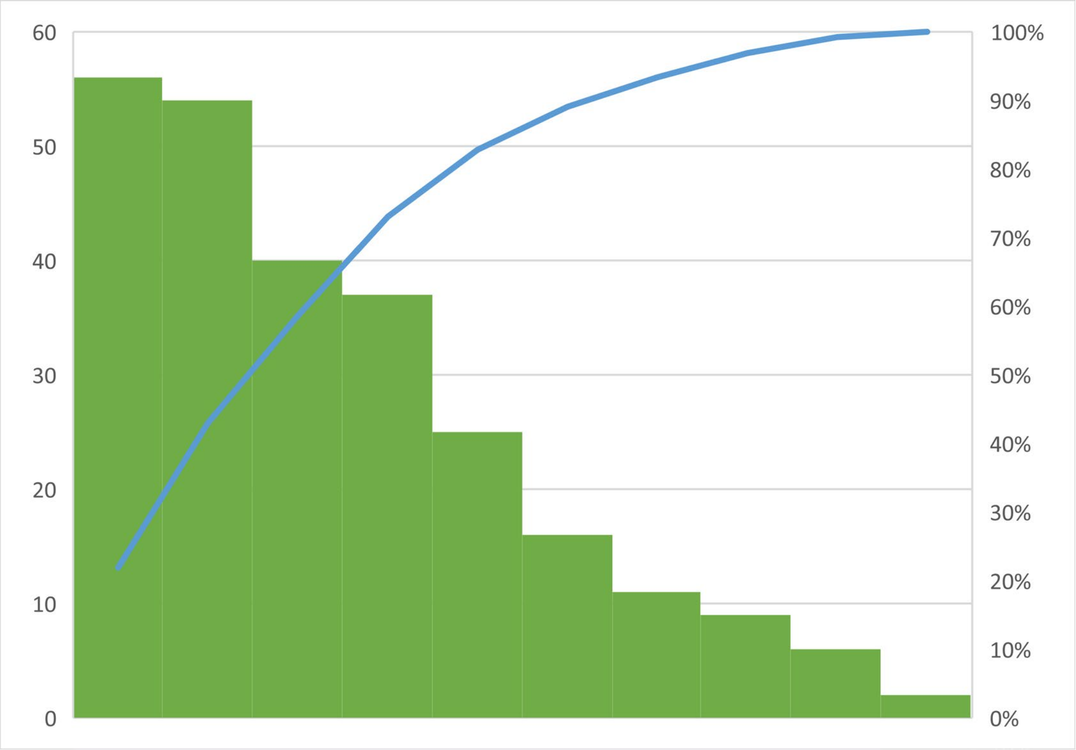


Figure 3-7: Frequency distribution for three stage oscillators.

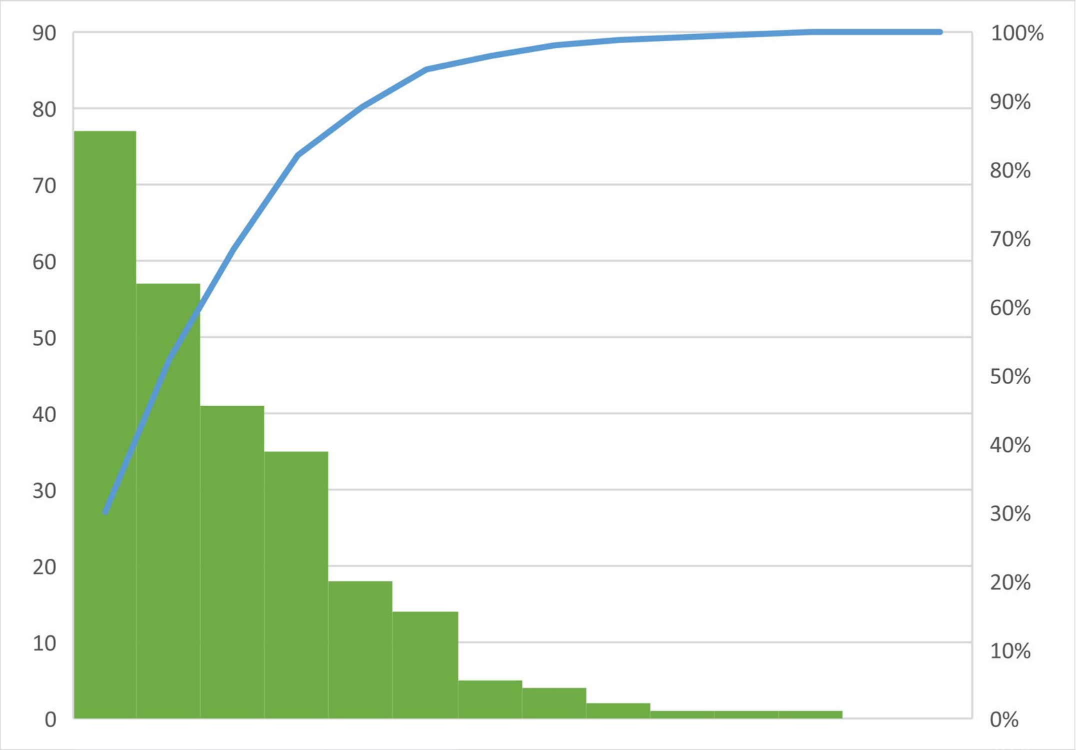


Figure 3-8: Frequency distribution of five stage oscillators.

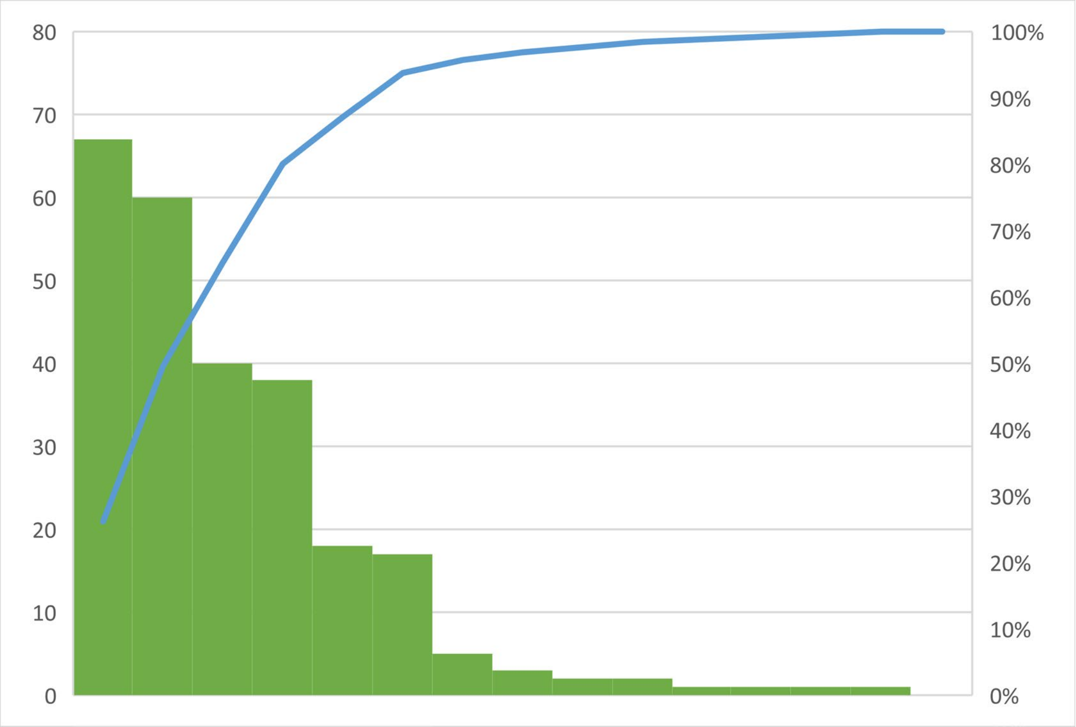


Figure 3-9: Frequency distribution of seven stage oscillators.

As seen from the results in Figure 3-7, 3-8 and 3-9, the frequency distribution of three-stage ROPUF is much better when compared to the five and seven stage ROPUFs. The number of bit flip occurrences are measured using 20 test runs for 10 separate Artix-7 FPGA boards. The percent bit flip occurrences in each of the 10 boards are shown in Figure 3-10. It is observed that the three-stage ROPUF performs better compared to the five stage ROPUF in terms of bit flip occurrence due to better frequency distribution.

Figure 3-11 shows the uniformity parameter obtained for the three stage AND-Inverter based ROPUF. For randomness, NIST has created a testbed to evaluate statistical data. A total of 11 NIST randomness tests were performed to evaluate the randomness of our ROPUF responses. The p-values and proportions are listed in Table 3.1. As the p-values were all larger than 0.01, it was concluded that the responses were random [70]. The AND-Inverter based ROPUF successfully passes the NIST Randomness tests. In Table 3.2, PUF parameters obtained from different research works are tabulated for comparison. The implemented AND-Inverter design predominantly reaches close to the ideal value and provides better results in the parametric evaluation.

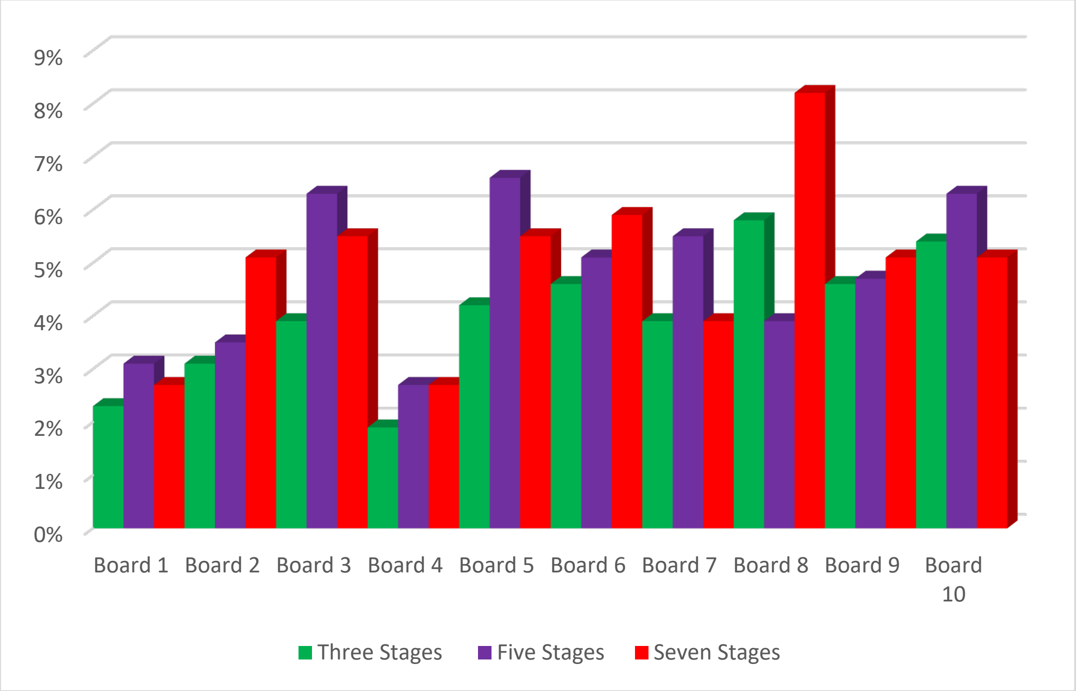


Figure 3-10: Bit Flip occurrences across ten different FPGAs.

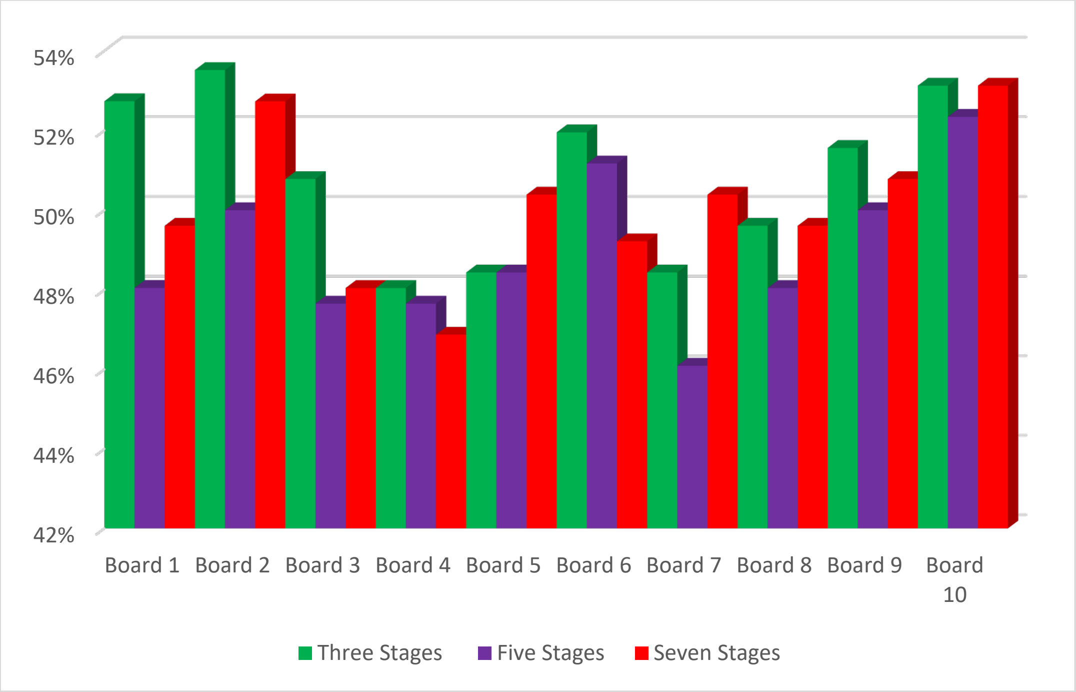


Figure 3-11: Uniformity accorss ten different FPGAs.

Table 3.1: National Institute of Standards and Technology (NIST) test results

Test Methods	P-Value	Result
Frequency Test (Monobit)	0.617075	Random
Frequency Test within a Block	0.882496	Random
Longest Run of Ones in a Block	0.021358	Random
Discrete Fourier Transform (Spectral) Test	0.730753	Random
Non-Overlapping Template Matching Test	0.999983	Random
Serial test	0.498961	Random
Approximate Entropy Test	1.0	Random
Cummulative Sums (Forward) Test	0.974204	Random
Cummulative Sums (Reverse) Test	0.945888	Random
Random Excursions Test	0.795191	Random
Random Excursions Variant Test:	0.215924	Random

Table 3.2: Comparison of PUF parameters for various research works.

Method		Reliability	Uniqueness	Bit-Aliasing	Uniformity	Standard Deviation of Frequency	FPGA
Ideal value (%)		**100%**	**50%**	**50%**	**50%**	**X**	**X**
Devadas [59]		X	45.40%	X	X	X	Spartan-3E
Maiti [63]		99.14%	47.24%	50.56%	50.56%	1.5 MHz	Spartan-3E
Mustapha [64]		98.86	39.79	50.45%	51.25%	1.6 MHz	Spartan-3E
		97.67%	45.15%	50.17%	50.17%	11.2 MHz	Artix-7
Gu [71]		98.97 %	45.15%	50.17%	50.17%	X	Artix-7
Proposed AND-Inverter ROPUF	**3-Stages**	95.77%	47.50%	50%	50.07%	10.39 MHz	Artix-7
	5-Stages	95.46%	43.55%	48.24%	48.24%	0.888 MHz	
	7-Stages	94.80%	45.27%	50%	50.82%	0.592 MHz	

X = Failed/Not reported.

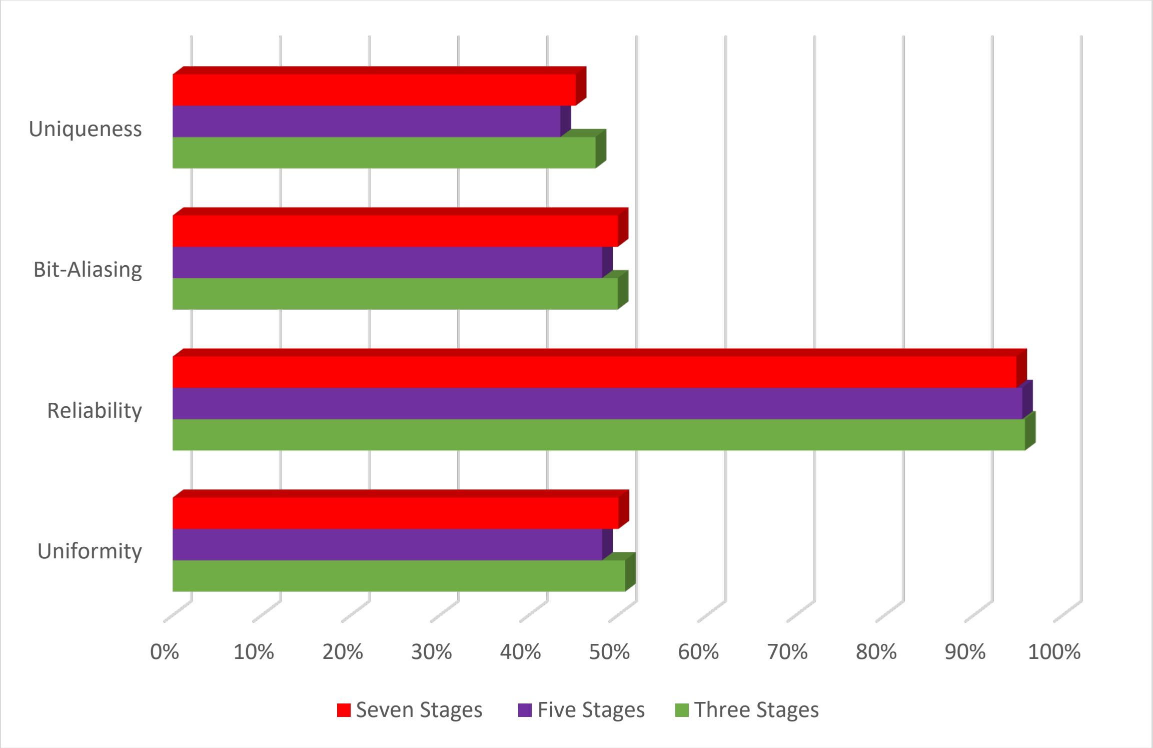


Figure 3-12: Comparison between different configurations of AND-Inverter ROPUF.

Figure 3-12 illustrates the comparison between performance metrics in different configurations of the ROPUF. As depicted in the figure, it is observed that the three stage ROPUF performs better in reliability, bit-aliasing, uniqueness, and standard deviation of frequency than the five stage and seven stage ROPUF.

Chapter 4

A Comprehensive Study of Environmental Impact on Ring Oscillator Physical Unclonable Functions

4.1 Introduction

Billions of devices utilize ASICs and Field Programmable Gate Arrays (FPGAs) for their functionality, which may be under threat without the availability of ample security features. This may result in loss of data, identity theft, or undesired access to classified information. The ASICs and FPGAs used to be limited to embedded systems, but now the industry is also adopting them, increasing the associated threat to another level. Not only this, but also autonomous vehicles that are either self-driving or remotely driven connected over the internet are also under threat and may face serious consequences in the case of a cyber-attack [72]. Any cyber-attack on an industry that uses digital systems for data acquisition or data sharing may have serious consequences [73].

The solution lies in the provision of foolproof hardware security for sensitive equipment under threat. Silicon-based Physical Unclonable Functions (SPUFs) are a promising solution [43,74-77]. They are produced by exploiting the fundamental characteristic of ASICs: propagation delays and transmission delays between the components. FPGAs also share this characteristic, so PUFs are well suited for them as well. These PUFs provide safety to silicon devices against IP theft, physical tempering, cloning or reverse engineering. They also protect silicon devices against hardware Trojan attacks and fault injections [10,78-83].

Silicon PUFs are of numerous types, such as Arbiter PUF, Butterfly PUF, Ring Oscillator PUF, etc. Some of them are more suitable to be implemented in ASICs, while others suit FPGAs better. One of the most efficient and FPGA-friendly silicon-based PUFs is the Ring Oscillator PUF (ROPUF) [84-86]. Like all other PUFs, ROPUFs exploit the manufacturing process variations of ASICs and FPGAs. This results in very minute differences in routing path delays and can be measured by the frequencies being produced by each of the ring oscillators employed in the development of the ROPUF. These ring oscillators oscillate uniquely. Therefore, a unique frequency is produced by each RO due to the manufacturing process variations [87-89]. Each of these RO pairs, which are placed randomly at different locations of an FPGA, produce their respective frequencies (f_1 and f_2). These frequencies are selected by their respective multiplexer by applying PUF challenge bits on its selected line. The output of these multiplexers (f_1 and f_2) are fed to counters, and subsequently to a comparator whose output is the response. The response bit r_{12}. This r_{12} can be written in the form of an equation:

$$r_{12} = \begin{cases} 1, & f_1 \geq f_2 \\ 0, & f_1 < f_2 \end{cases} \tag{4-1}$$

As opposed to an Arbiter-based design, the ROPUF approach is less influenced by routing skew. However, it should be noted that the frequencies produced by ring oscillators are more susceptible to external factors such as temperature, voltage, and aging [90]. These factors alter the propagation delays of oscillators resulting in alteration of frequency responses and ultimately altering the response bit generation of that particular ROPUF. There are multiple variations possible in the architecture of ROPUFs, like the use of the AND or the NAND gates in the design, or the number of gates (referred to as stages), which may affect the performance of ROPUFs. Due to these variations, the most effective stage and architecture-wise ROPUF must be selected as a standard for further investigations [91-92]. This can be done by implementing different stage ROPUFs and testing them against multiple factors like temperature variation, voltage variation, and accelerated aging with voltage variation [93-96].

Cryptography, a significant application of ROPUFs, is highly dependent upon the secret key generated with the help of the bit-sequence generated by the ROPUF. This secret key generation should be of utmost reliability and reproducible under all environmental conditions. Any encrypted system requires a secret key at both the encryption and decryption ends. If there is a mismatch at either end, the message gets distorted and illegible [97-99].

As PUFs can be implemented in secure systems like military equipment, space equipment, and many other critical systems; they may face harsh environmental conditions. These environmental conditions, like extreme temperatures and voltage variations or aging effects, may lead to temporary or permanent performance degradation and lower reliability. Therefore, we must know firsthand the performance of the proposed design in conditions like extreme temperature conditions, unstable power supply, or aged systems with unstable power supply [100].

It is recommended that PUFs be robust against temporal changes occurring in the chip due to environmental conditions or aging; temporal variations directly affect the frequency of the ring oscillator. These variations are split into two types: reversible and irreversible variations. Because temperature and voltage variations temporarily change the circuit's behavior, they lie in reversible variations. On the other hand, long-term exposure to extreme environmental conditions may lead to irreversible variability [99-101].

The aging of ASICs/FPGAs may also lead to irreversible variability. Aging within an ASIC or a FPGA could be of three types: hot carrier injection (HCI), charge trapping in a dielectric, and oxide breakdown (traps). In this chapter, the aging is simulated through the prolonged and continuous operation of FPGAs while varying their voltages. Temperature and voltage variations are tested separately for three different stages of the ROPUF.

In this chapter, the contributions are as follows:

- Detailed analysis of PUF metrics in temperature variations as well as voltage variations where the temperature range was from -70°C to 75°C while the voltage range was from 0.9 V to 1.05 V.
- A unique analysis is performed and named "hybrid reversible and irreversible temporal variations," in which aging that is irreversible variations is combined with reversible voltage variations.

4.2 Experimental Set-Up

The current work is an extension of our earlier work presented in chapter 3. In the aforementioned chapter, the performance analysis of an AND-Inverter based ROPUF was carried out. However, the impact of changes in environmental conditions on the performance of the ROPUF was not studied. The layouts of ROPUFs for each of the three different stages, used in our study, are shown in Figure 3-1. The stage of the ROPUF is defined by the number of inverters inherent in its circuitry. Thus, a 3-stage ROPUF has three inverters, a 5-stage has five inverters, and a 7-stage has seven inverters.

In order to study the effects of temperature variations, voltage variations, and aging with voltage variations on the performance of the ROPUF, multiple experiments on each of the three different configurations of the ROPUF are performed. The Artix-7 FPGA that comes with the NEXYS4 development board is used. The results are compiled and explained in the next section.

4.2.1 Temperature variations

ASICs and FPGAs are used in embedded and industrial systems where they may undergo extreme temperature conditions (i.e., space probes, land or air-based military vehicles). Therefore, it is necessary to observe temperature variation effects on these devices in terms of hardware security measures. In the temperature variation experiment, the ROPUF is placed in a temperature chamber and a logic analyzer is used to record its frequency response. The experiment is performed at -70°C, -60°C, -50°C, -40°C, -30°C, -20°C, -10°C, 0°C, 10°C, 21°C (room temperature), 25°C, 30°C, 40°C, 50°C, 70°C, and 75°C. A total of ten NEXSYS4 FPGA boards are used in this experiment. Figure 4-1 shows the temperature variation experimental setup. A 1000 series Test-Equity temperature chamber is used for recording and applying different temperatures, and an Agilent 16801A logic analyzer is used for recording the frequencies.

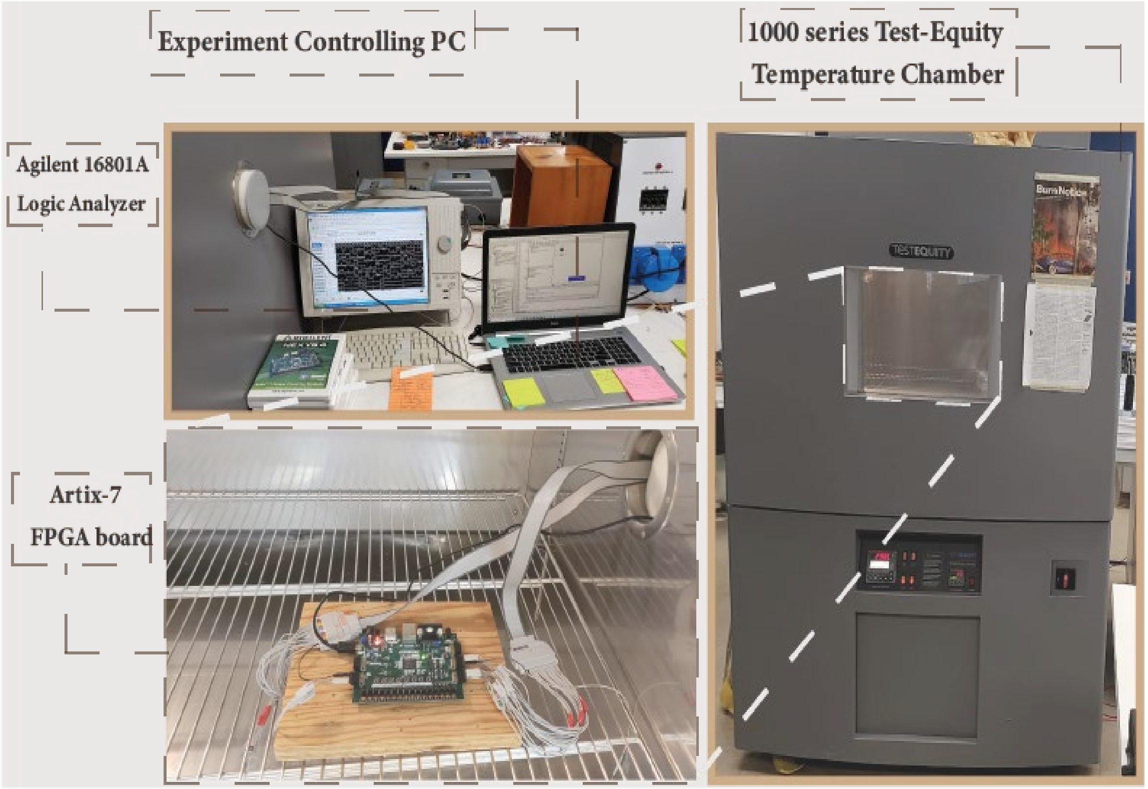

Experiment Controlling PC
1000 series Test-Equity Temperature Chamber
Agilent 16801A Logic Analyzer
Artix-7 FPGA board

Figure 4-1: Experimental setup for temperature variation experiment.

4.2.2 Voltage Variations

Temperature, humidity, and numerous other factors may lead to an unstable or fluctuating current in ICs, especially in a remote environment with limited resources. Therefore, it is necessary to study the effects of voltage variations on hardware security measures. Variations in the voltage supply may lead to deviation in the frequency response of a ROPUF. In order to study the deviation in the frequency response, various voltages are applied to the ROPUF, and the responses are recorded.

In this voltage variations experiment, the voltage supply for I/O banks (V_{CCO}) and the voltage supply for auxiliary logic (V_{CCAUX}) are fixed to 3.3 V and 1.8 V, respectively, while the voltage supply for the internal core logic (V_{CCINT}) is varied to study the change in behavior of the ROPUF [102]. Figure 4-2 shows the setup for performing the voltage variation experiment. It is important to note that the voltage is supplied from a power supply instead of the USB port. Figure 4-3 shows the points where these voltages are applied on the board.

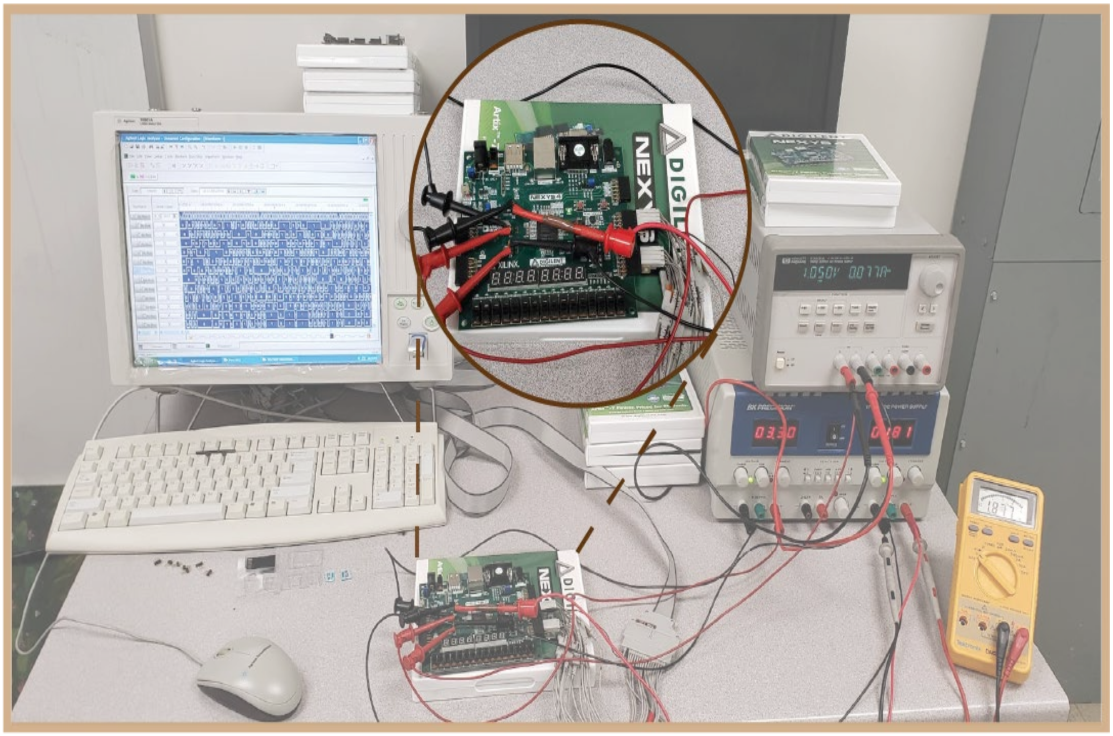


Figure 4-2: Experimental setup for voltage variations experiment.

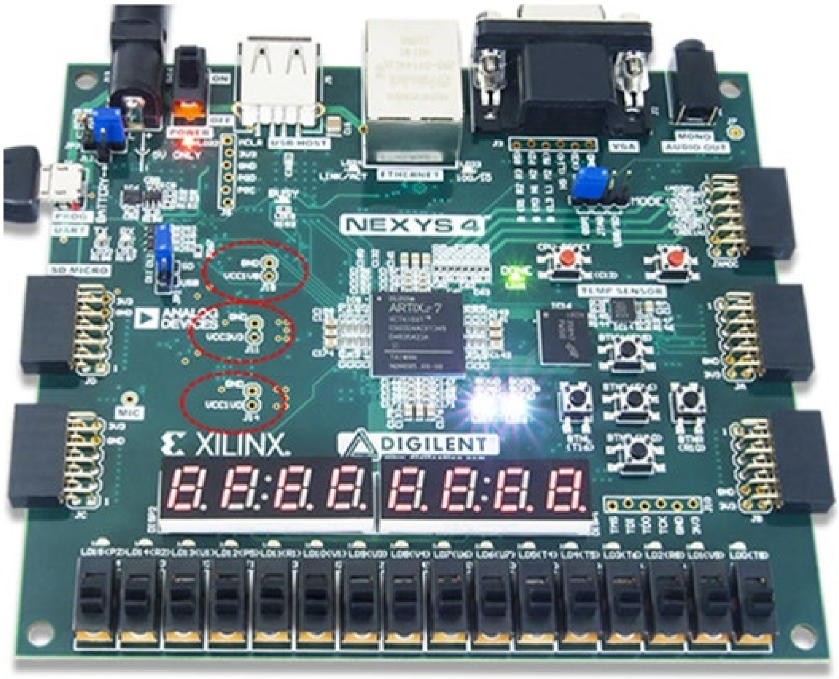


Figure 4-3: Nexys-4 Board with voltage supply points circled in red.

These voltage ranges are divided into equal interval voltages within the recommended range. For example, the V_{CCINT} is applied for the following values: 0.95 V, 0.975 V, 1.0 V, 1.025 V, and 1.05 V.

4.2.3 Aging with Voltage Variations

In this section, the experimental set-up for studying the impact of aging with changes in voltages is described. In this experiment, the ROPUFs are programmed on the 10 different FPGA boards and powered continuously for 30 days. The frequency responses of the ROPUFs are measured every five days for varying voltages. The following voltages are applied: 0.95 V, 0.975 V, 1.0 V, 1.025 V, and 1.05 V. After performing this experiment for the 3-stage ROPUF, the experiment is repeated for the 5 and 7 stage ROPUFs. The range of voltage variation in this experiment is similar to the one as in the previous experiment. This experiment is helpful in studying the aging effects on the performance of the ROPUF as the voltage is varied. Figure 4-4 shows the setup for the aging with voltage variations experiment.

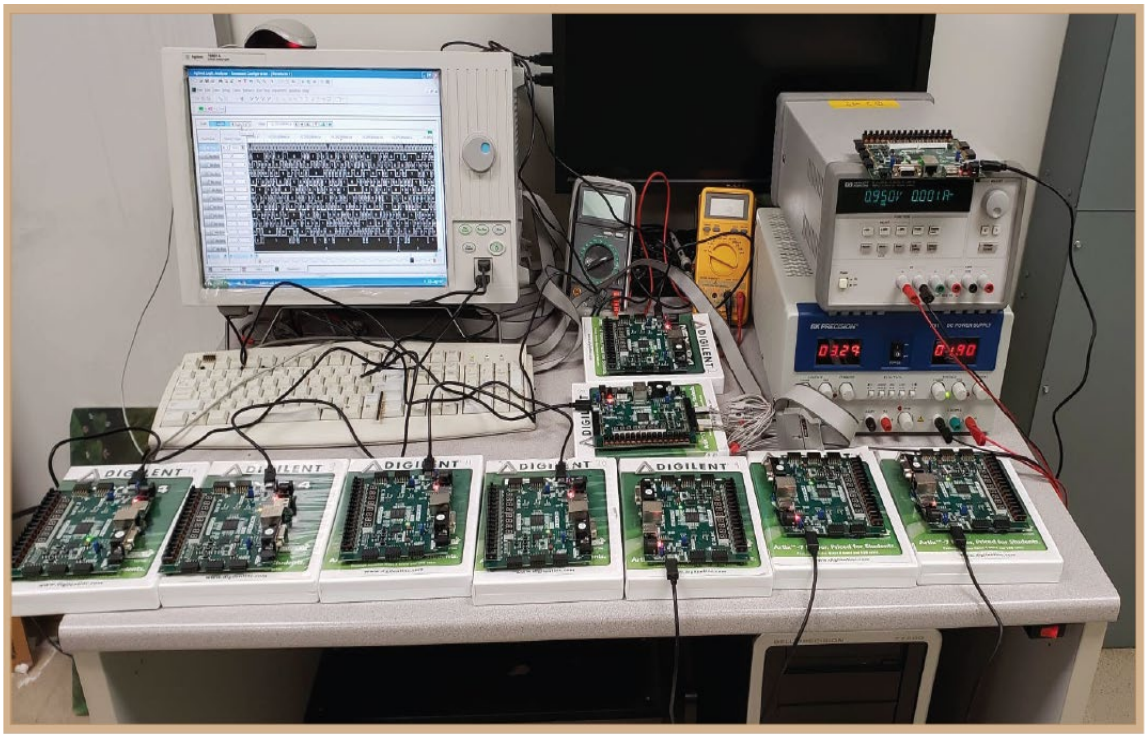


Figure 4-4: Experimental setup for aging with voltage variations experiment.

4.3 Experimental Results

In this section, the experimental results are divided in three sections: temperature variations, voltage variations, and aging with voltage variations. The performance is measured for the commonly used PUF metrics such as uniformity, reliability, bit-aliasing, and uniqueness.

The randomness of the response sequence is evaluated using a statistical test suite SP800-22 from the National Institute of Standards and Technology (NIST). This is a widely used test suite for analyzing randomness of a binary sequence of numbers [103].

The results of the tests for the frequency response of the ROPUFs are shown in Table 4-1. A total number of 100 response sequences from the output of the ROPUF is analyzed where each sequence is comprised of 256 random bits. The test outputs show promising results. It is to be noted that all p-values are larger than 0.0001, which implies that all responses are random. [70, 103-104]. Therefore, the AND-Inverter based ROPUF successfully passes the NIST randomness tests.

Table 4.1: NIST statistical test suite.

Test Methods	**No. of Sequence**	**Length**	**3-Stages**	**5-Stages**	**7-Stages**	**Result**
			P-Value	**P-Value**	**P-Value**	
Frequency Test (Monobit)	100	256 bits	0.53197	0.80258	0.53197	Random
Frequency Test within a Block	100	256 bits	0.56094	0.85534	0.81617	Random
Longest Run of Ones in a Block	100	256 bits	0.05812	0.28750	0.00927	Random
Discrete Fourier Transform (Spectral)	100	256 bits	0.73075	0.35879	0.13590	Random
Non-Overlapping Template Matching	100	256 bits	0.99998	0.99998	0.99998	Random
Serial test	100	256 bits	0.84134	0.15865	0.84134	Random
Approximate Entropy	100	256 bits	1.0	1.0	1.0	Random
Cummulative Sums (Forward)	100	256 bits	0.74584	0.99084	0.62922	Random
Cummulative Sums (Reverse)	100	256 bits	0.85796	0.90638	0.85796	Random
Random Excursions	100	256 bits	0.96256	0.79963	0.92576	Random
Random Excursions Variant	100	256 bits	0.78926	0.322291	0.34278	Random

4.3.1 Temperature Variations

The temperature variation experiment was performed using 10 FPGAs for fifteen different temperatures. These 10 FPGAs were programmed for the 3-stage, 5-stage, and 7-stage ROPUFs, in order to observe and compare the PUF metrics of each stage. Each ROPUF's uniformity, reliability, bit-aliasing, and uniqueness are shown in Figure 4-5 (a-d) for varied operating temperatures. The results show that the ROPUF parameters improve for all ROPUF configurations with the increase of temperature. This is due to the increase in path delay with the increase in temperature [105].

The uniformity at -70°C are 48.87%, 45.17%, and 47.44% for the 3-stage, 5-stage, and 7-stage respectively. At room temperature, the uniformity stays at 50.82%, 48.24%, and 50.07%. However, when the temperature reaches 75°C, the 3-stage uniformity approaches the optimal value (50.24%), while the 5-stage and 7-stage uniformity increases slightly (51.39% and 53.13%, respectively). Comparing these results with the bit-aliasing metrics results at -70°C, room temperature and 75°C, it can be observed that their values for the 3 different stages are relatively comparable with each other. For instance, at room temperature the results are 50.04%, 48.25%, and 50.07% for the 3-stage, 5-stage, and 7-stage respectively. Similarly, when the temperature exceeds 75°C, the bit-aliasing of the different stages increases to 50.24%, 51.38%, and 53.12%, respectively. As the temperature rises, the uniformity and bit-aliasing as shown in Figure 4-5 (a) and (c) steadily improve.

In terms of reliability, at -70°C the results for the 3 different stages are 93.66%, 90.14%, and 92.56% progressively. However, at room temperature the reliability remained at 95.77%, 95.45%, and 94.80% respectively. When the temperature rises above 75°C, the reliability of the different stages are 97.31%, 96.78%, and 96.48% respectively. As illustrated in Figure 4-5 (b), there is a clear trend of increased reliability as the temperature increases.

In case of uniqueness at -70°C, the values are 44.39%, 39.54%, and 42.11% for the different stages. At room temperature, the uniqueness maintains at 47.50%, 43.55%, and 45.27%, respectively. When the temperature approaches 75°C, the measure of uniqueness increases to 47.85%, 45.11%, and 47.09 %, respectively. As represented in Figure 4-5 (d), there is a clear trend toward better uniqueness as the temperature increases. From the different configurations of the ROPUF, it can be noticed that the three-stage ROPUF appears to operate better in various temperature settings than the five-stage and seven-stage ROPUFs. Tables 4-2, 4-3, and 4-4 summarize the results of temperature variations for the 3, 5, and 7 stages, respectively.

Table 4.2: Temperature variations for 3 Stage ROPUF.

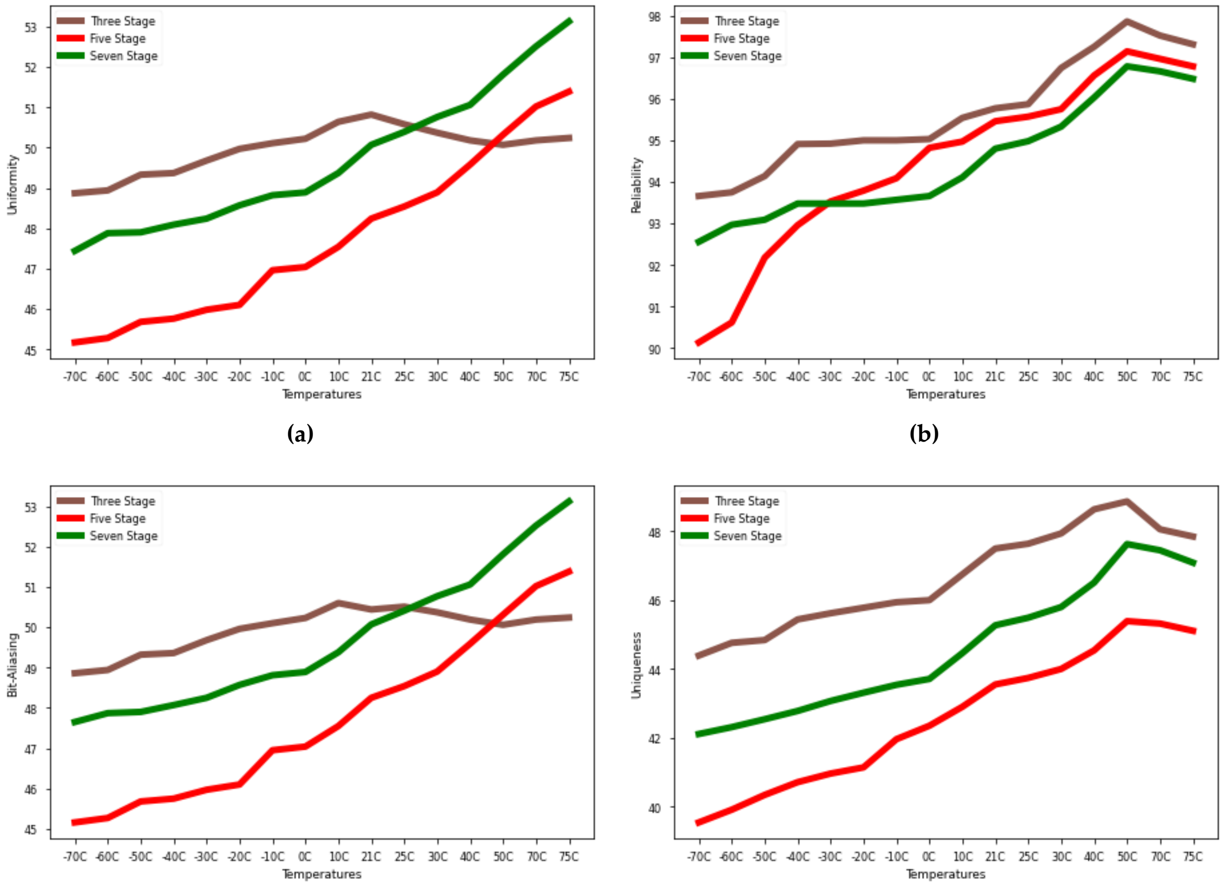
Metrics	**Ideal value**	**-70°C Min**	**-60° C**	**-50° C**	**-40° C**	**-30° C**	**-20° C**	**-10° C**	**0° C**	**10° C**	**21° C RT**	**25° C**	**30° C**	**40° C**	**50° C**	**70° C**	**75°C Max**
Uniformity	50%	48.87	48.9	49.3	49.3	49.6	49.9	50.1	50.2	50.6	50.8	50.5	50.3	50.1	50	50.1	50.24
Reliability	100%	93.66	93.7	94.1	94.9	94.9	95	95	95.0	95.5	95.7	95.8	96.7	97.2	97.8	97.5	97.31
Bit-Aliasing	50%	48.86	48.9	49.3	49.3	49.6	49.9	50.1	50.2	50.6	50.0	50.5	50.3	50.1	50.0	50.1	50.24
Uniqueness	50%	44.39	44.7	44.8	45.4	45.6	45.7	45.9	46	46.7	47.5	47.6	47.9	48.6	48.8	48.0	47.85
Standard Deviation of Frequency	X	5.45 MHz	6.65 MHz	7.9 MHz	8.93 MHz	9.32 MHz	9.65 MHz	10.0 MHz	10.2 MHz	10.2 MHz	10.3 MHz	13.5 MHz	15.7 MHz	15.9 MHz	14.3 MHz	17.4 MHz	18.43 MHz

Table 4.3: Temperature variations for 5 Stages ROPUF.

Metrics	**Ideal value**	**-70°C Min**	**-60° C**	**-50° C**	**-40° C**	**-30° C**	**-20° C**	**-10° C**	**0° C**	**10° C**	**21° C RT**	**25° C**	**30° C**	**40° C**	**50° C**	**70° C**	**75°C Max**
Uniformity	50%	45.17	45.2	45.6	45.7	45.9	46.1	46.9	47.0	47.5	48.2	48.5	48.8	49.5	50.3	51.0	51.39
Reliability	100%	90.14	90.6	92.1	92.9	93.5	93.7	94.0	94.8	94.9	95.4	95.5	95.7	96.5	97.1	96.9	96.78
Bit-Aliasing	50%	45.16	45.2	45.6	45.7	45.9	46.1	46.9	47.0	47.5	48.2	48.5	48.9	49.5	50.3	51.0	51.38
Uniqueness	50%	39.54	39.9	40.3	40.7	40.9	41.1	41.9	42.3	42.9	43.5	43.7	44	44.5	45.3	45.3	45.11
Standard Deviation of Frequency	X	2.35 MHz	3.6 MHz	3.79 MHz	4.76 MHz	6.1 MHz	6.41 MHz	6.74 MHz	7.48 MHz	8.33 MHz	9.21 MHz	10.1 MHz	11.1 MHz	12.5 MHz	13.9 MHz	13.9 MHz	14.43 MHz

Table 4.4: Temperature variations for 7 Stages ROPUF.

Metrics	Ideal value	-70°C Min	-60° C	-50° C	-40° C	-30° C	-20° C	-10° C	0° C	10° C	21° C RT	25° C	30° C	40° C	50° C	70° C	75°C Max
Uniformity	50%	47.44	47.8	47.9	48.0	48.2	48.5	48.8	48.8	49.3	50.0	50.3	50.7	51.0	51.8	52.5	53.13
Reliability	100%	92.56	92.9	93.0	93.4	93.4	93.4	93.5	93.6	94.1	94.8	94.9	95.3	96.0	96.7	96.6	96.48
Bit-Aliasing	50%	47.65	47.8	47.9	48.0	48.2	48.5	48.8	48.8	49.3	50.0	50.4	50.7	51.0	51.8	52.5	53.12
Uniqueness	50%	42.11	42.3	42.5	42.7	43.0	43.3	43.5	43.7	44.4	45.2	45.4	45.8	46.5	47.6	47.4	47.09
Standard Deviation of Frequency	X	1.75 MHz	2.50 MHz	3.91 MHz	5.05 MHz	6.08 MHz	6.47 MHz	6.74 MHz	7.19 MHz	7.78 MHz	8.37 MHz	8.90 MHz	9.35 MHz	9.99 MHz	10.6 MHz	11.4 MHz	12.27 MHz



(a)

(b)

(c)

(d)

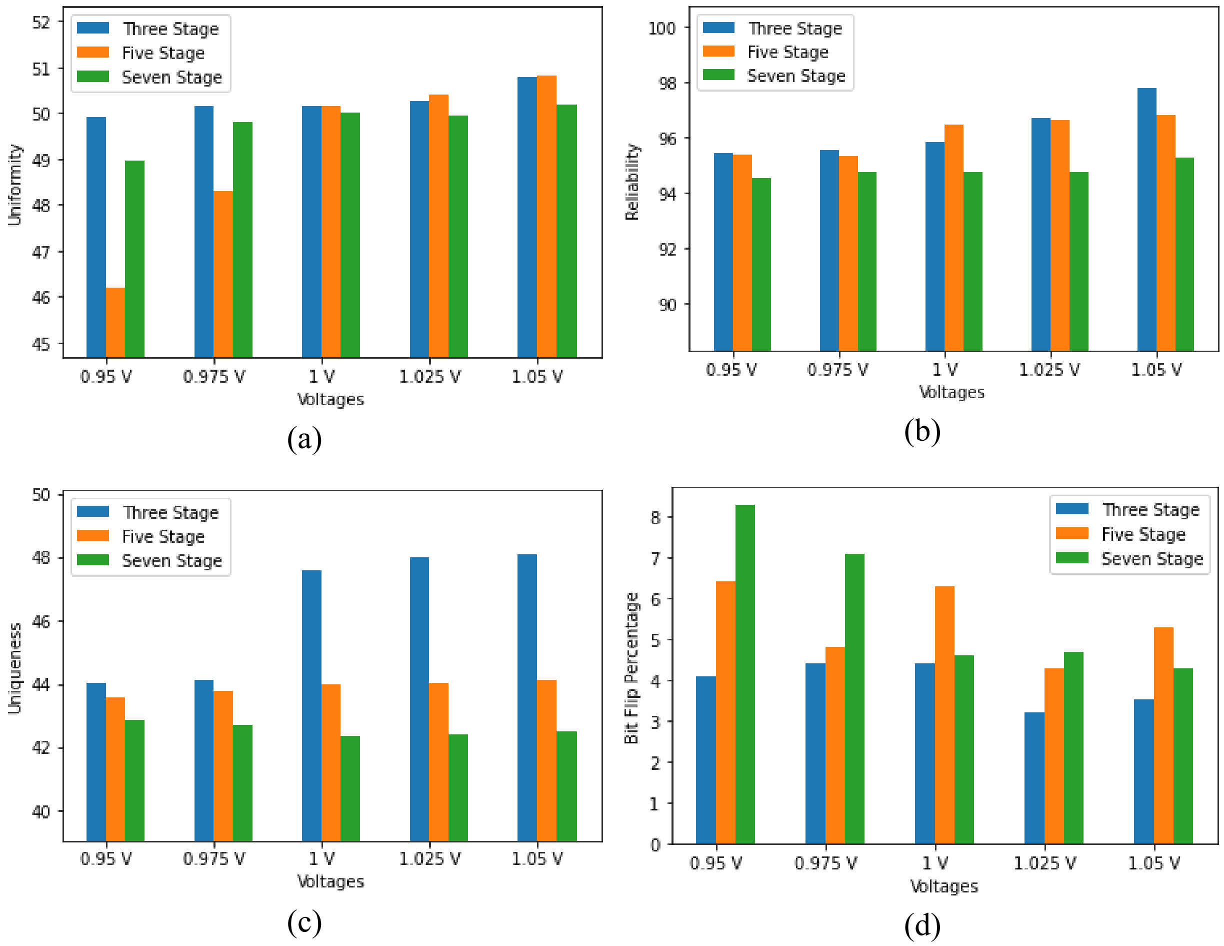
Figure 4-5: Environmental impact on the ROPUF for ten different temperatures: (a) Uniformity; (b) Reliability; (c) Bit-Aliasing; (d) Uniqueness.

4.3.2 Voltage Variations

The voltage variation experiment is performed by varying V_{CCINT} within a range of 0.95 V and 1.05 V with an interval of 0.025 V. This gives us five voltage levels to perform our experiment on. This experiment is repeated thrice for each ROPUF configuration. Figure 4-6 (a-d) shows the uniformity, reliability, uniqueness, and bit-flips under different operating voltages for different stages. As seen in the figure, the parameters for different stage ROPUFs improve as the operating voltage increases in high voltage settings while it decreases in low voltage settings. The uniformity is lower for five and seven stage ROPUFs in low voltage settings. In terms of bit flip percentage, 0.95V has a higher bit flip occurrence than 1.025V. Also, the best reliability is obtained when all three ROPUF configurations are operating at 1.05V. Table 4-5 shows the voltage variations experiment results for three, five, and seven stages, respectively.

Table 4.5: Voltage variations results for three, five, and seven stages.

Metrics	Ideal value	3 Stages ROPUF					5 Stages ROPUF					7 Stages ROPUF				
		0.95 V	**0.975 V**	**1 V**	**1.025 V**	**1.05 V**	**0.95 V**	**0.975 V**	**1 V**	**1.025 V**	**1.05 V**	**0.95 V**	**0.975 V**	**1 V**	**1.025 V**	**1.05 V**
Uniformity	50%	49.9	50.1	50.1	50.2	50.8	46.1	48.3	50.1	50.3	50.8	48.9	49.7	50	49.9	50.1
Reliability	100%	95.4	95.5	95.8	96.7	97.7	95.3	95.3	96.4	96.6	96.8	94.5	94.7	94.7	94.7	95.2
Bit-Aliasing	50%	49.9	50.1	50.1	50.2	50.7	46.1	48.2	50.1	50.3	50.8	48.9	49.7	50.0	49.9	50.1
Uniqueness	50%	44	44.1	47.6	47.9	48.1	43.5	43.7	43.9	44.0	44.1	42.8	42.6	42.3	42.4	42.5
Standard Deviation of Frequency	X	1.68 MHz	13.4 MHz	11.9 MHz	16.1 MHz	17.1 MHz	0.85 MHz	1.08 MHz	5.47 MHz	1.8 MHz	2.02 MHz	0.88 MHz	0.58 MHz	0.59 MHz	7.85 MHz	9.84 MHz



(a)

(b)

(c)

(d)

Figure 4-6: Environmental impact on the ROPUF for five different voltages: (a) Uniformity; (b) Reliability; (c) Uniqueness; (d) Bit Flip.

4.3.3 Aging with Voltage Variations

The experiment in which we have studied the impact of both aging and voltage variations simultaneously is presented in this section. Here, the FPGAs are run for 30 consecutive days, and the responses are recorded on every fifth day while varying the voltage of the FPGA boards. Thus, we are able to observe the aging effects on ROPUF due to prolonged operation as well as detrition in results from non-aged voltage variation.

The tables below show the results for each reading:

Table 4.6: Aging with voltage variation results at Day 1.

Metrics	**Ideal value**	**3 Stages ROPUF**					**5 Stages ROPUF**					**7 Stages ROPUF**				
		0.95 V	**0.975 V**	**1 V**	**1.025 V**	**1.05 V**	**0.95 V**	**0.975 V**	**1 V**	**1.025 V**	**1.05 V**	**0.95 V**	**0.975 V**	**1 V**	**1.02 5V**	**1.05 V**
Uniformity	50%	49.9	50.1	50.1	50.2	50.8	46.1	48.3	50.1	50.3	50.8	48.9	49.7	50	49.9	50.1
Reliability	100%	95.4	95.5	95.8	96.7	97.7	95.3	95.4	96.3	96.6	96.8	94.5	94.7	94.7	94.7	95.2
Bit-Aliasing	50%	49.9	50.1	50.1	50.2	50.7	46.1	48.2	50.1	50.3	50.8	48.9	49.7	50	49.9	50.1
Uniqueness	50%	44.0	44.1	47.6	47.9	48.1	43.5	43.7	43.9	44.0	44.1	42.8	42.6	42.3	42.4	42.5
Standard Deviation of Frequency	X	1.6 MHz	13.4 MHz	11.9 MHz	16.1 MHz	17.1 MHz	0.8 MHz	1.08 MHz	5.4 MHz	1.8 MHz	2.02 MHz	0.8 MHz	0.5 MHz	0.5 MHz	7.8 MHz	9.8 MHz

Table 4.7: Aging with voltage variation results at Day 5.

Metrics	**Ideal value**	**3 Stages ROPUF**					**5 Stages ROPUF**					**7 Stages ROPUF**				
		0.95 V	**0.975 V**	**1 V**	**1.025 V**	**1.05 V**	**0.95 V**	**0.975 V**	**1 V**	**1.025 V**	**1.05 V**	**0.95 V**	**0.975 V**	**1 V**	**1.02 5V**	**1.05 V**
Uniformity	50%	49.8	49.9	49.9	50.1	50.2	49.1	50.8	50.9	51.2	50.3	49.7	49.7	50.2	50.1	49.8
Reliability	100%	95.4	95.5	95.5	96.4	97.1	95.6	95.9	96.1	96.4	96.8	95.0	95.1	95.2	95.2	95.1
Bit-Aliasing	50%	49.8	49.8	49.9	50.1	50.2	49.1	50.8	50.9	51.2	50.3	49.7	49.7	50.2	50.1	49.8
Uniqueness	50%	43.1	43.4	43.6	44.4	45.7	43.3	43.1	42.9	42.7	42.4	42.4	42.1	41.9	41.4	41.4
Standard Deviation of Frequency	X	1.6 MHz	1.7 MHz	1.8 MHz	1.8 MHz	1.9 MHz	1.5 MHz	1.6 MHz	1.6 MHz	1.7 MHz	1.7 MHz	1.3 MHz	13.9 MHz	15.4 MHz	15.1 MHz	15.9 MHz

Table 4.8: Aging with voltage variation results at Day 10.

Metrics	**Ideal value**	**3 Stages ROPUF**					**5 Stages ROPUF**					**7 Stages ROPUF**				
		0.95 V	**0.975 V**	**1 V**	**1.025 V**	**1.05 V**	**0.95 V**	**0.975 V**	**1 V**	**1.025 V**	**1.05 V**	**0.95 V**	**0.975 V**	**1 V**	**1.025V**	**1.05 V**
Uniformity	50%	50.2	49.9	50.1	50	50.1	50.3	50.3	50	50.2	50.7	50.2	50.1	49.8	50	50.2
Reliability	100%	96.1	96.1	96.2	96.5	97.5	95.1	95.5	95.5	96.1	97.1	95.1	94.9	95.2	95.2	95.5
Bit-Aliasing	50%	50.2	49.9	50.1	50	50.1	50.3	50.3	49.9	50.2	50.7	50.2	50.1	49.8	49.9	50.2
Uniqueness	50%	43.6	44.8	45.1	47.3	49.1	43.1	43.3	43.3	43.2	43.1	41.6	41.4	41.1	40.9	40.8
Standard Deviation of Frequency	X	1.6 MHz	1.7 MHz	1.8 MHz	1.7 MHz	1.9 MHz	1.5 MHz	1.6 MHz	1.7 MHz	1.7 MHz	1.7 MHz	1.3 MHz	14.1 MHz	12.7 MHz	9.1 MHz	10.4 MHz

Table 4.9: Aging with voltage variation results at Day 15.

Metrics	**Ideal value**	**3 Stages ROPUF**					**5 Stages ROPUF**					**7 Stages ROPUF**				
		0.95 V	**0.975 V**	**1 V**	**1.025 V**	**1.05 V**	**0.95 V**	**0.975 V**	**1 V**	**1.025 V**	**1.05 V**	**0.95 V**	**0.975 V**	**1 V**	**1.025V**	**1.05 V**
Uniformity	50%	49.9	50.2	50.3	50	49.9	50.2	49.7	50.5	50.1	50.7	50.2	50.2	50.1	50	49.7
Reliability	100%	95.8	95.8	96.8	97.1	97.1	96.3	96.3	96.3	96.7	96.7	94.4	94.4	95.1	95.2	95.2
Bit-Aliasing	50%	49.9	50.2	50.3	50	49.9	50.2	49.7	50.5	50.1	50.7	50.2	50.2	50.1	49.9	49.7
Uniqueness	50%	44.1	44.1	44.5	44.9	45.2	42.9	43	43	43	43.1	42.9	42.7	42.1	41.6	41.4
Standard Deviation of Frequency	X	1.6 MHz	1.7 MHz	1.8 MHz	1.7 MHz	1.9 MHz	1.5 MHz	1.6 MHz	1.6 MHz	1.72 MHz	1.7 MHz	11.3 MHz	14.5 MHz	10.2 MHz	10.4 MHz	10.4 MHz

Table 4.10: Aging with voltage variation results at Day 20.

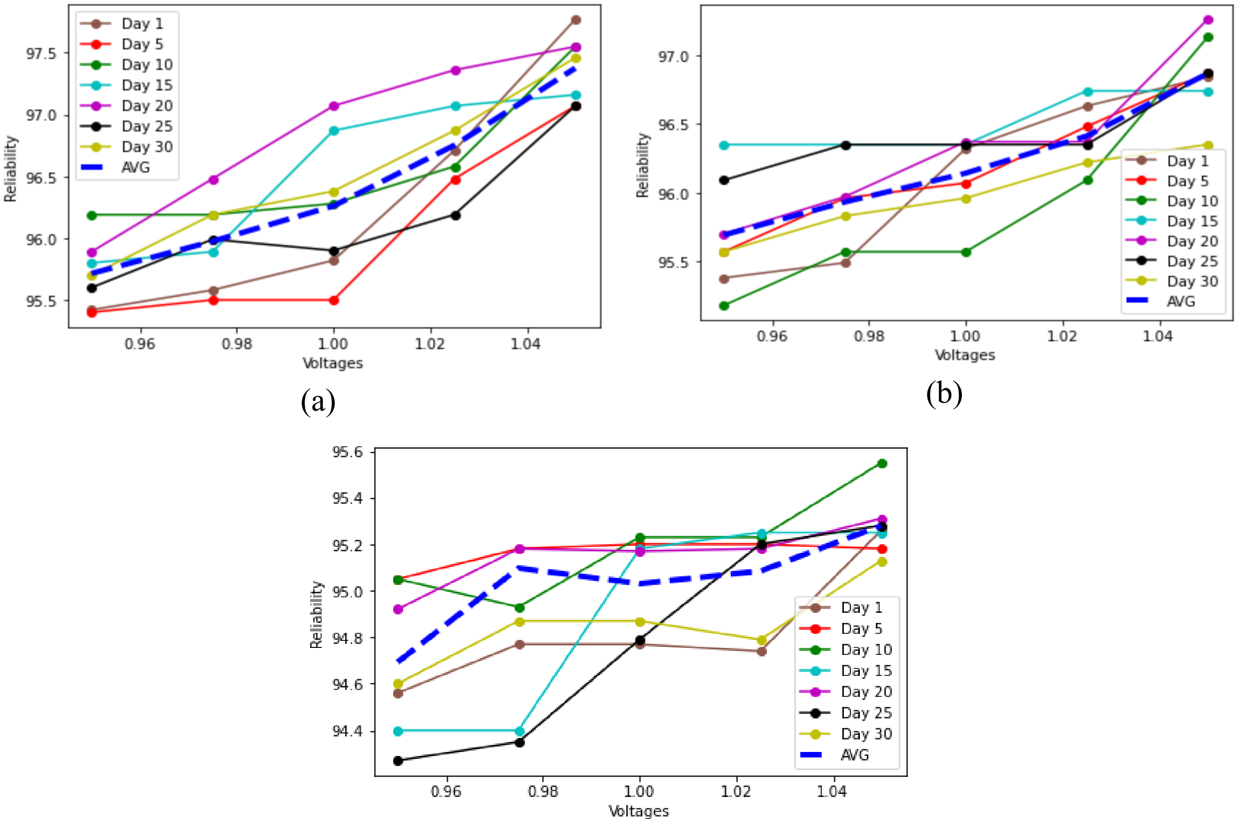
Metrics	Ideal value	3 Stages ROPUF					5 Stages ROPUF					7 Stages ROPUF				
		0.95 V	**0.975 V**	**1 V**	**1.025 V**	**1.05 V**	**0.95 V**	**0.975 V**	**1 V**	**1.025 V**	**1.05 V**	**0.95 V**	**0.975 V**	**1 V**	**1.025V**	**1.05 V**
Uniformity	50%	50.2	50.3	50.2	50.1	50.1	50.2	49.8	50.2	50.9	50.5	50.7	50.3	50.2	50.1	50.1
Reliability	100%	95.8	96.4	97.1	97.3	97.5	95.7	95.9	96.3	96.3	97.2	94.9	95.1	95.1	95.1	95.3
Bit-Aliasing	50%	50.2	50.3	50.2	50.1	50.1	50.2	49.8	50.2	50.9	50.5	50.7	50.3	50.2	50.1	50.1
Uniqueness	50%	43.6	44.6	45	45.4	46.1	43.4	43.8	43.8	43.7	43.5	42.1	42.4	41.6	41.9	41.8
Standard Deviation of Frequency	X	1.6 MHz	1.7 MHz	1.7 MHz	1.8 MHz	1.7 MHz	1.5 MHz	1.6 MHz	1.6 MHz	1.7 MHz	1.7 MHz	11.1 MHz	11.9 MHz	9.4 MHz	10.3 MHz	10.4 MHz

Table 4.11: Aging with voltage variation results at Day 25.

Metrics	Ideal value	3 Stages ROPUF					5 Stages ROPUF					7 Stages ROPUF				
		0.95 V	**0.975 V**	**1 V**	**1.025 V**	**1.05 V**	**0.95 V**	**0.975 V**	**1 V**	**1.025 V**	**1.05 V**	**0.95 V**	**0.975 V**	**1 V**	**1.025V**	**1.05 V**
Uniformity	50%	50.1	50.1	49.9	50	50.1	50.3	50.2	50.3	50.7	50.6	50.3	50.3	50.3	50.6	50.2
Reliability	100%	95.6	95.9	95.9	96.1	97.1	96.1	96.3	96.3	96.3	96.8	94.2	96.3	94.7	95.2	95.2
Bit-Aliasing	50%	50.1	50.1	49.9	49.9	50.1	50.3	50.2	50.3	50.7	50.6	50.3	50.3	50.3	50.6	50.2
Uniqueness	50%	44.3	44	43.9	44.7	46.4	43.8	43.6	43.5	43.5	43.3	41.9	41.9	42.1	42.1	42.1
Standard Deviation of Frequency	X	1.7 MHz	1.7 MHz	1.7 MHz	1.8 MHz	1.9 MHz	1.5 MHz	1.6 MHz	1.6 MHz	1.7 MHz	1.7 MHz	13 MHz	11.5 MHz	14.5 MHz	10.3 MHz	10.4 MHz

Table 4.12: Aging with voltage variation results at Day 30.

Metrics	**Ideal value**	**3 Stages ROPUF**					**5 Stages ROPUF**					**7 Stages ROPUF**				
		0.95 V	**0.975 V**	**1 V**	**1.025 V**	**1.05 V**	**0.95 V**	**0.975 V**	**1 V**	**1.025 V**	**1.05 V**	**0.95 V**	**0.975 V**	**1 V**	**1.025V**	**1.05 V**
Uniformity	50%	50.1	50.1	50	50	50.1	50.7	50.3	50.3	51	51.6	50.9	50.7	49.8	50.1	50.2
Reliability	100%	95.7	96.19	96.3	96.8	97.4	95.5	95.8	95.9	96.2	96.3	94.6	94.8	94.8	94.7	95.1
Bit-Aliasing	50%	50.1	50.1	50	50	50.1	50.7	50.2	50.3	51	51.6	50.9	50.7	49.8	50.1	50.2
Uniqueness	50%	44.2	44.7	44.8	45.1	47.4	43.1	43	42.9	42.8	42.5	41.6	41.9	41.6	42.1	42.1
Standard Deviation of Frequency	X	1.6 MHz	1.7 MHz	1.8 MHz	1.8 MHz	1.9 MHz	1.5 MHz	1.6 MHz	1.7 MHz	1.7 MHz	1.8 MHz	10.2 MHz	1.4 MHz	13.1 MHz	10.3 MHz	10.4 MHz



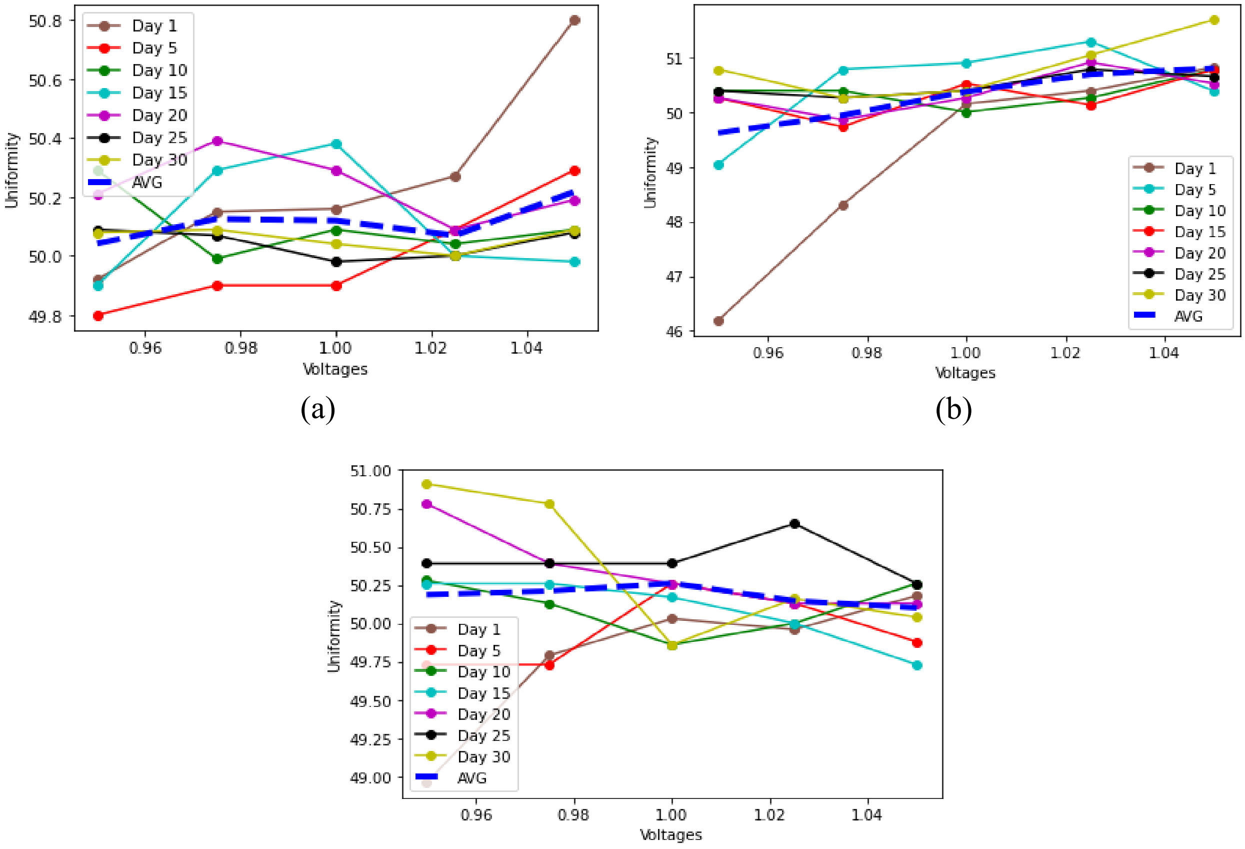
(a)

(b)

(c)

Figure 4-7: Reliability changes in ROs due to voltage variations: (a) Three stage; (b) Five stage; (c) Seven stage.

Figure 4-7 (a-c) represents the reliability for aging and voltage variations. From the figure, it is observed that the reliability for three stage and five stage ROPUFs increases with the increase in operating voltage; while the effect of voltage variation with aging in seven stage ROPUF stays minimum. The effect is maximum for three stage and minimum for 7 stage configurations. The maximum reliability obtained for different configurations are (95.77%, 97.22%, and 95.55% respectively).



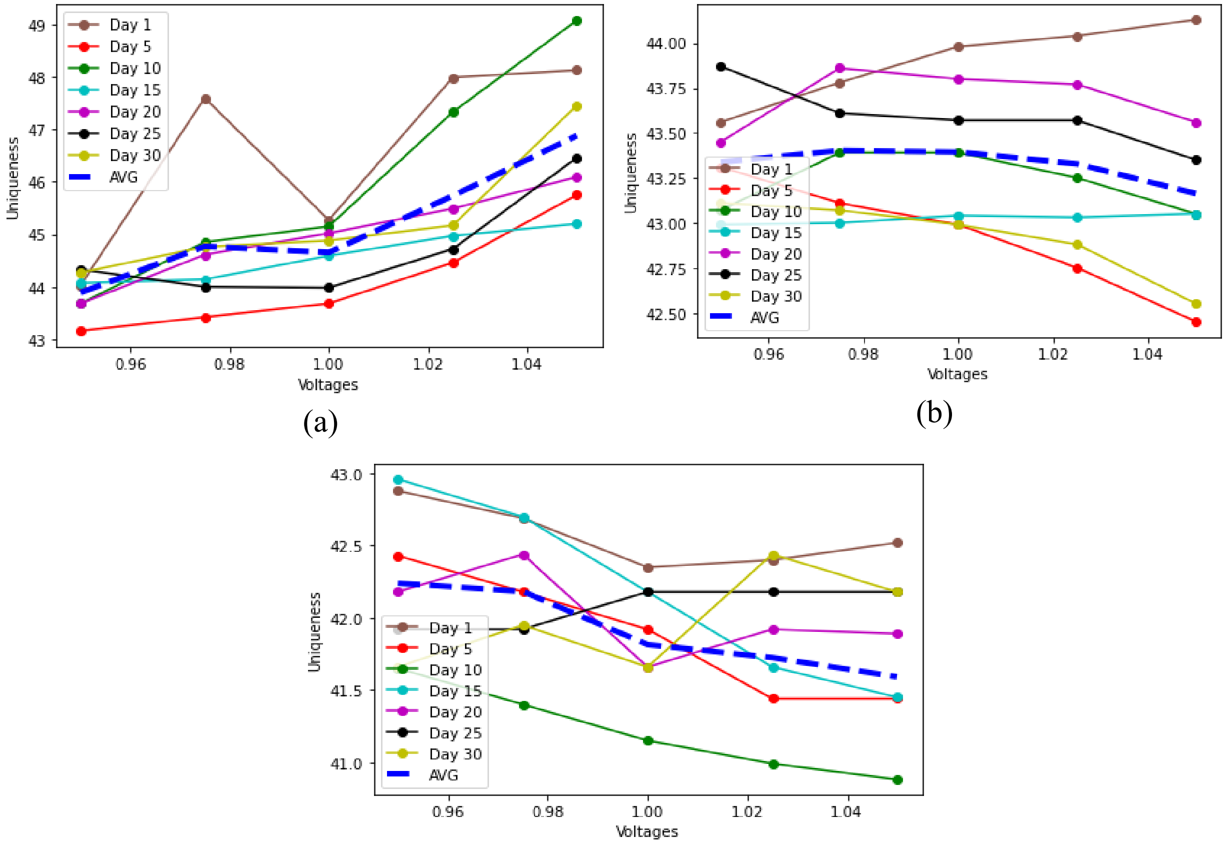
(a)

(b)

(c)

Figure 4-8: Uniformity changes in ROs due to voltage variations: (a) Three stage; (b) Five stage; (c) Seven stage.

Figure 4-8 (a-c) depicts the uniformity for aging and voltage variations. The figure shows that the uniformity for the three stage structure approaches the ideal value of 50% as there is an increase in operating voltage. In a five stage ROPUF, the uniformity increases with the increase in operating voltage, whereas the uniformity for a seven stage ROPUF approaches the ideal value.



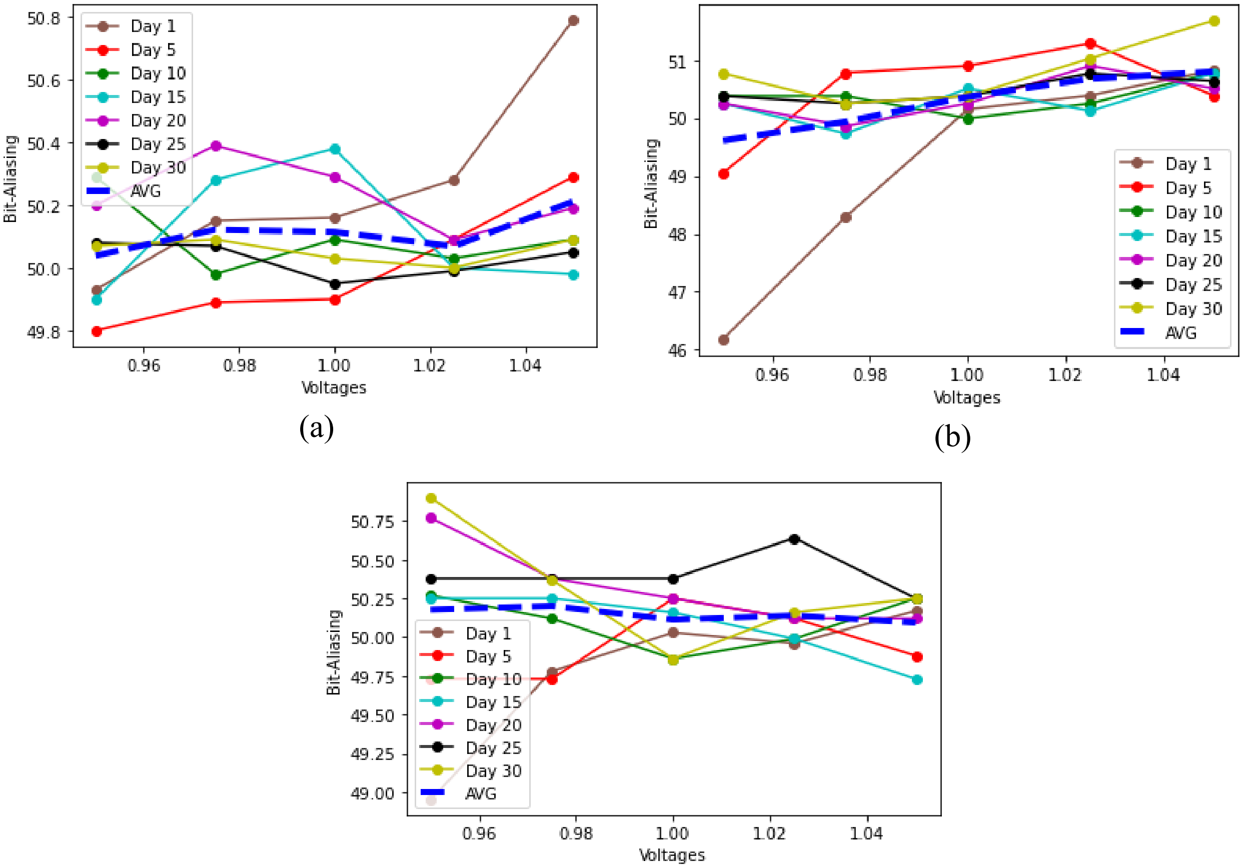
(a)

(b)

(c)

Figure 4-9: Uniqueness changes in ROs due to voltage variations: (a) Three stage; (b) Five stage; (c) Seven stage.

Figure 4.9 (a-c) depicts that the uniqueness of a three stage ROPUF improves against aging and voltage variations; while uniqueness for five stage and seven stage ROPUFs decreases considerably against a change in voltage. The uniqueness is higher in each voltage level but decreases with time.



(a)

(b)

(c)

Figure 4-10: Bit-aliasing changes in ROs due to voltage variations: (a) Three stage; (b) Five stage; (c) Seven stage.

Figure 4.10 (a-c) illustrates the bit-aliasing results for three stage, five stage, and seven stage ROPUFs against voltage variation with aging. The three stage bit-aliasing results converge towards the ideal value. Five stage bit-aliasing results increased slightly, and seven stage bit-aliasing results remained consistent, close to the ideal value.

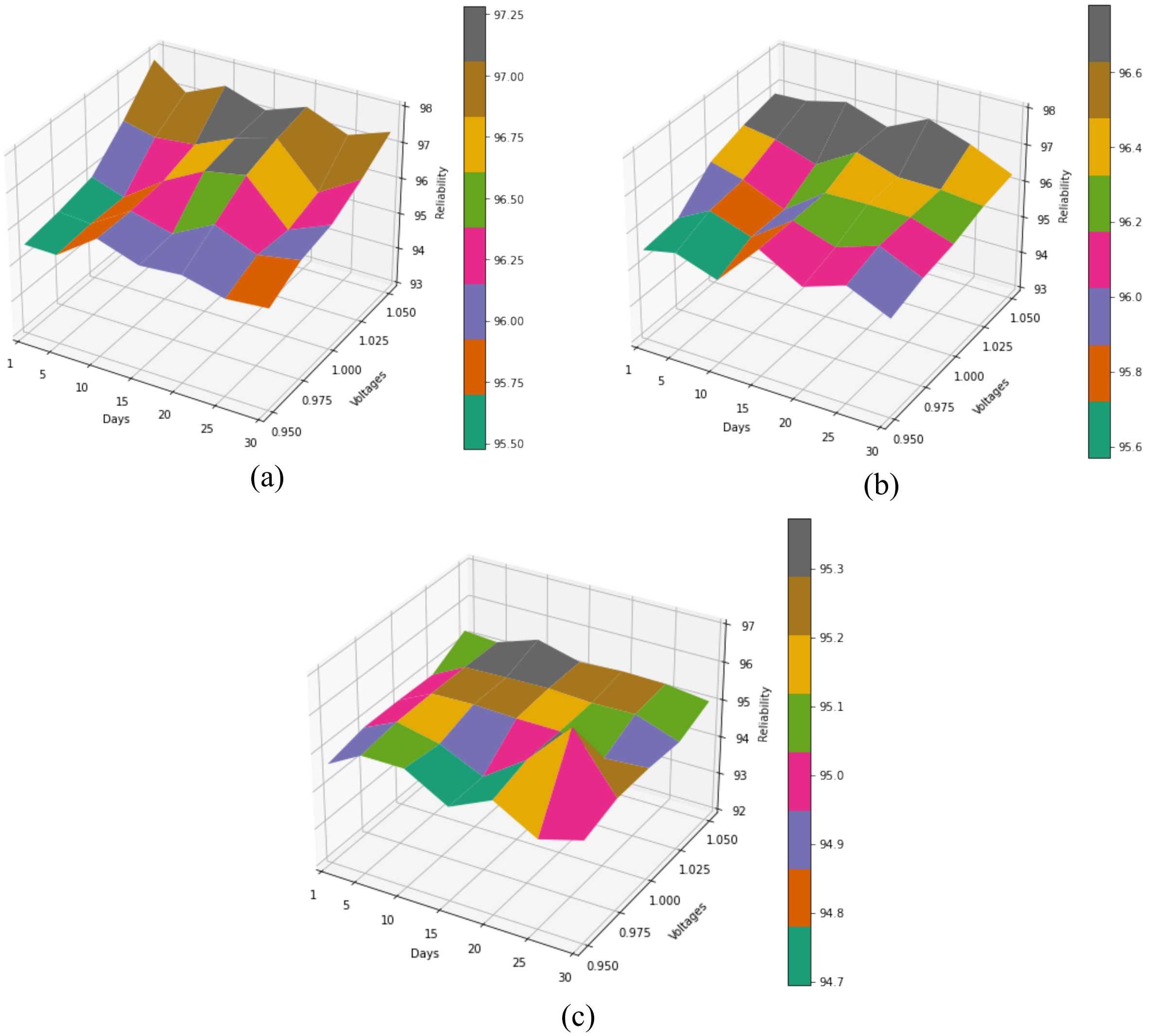


Figure 4-11: Reliability changes in ROs due to aging and voltage variations combined: (a) Three stage; (b) Five stage; (c) Seven stage.

Figure 4-11 (a-c) represents the reliability with aging and voltage variations. From the Figure, it is observed that there is an aging effect in low voltage for each configuration, and the effect of aging is minimal in higher voltage.

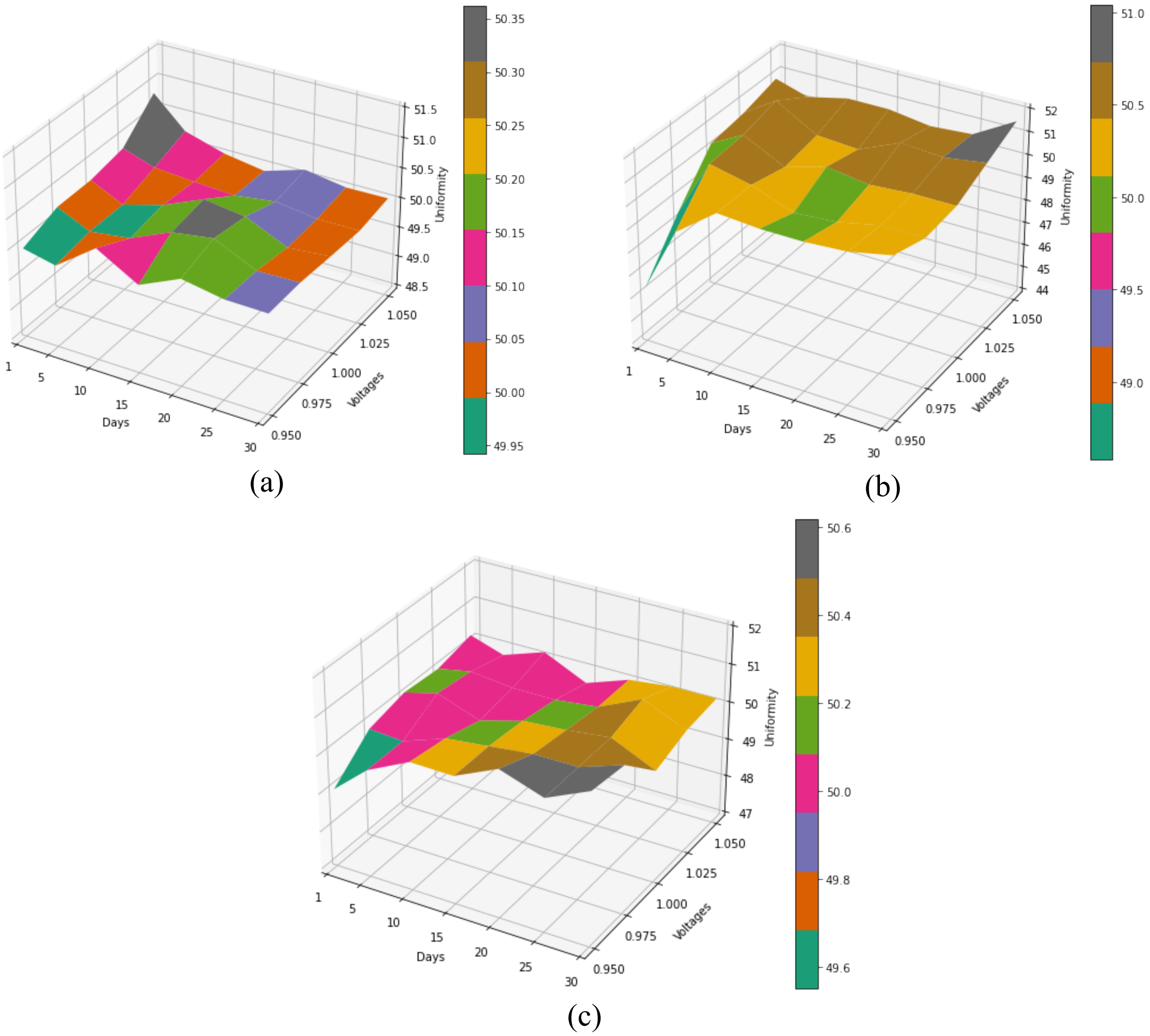
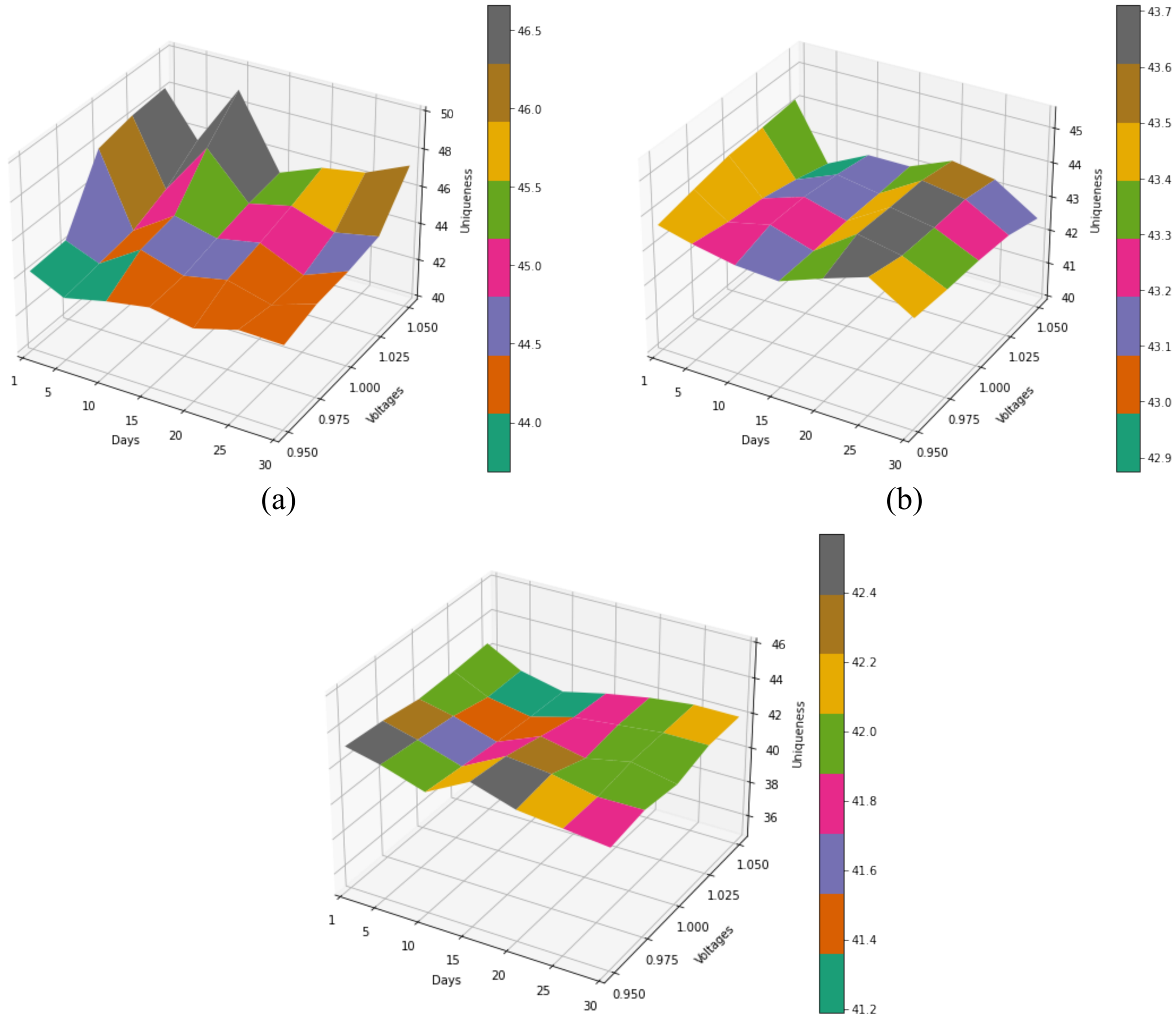


Figure 4-12: Uniformity changes in ROs due to aging and voltage variations combined: (a) Three stage; (b) Five stage; (c) Seven stage.

In the case of uniformity, the three stage and five stage designs from the ideal value with aging. Whereas, in the seven stage, there is barely any impact on the uniformity at any voltage level, which is represented in Figure 4-12 (a-c).



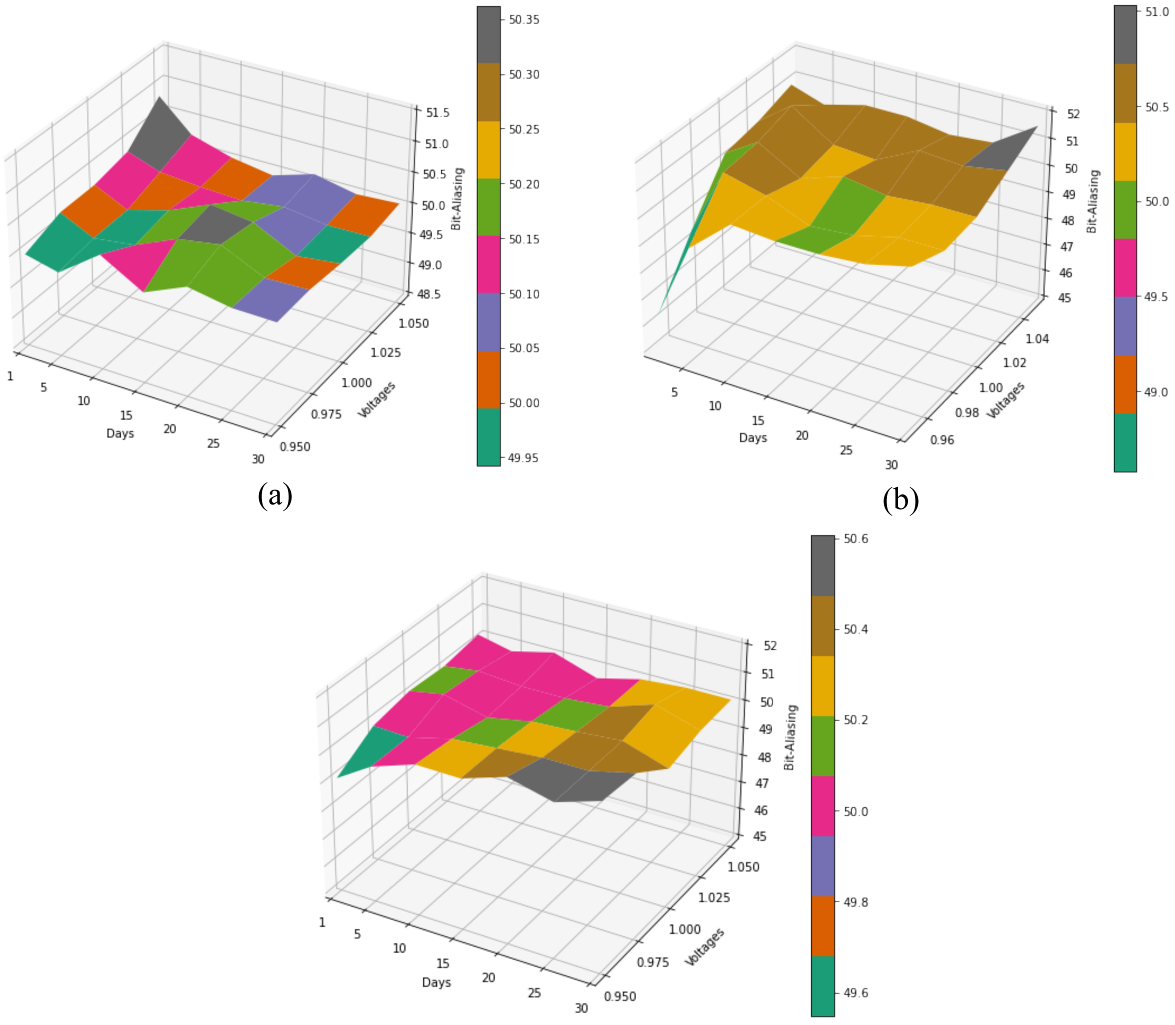
(a)

(b)

(c)

Figure 4-13: Uniqueness changes in ROs due to aging and voltage variations combined: (a) Three stage; (b) Five stage; (c) Seven stage.

Uniqueness with aging and voltage variations are represented in Figure 4-13 (a-c). As shown in the figure the uniqueness decreases with aging in each design in different voltages. The uniqueness is higher in each voltage level but decreases with time.



(a)

(b)

(c)

Figure 4-14: Bit-aliasing changes in ROs due to aging and voltage variations combined: (a) Three stage; (b) Five stage; (c) Seven stage.

The effect of voltage variation with aging on bit-aliasing is represented in Figure 4-14 (a-c). The Figure shows that the bit-aliasing remains almost the same in different voltage levels throughout the aging experiment.

The findings of the ideal values for each PUF metric are summarized in Tables 4-2–4-12. An ideal RO value must be 100% reliable, while other parameters like uniformity, bit-aliasing, and uniqueness must be around 50%. However, the actual systems are not ideal and parameters are affected by the change in operating voltage over time.

4.4 Summary

This chapter work primarily discusses the environmental impacts (i.e., temperature, voltage, and aging with voltage variations) on the performance (uniformity, reliability, bit-aliasing, and uniqueness) of different configurations of ROPUFs. From the detailed study, it is observed that the performance of different configurations of ROPUFs are impacted by environmental factors. It has been discovered that as temperatures rise, the uniformity, reliability, bit-aliasing, and uniqueness of different ROPUF configurations increase. The best values obtained for the 3 stage ROPIUF are 50.07% uniformity, 97.86% reliability, 50.06% bit-aliasing, and 48.87% uniqueness; for the 5 stage, the best values are 50.32% uniformity, 97.14% reliability, 50.31% bit-aliasing, and 45.39%; and for the 7 stage, 50.07% uniformity, 96.78% reliability, 50.07% bit-aliasing, and 47.63% uniqueness. Also, the performance of the ROPUF increases, with increase in operating voltage and decreases with aging for the three and five stage ROPUFs. When the voltage and aging experiments are conducted simultaneously, it is observed that different ROPUF parameters change with aging under different voltages. The impact of aging is also studied for the three different ROPUFs. For the three stage ROPUF, the impact of aging is minimal, whereas aging is more evident in five stage and seven stage ROPUFs. From the study, it can be concluded that the effect of voltage and temperature variation is maximum on ROPUFs whereas the effect of aging is minimum. Also, three stage ROPUF performs better in different environmental conditions compared to five stage and seven stage ROPUF configurations.

Chapter 5

A Study of the Impact of Temperature with Voltage Variations on Different Stages of the ROPUF

5.1 Introduction

The significance of security in Internet-of-things (IoT) and Cyber Physical Systems (CPS) has increased so much that it has become the top-most concern among researchers. Hardware security has become a serious issue in today's world, and immense effort has been put into securing software; however, hardware security needs much more progress to reach at par. The foremost reason of unreliable hardware is outsourcing the manufacturing processes of ASICs.

Physical Unclonable Functions (PUFs) exploit the intrinsic property of the electronic chip manufacturing process to generate a unique identity. PUFs are useful in unique key generation for encryption and decryption, IP theft detection, IoT device authentication, and numerous other applications [26, 106, 107]. A set of challenges is provided to a PUF where unique responses are generated against them. The architecture of a PUF dictates that it gets highly affected by environmental variations. The responses are supposed to be repetitive for the same set of challenges, but it may not provide desired results due to environmental and other variations. Any fluctuation in voltage supply, extreme temperature conditions or aging, result in deterioration of results. The key performance metrics to evaluate the PUFs are uniformity, reliability, bit-aliasing, uniqueness, and randomness. These metrics should ideally remain unaffected by any of the environmental variations. However, this is not the case in real-life scenarios; PUFs suffer from output errors, and these deviations from results further diverge due to temperature and voltage supply variations [105, 108-110].

In order to design reliable solutions, the behavior of PUF designs in varying environmental conditions must be known. Individual environmental variations such as temperature and unstable voltage supply are studied, but only a few works address the combined impact of these two factors comprehensively [90, 96, 111, 112]. Separate solutions for both variation types exist but devising a unique solution that solves the issue (impacts of temperature and voltage variations) is yet to be found. Moreover, this solution must be generic and not specific to a particular type of PUF.

This chapter examines the reversible temporal fluctuations of temperature with voltage variations on ten different Artix-7 Xilinx FPGAs for the three, five, and seven stage configurations. Moreover, this paper studies the importance of PUF performance metrics such as uniformity, reliability, bit-aliasing, uniqueness, and standard deviation of frequency. The temperature is varied from -70°C to 70°C through the temperature chamber while the voltage is varied from 0.95 V to 1.05 V through the power supply and all the results are recorded.

5.2 Related Work

Researchers have presented various PUF architectures and demonstrated their advantages and shortcomings [7, 58, 90, 113, 114]. Each of them has a specific utilization. As its name suggests, ROPUF is based on a ring oscillator comprising of an odd number of inverters cascaded in a feedback loop [7, 58]. This configuration produces a specific frequency measured with a counter. This frequency is a function of loop delay and is unique for each chip. ROPUFs are most suitable to be implemented in reconfigurable hardware like FPGAs [101, 113, 114].

The first mention of static random access memory (SRAM) PUFs was found in [41]. The principle behind it is that memory cells when pushed into unstable states will show oscillations. This is due to the process variations intrinsic to chip manufacturing. Some specific PUFs were introduced specifically for reconfigurable devices like Butterfly PUFs. A reconfigurable device like FPGA can emulate the behavior of an SRAM cell. This is performed by cross-coupling two data latches [42]. This architecture can generate an unstable state that converges to a stable state. The unstable state depends on the set/reset functionality of the latches while the stable state is determined by latch mismatch. All silicon based PUFs exploit the intrinsic property of ASIC components causing uneven delays due to random manufacturing variations. The random variations lead to disturbing circuit parameters such as leakage current, threshold voltage, gate delays, etc., which ultimately affect the logical and timing behavior of the circuit [115]. Due to extrinsic influences, such as operating voltage fluctuation and temperature variation, the output of the ROPUF can be affected [116].

Environmental factors may have a major impact on PUF responses, but only a few studies have addressed the issue comprehensively [96, 105, 112]. The temperature variations affect the reliability of PUFs because the operating temperature alters the threshold voltage, resulting in the distortion of the device delay. Temperature is inversely proportional to threshold voltage as well as the mobility of FETs. MOSFET mobility decreases the drain saturation current. Therefore, the delay of the device decreases. This change in the delay is reversible, the delays get back to normal as soon as the device returns to the normal temperature range [117, 118]. Voltage variations, just like temperature variations, also affect timing delays. However, these approaches only cater to a single performance metric, and a detailed study regarding the impact of environmental factors on PUFs is lacking. In this chapter, the impact of temperature with voltage variations are studied in terms of six major performance metrics for different stages of the ROPUF.

5.3 Experimental Setup

The layouts of ROPUFs for each of the three different stages used in our study are shown in Figure 3-1. The stage of the ROPUF is defined by the number of inverters inherent in its circuitry. Thus, a 3-stage ROPUF has three inverters, a 5-stage has five inverters, and a 7-stage has seven inverters.

Figure 3-2 shows the component level layout of the ROPUF mapped on an Artix-7 FPGA. The three stage ROPUF utilizes 4 LUTs, the five stage utilizes 6 LUTs, and the seven stage utilizes 8 LUTs. A total of 256 oscillators are used in this design. Each RO is manually mapped using the FPGA Editor tool in order to have identical ROs placed at different spatial locations of the FPGA. Figure 3-3 shows the floorplan layout of the RO hard macros on four different CLBs taken from the Xilinx FPGA Editor. In the figure, the four ROs are shown in green, red, purple, and blue color with small circles inscribed on them. It is important to note that the correct placement of the ROs within the FPGA is of critical importance for obtaining accurate results. In our design, challenges for choosing the ROs are produced through a 10-bit challenge generator. After the challenge is applied, the frequency counter is switched on for 0.4 ms to measure the frequency response. A 0.1 ms delay is used between challenges to select the next RO.

Multiple experiments on each stage of ROPUFs were performed to examine the impact of temperature with voltage variations on various stages of ROPUF. It is critical to understand which stage is least and most vulnerable to environmental variables. The results are compiled and explained in the next section. All the experiments have been performed on an Artix-7 FPGA on the NEXYS4 development board.

FPGAs and ASICs have various applications in industrial as well as embedded systems. Some of those applications may encounter harsh environmental conditions such as extreme temperatures in space, avionics, defense systems and many more. Such harsh environmental conditions like moisture, temperature, and EM noise may result in a fluctuating power supply in ICs [119]. Therefore, it is necessary to study the effects of temperature with voltage variations on hardware security measures. Variations in the voltage supply may lead to deviation in the frequency response of ROPUF. To investigate these deviations in the frequency response, voltage (V_{CCINT}) is recorded at 0.95 V, 1.0 V, and 1.05 V. These voltages are applied to the ROPUF, and operating at a variety of temperatures from -70°C, 25°C, and 70°C. The responses are observed for further analysis and verification. In the temperature with voltage variations experiment, the ROPUF is placed in a temperature chamber. A total of ten NEXSYS4 FPGA boards are used in this experiment. Figure 5-1 shows the experimental setup for recording the impact of temperature with voltage variations on the ROPUF. A 1000 series Test-Equity temperature chamber is used for recording and applying different temperatures, an Agilent 16801A logic analyzer is used for recording the frequencies, and a power supply for providing voltages to test points on the board.

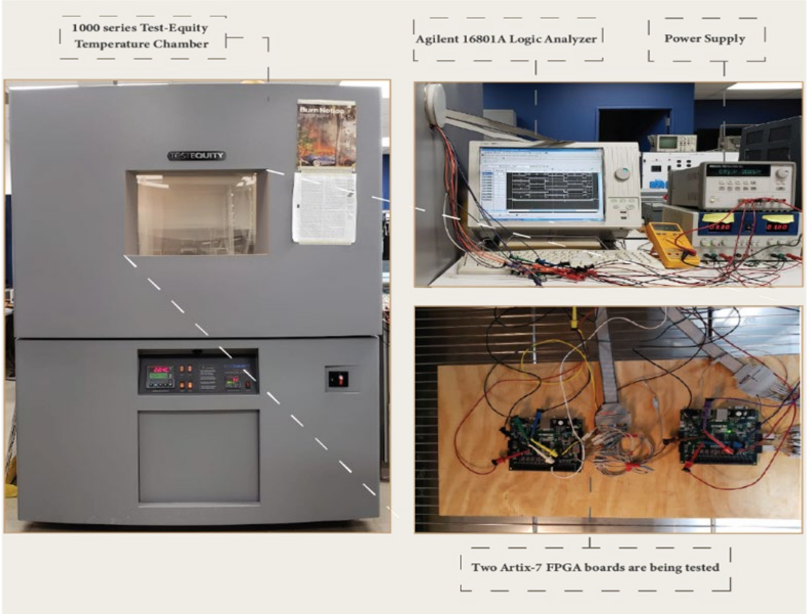

1000 series Test-Equity Temperature Chamber
Agilent 16801A Logic Analyzer
Power Supply
Two Artix-7 FPGA boards are being tested

Figure 5-1: Experimental setup for temperature with voltage variations experiment.

5.4 Results And Discussions

The experimental set-up for studying the impact of temperature with voltage variations is presented in this section. The performance is measured for the commonly used PUF metrics such as uniformity, reliability, bit-aliasing, uniqueness, randomness, and standard deviation of frequency.

The statistical test suite SP800-22 from the National Institute of Standards and Technology (NIST) is used to evaluate the randomness of the response sequence. This test suite is commonly used to evaluate the randomness of a binary sequence of numbers [103]. The frequency response test results for the ROPUFs are presented in Table 4-1. A total of 100 response sequences from the ROPUF output are evaluated, with each sequence consisting of 256 random bits. All of the p-values are greater than 0.01; this implies that all of the response sequences are random, resulting in a successful NIST randomness test pass.

The temperature with voltage variations experiment is performed using ten Artix-7 FPGA boards for three different temperatures. Ten Artix-7 FPGA boards are programmed for the three stage, five stage, and seven stage ROPUFs, in order to observe and compare the PUF metrics of each stage. Each ROPUF's uniformity, reliability, bit-aliasing, uniqueness, and standard deviation of frequency are shown in Tables 5-1, 5-2, and 5-3 for -70°C (minimum), 25°C (room temperature), and 70°C (maximum). The voltage is varied at each of the temperatures from 0.95 V to 1.05 V with a central value of 1.0 V. The results show that the ROPUF parameters significantly improve for all ROPUF configurations with the increase of voltage.

At -70°C, the uniformity is 49.84%, 48.06%, and 48.68% for the three stage, five stage, and seven stage respectively. At room temperature, the uniformity increases to 50.19%, 48.98%, and 49.50%. However, when the temperature reaches 70°C, the three stage uniformity approaches the optimal value (50%), while the five stage and seven stage uniformity increases (49.18% and 50.14%, respectively). When these results are compared to the bit-aliasing metrics results at -70°C, room temperature, and 70°C, it can be seen that their values for the three different stages are close to each other. For instance, at room temperature the results are 50.19%, 48.97%, and 48.59% for the three stage, five stage, and seven stage respectively. Similarly, as the temperature exceeds 70°C, the bit-aliasing of the various stages increases to 50%, 48.86%, and 50.15%, respectively. As the temperature rises, the uniformity and bit-aliasing as shown in Tables 5-1, 5-2, and 5-3 steadily improve.

The best values of the reliability at -70°C for the 3 different stages are 98.82%, 94.96%, and 94.46% progressively. However, at room temperature reliability remained at 98.13%, 95.31%, and 95% respectively. When the temperature rises above 70°C, the reliability of the different stages are 99.08%, 96.53%, and 96.66% respectively. As illustrated in Tables 5-1, 5-2, and 5-3, there is a clear trend of increased reliability as the temperature increases.

At -70°C, the optimal values for uniqueness are 49.09%, 43.13%, and 43.33% for the different stages. At room temperature, the uniqueness maintains at 49.77%, 44.13%, and 45.02%, respectively. When the temperature approaches 70°C, the measure of uniqueness increases to 49.93%, 45.32%, and 48.12%, respectively. As represented in Tables 5-1, 5-2, and 5-3, there is a clear trend toward better uniqueness as the temperature increases.

The standard deviation of frequencies against different ROPUF stages are shown in Tables 5-1, 5-2, and 5-3. Notably, three stage ROPUF has the highest standard deviation frequency among other stages. Low standard deviation specifies that the ring oscillators are more prone to bit flipping due to noise resulting in erroneous results [120]. This indicates that higher stages of ROPUFs are not appropriate for ROPUF applications, whereas the higher frequencies of a three stage ROPUF makes it more appropriate to use.

From the different configurations of the ROPUF, it can be concluded that the three stage ROPUF appears to operate better under various temperature and voltage settings than the five stage and seven stage ROPUFs. Tables 5-1, 5-2, and 5-3 summarize the results of temperature variations combined with voltage variations for the three, five, and seven stage configurations.

Table 5.1: Temperature with Voltage Variations Results at -70°C.

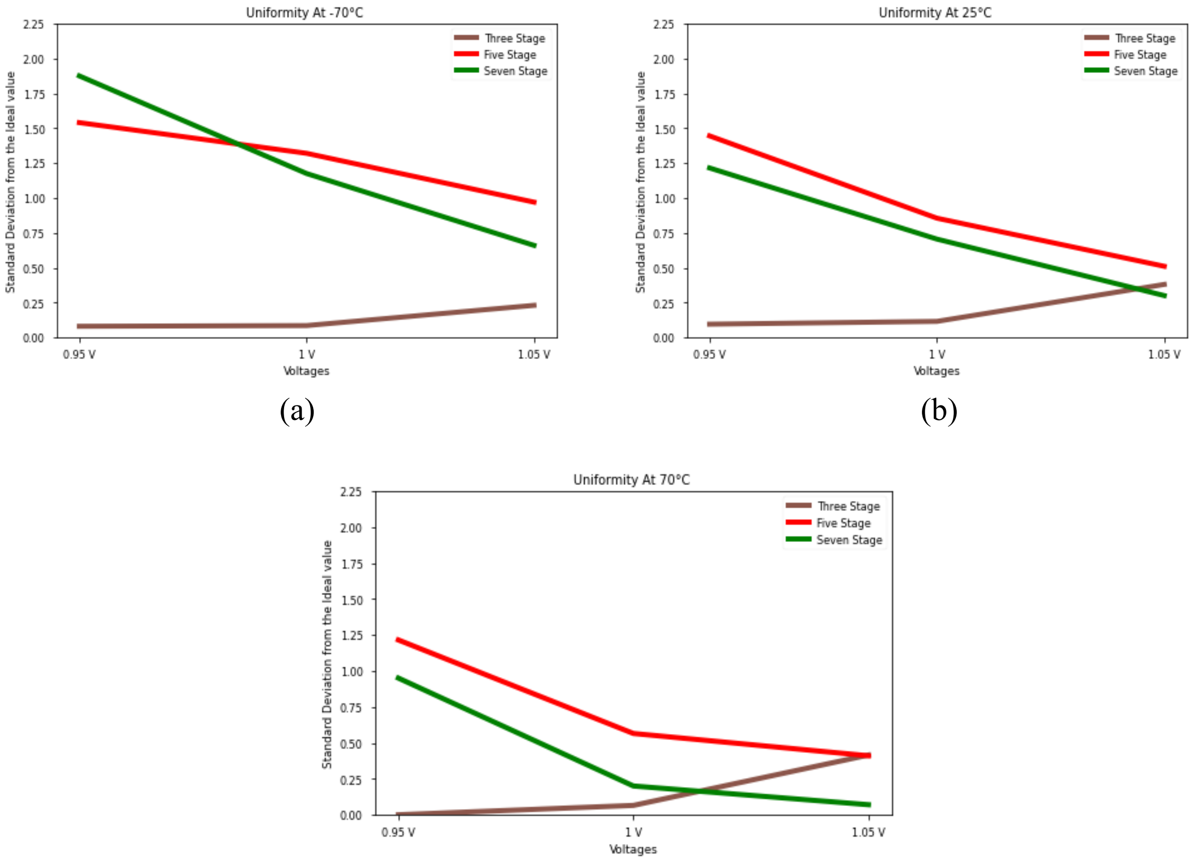
Metrics	**Ideal value**	**At -70°C (minimum)**								
		3 Stages ROPUF			**5 Stages ROPUF**			**7 Stages ROPUF**		
		0.95 V	**1 V**	**1.05 V**	**0.95 V**	**1 V**	**1.05 V**	**0.95 V**	**1 V**	**1.05 V**
Uniformity	50%	49.84	50.17	50.46	46.92	47.36	48.06	46.25	47.65	48.68
Reliability	100 %	96.48	97.28	98.82	92.26	93.79	94.96	92.68	93.39	94.46
Bit-Aliasing	50%	49.84	50.16	50.45	46.91	47.36	48.05	46.25	47.65	48.68
Uniqueness	50%	47.39	48.68	49.09	41.87	42.56	43.13	42.07	42.97	43.33
Standard Deviation of Frequency	X	5.55 MHz	6.89 MHz	8.29 MHz	2.35 MHz	4.47 MHz	7.48 MHz	2.89 MHz	4.44 MHz	6.19 MHz

Table 5.2: Temperature with Voltage Variations Results at 25°C.

Metrics	**Ideal value**	**At 25°C (room temperature)**								
		3 Stages ROPUF			**5 Stages ROPUF**			**7 Stages ROPUF**		
		0.95 V	**1 V**	**1.05 V**	**0.95 V**	**1 V**	**1.05 V**	**0.95 V**	**1 V**	**1.05 V**
Uniformity	50%	50.19	50.23	50.76	47.11	48.29	48.98	47.57	48.59	49.40
Reliability	100%	96.92	97.75	98.13	93.94	94.82	95.31	93.66	94.44	95
Bit-Aliasing	50%	50.19	50.23	50.75	47.11	48.28	48.97	47.57	48.59	49.39
Uniqueness	50%	48.14	49.02	49.77	42.56	43.98	44.13	43.71	44.45	45.02
Standard Deviation of Frequency	X	7.78 MHz	8.96 MHz	10.09 MHz	3.02 MHz	4.93 MHz	6.35 MHz	3.75 MHz	5.39 MHz	6.91 MHz

Table 5.3: Temperature with Voltage Variations Results at 70°C.

Metrics	**Ideal value**	**At 70°C (maximum)**								
		3 Stages ROPUF			**5 Stages ROPUF**			**7 Stages ROPUF**		
		0.95 V	**1 V**	**1.05 V**	**0.95 V**	**1 V**	**1.05 V**	**0.95 V**	**1 V**	**1.05 V**
Uniformity	50%	50	50.13	50.83	47.57	48.87	49.18	48.10	49.60	50.14
Reliability	100%	97.19	98.52	99.08	94.92	95.87	96.53	94.73	95.82	96.66
Bit-Aliasing	50%	50	50.13	50.82	47.57	48.86	48.18	48.10	49.60	50.14
Uniqueness	50%	48.22	49.66	49.93	44.07	44.91	45.32	47.09	47.88	48.12
Standard Deviation of Frequency	X	11.67 MHz	13.96 MHz	16.41 MHz	3.77 MHz	7.06 MHz	7.93 MHz	5.13 MHz	8.68 MHz	10.33 MHz



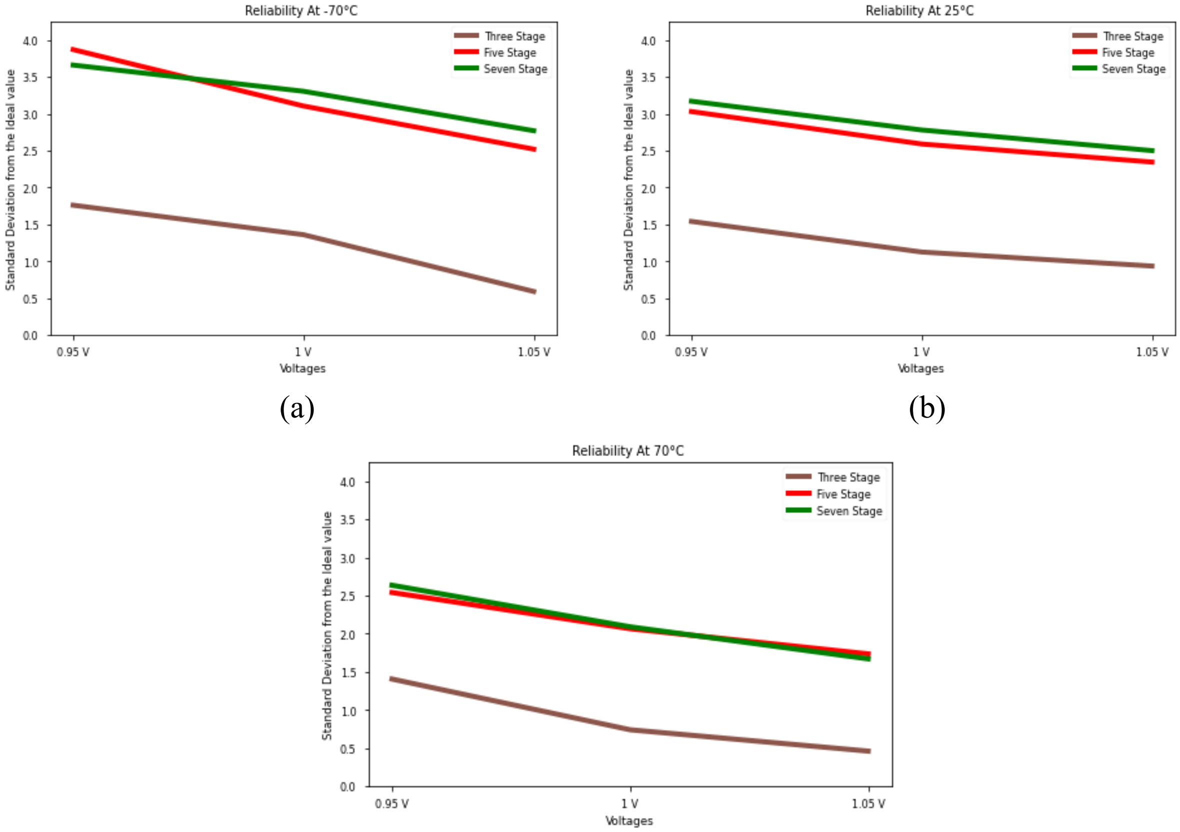
(a)

(b)

(c)

Figure 5-2: Environmental impact on the ROPUF in terms of uniformity: (a) -70°C; (b) 25°C; (c) 70°C.

Figure 5-2 (a-c) depicts the uniformity for different temperature and voltage levels. From the figure, it is observed that with the increase in voltages, the uniformity of different ROPUF configurations converge towards the ideal value which is 50%. With the increase in operating temperature the deviation from the ideal value tends to decrease. The uniformity deviation reaches its maximum at -70°C, while it reaches its minimum at 70°C. The closer it gets to 50%, the performance of the ROPUF is better. For a three stage configuration, the smallest deviation is observed at 0.95 V for all temperatures. For five stage and seven stage configurations, the minimum deviation from the ideal value occurs at 1.05 V. From the figures it can be devised that while selecting 7 stage and 5 stage configurations, the ideal voltage level would be 1.05 V, whereas for three stage, the ideal value is 0.95 V. Regarding temperature, three stage performs better in conditions ranging from -70°C to 70°C.



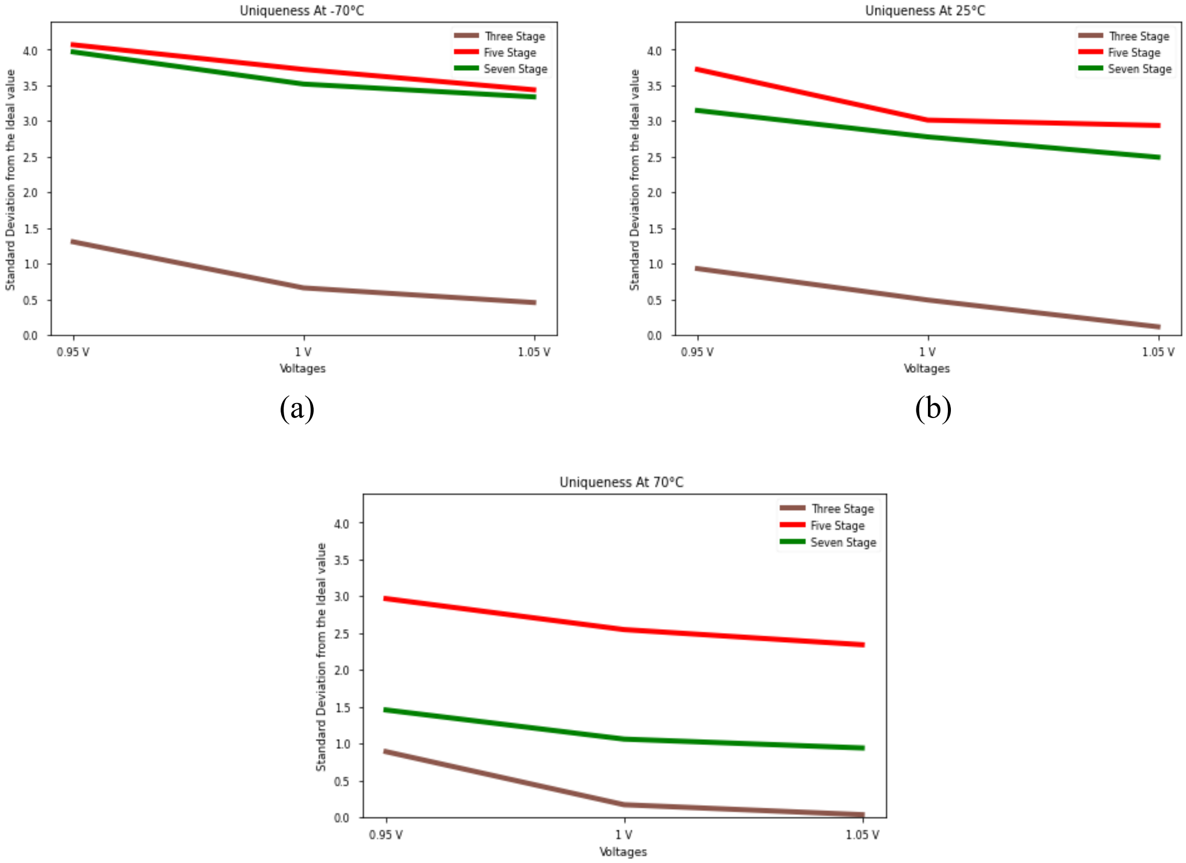
(a)

(b)

(c)

Figure 5-3: Environmental impact on the ROPUF in terms of reliability: (a) -70°C; (b) 25°C; (c) 70°C.

Figure 5-3 (a-c) represents the reliability for temperature and voltage variations. With the increase in operating temperature the reliability increases. For all configurations, the best reliability is observed at 70°C and 1.05 V. From this figure, it can be deduced that the higher the operating voltage of the ROPUF, the better the reliability. In terms of voltage, 1.05 V should be selected while designing a ROPUF. Also, it is observed that the reliability of three stage ROPUF is better in different operating conditions. It can be concluded that three stage ROPUF is more reliable than other configurations.



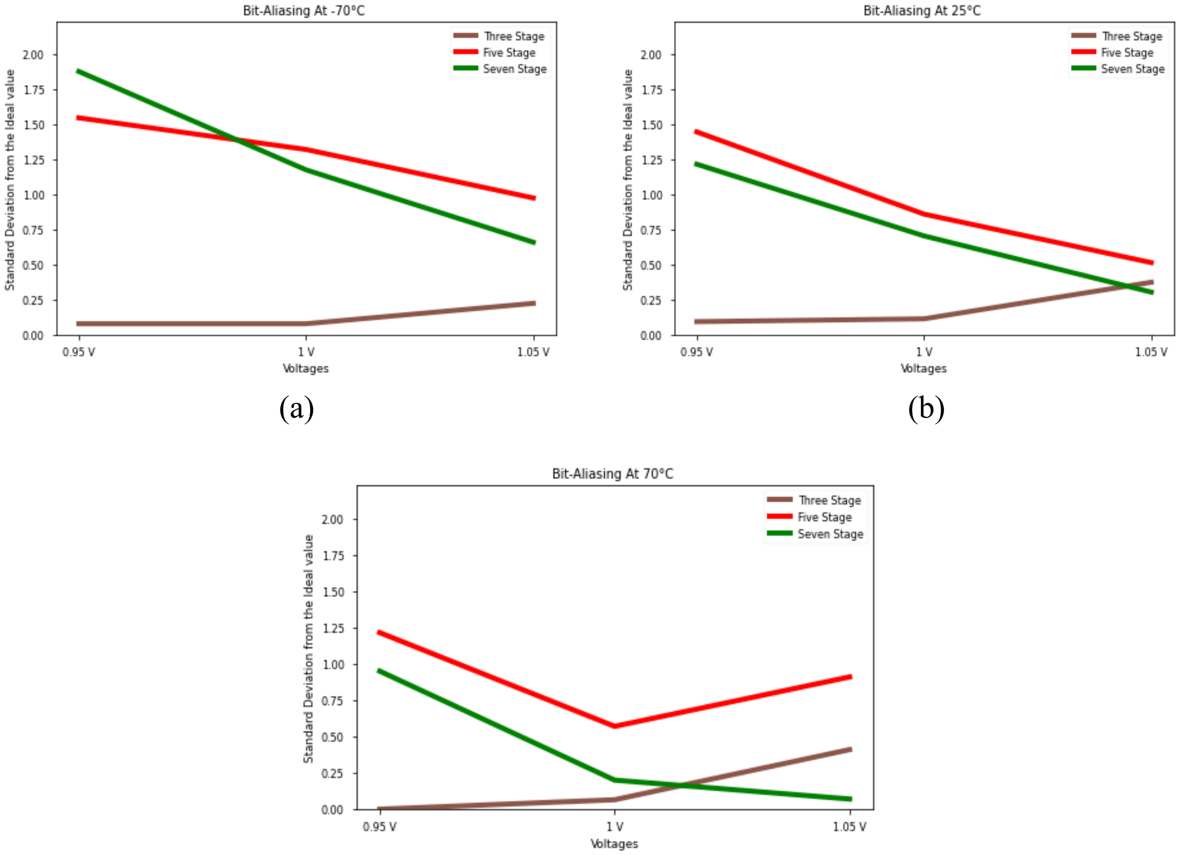
(a)

(b)

(c)

Figure 5-4: Environmental impact on the ROPUF in terms of uniqueness: (a) -70°C; (b) 25°C; (c) 70°C.

Uniqueness with temperature and voltage variations are represented in Figure 5-4 (a-c). According to the data, the optimum value of uniqueness is observed at 70°C. With the increase in operating voltage at different temperature levels, the uniqueness increases and the deviation approaches towards minimum value. The three stage ROPUF has the best uniqueness. From the results, the optimal voltage level for all configurations is 1.05 V. From the uniqueness parameter, three stage ROPUF would be an obvious choice while selecting the ROPUF configurations



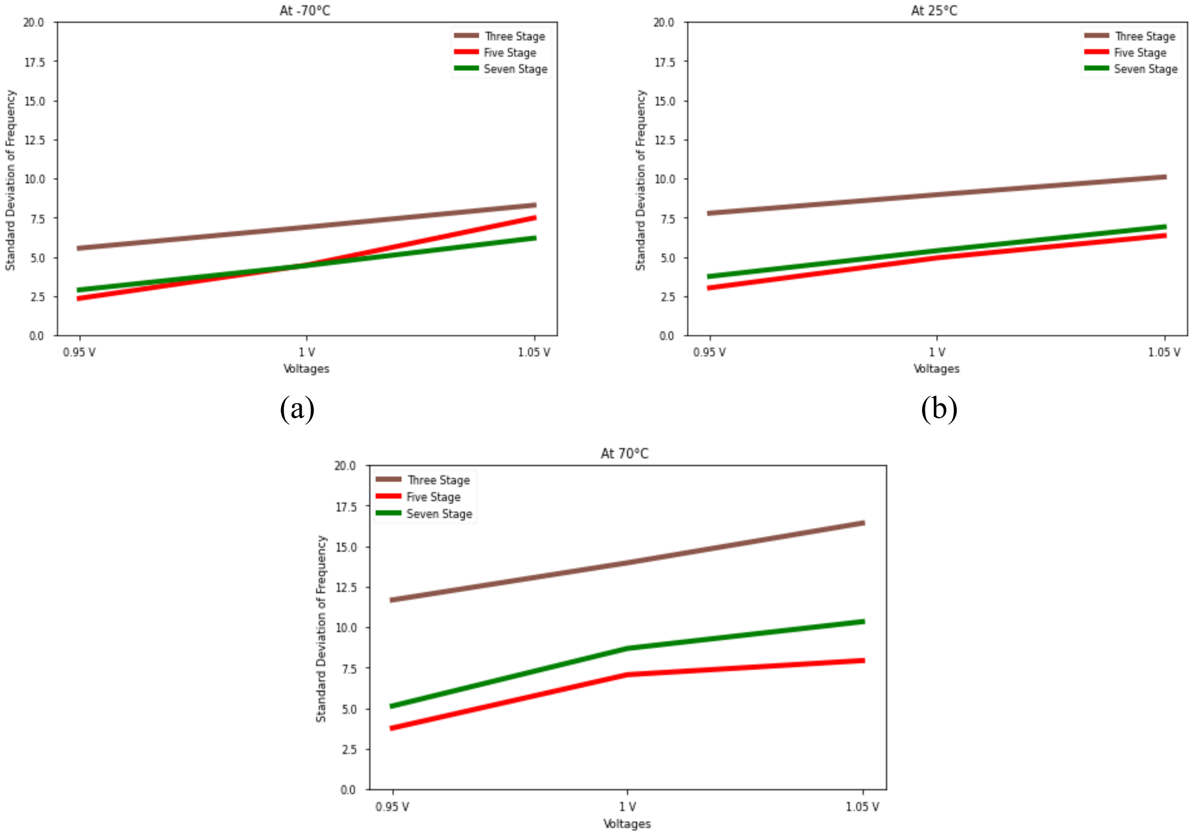
(a)

(b)

(c)

Figure 5-5: Environmental impact on the ROPUF in terms of bit-aliasing: (a) -70°C; (b) 25°C; (c) 70°C.

Figure 5-5 (a-c) illustrates the bit-aliasing results for three, five, and seven stage ROPUFs against temperature with voltage variation. At different temperatures, the bit aliasing converges towards the ideal value with the increase in operating voltage for five and seven stage ROPUFs, while for three stage the bit aliasing diverges. The minimum deviation observed for bit aliasing is 0.95V for the three stage ROPUF in every case. From this figure, it can be concluded that a three stage ROPUF provides superior bit aliasing results than the other two configurations of the ROPUF.



(a)

(b)

(c)

Figure 5-6: Environmental impact on the ROPUF in terms of standard deviation of frequency: (a) -70°C; (b) 25°C; (c) 70°C.

Figure 5-6 (a-c) illustrates the standard deviation of frequency results for three stage, five stage, and seven stage ROPUFs against temperature with voltage variation. From the figures, it is obvious that the standard deviation of frequency increases with the increase in voltage and temperature. Since higher frequency deviation lessens the chance of a bit flip, the three stage ROPUF is suitable for different applications than the other two ROPUF configurations. The maximum standard deviation of frequency for the three stage ROPUF is recorded at 70C operating at 1.05V, which is 16.41 MHz.

5.5 Summary

This chapter focused on determining the environmental impacts of temperature with voltage variations on the performance (uniformity, reliability, bit aliasing, uniqueness, randomness, and standard deviation) of three different configurations of the ROPUFs. The experiment was conducted using 10 different Xilinx Artix-7 FPGA chips. From the observed data, it can be concluded that the impact of temperature with voltage variations increases for all metrics for each configuration of the ROPUF. From the data, it can be observed that the optimum value (50%) of uniqueness is observed at 70°C. With the increase in operating voltage at different temperature levels, the uniqueness increases and the deviation approaches towards minimum value. The three stage ROPUF performs better when compared to the five stage or seven stage ROPUF. The best values for the three stage ROPUF in terms of uniformity, reliability, bit aliasing, uniqueness, and standard deviation of the frequency are 50%, 99.08%, 50%, 49.93%, and 16.41 MHz respectively.

Chapter 6

A PUF-Based, Zero Trust Design for Securing Advanced Metering Infrastructure (AMI) using Blockchain Technology

6.1 Introduction

As time necessitates the modernization of the electrical grid, the smart grid system has been proposed to update the existing architecture. The smart grid utilizes communication between the entities in a network and the computing to improve the efficiency and reliability of the current system while only being an enhancement of the preexisting infrastructure [121].

Most of the equipment used in grids and energy distribution is made up of embedded systems. These systems have limited processing and computational power. The equipment and infrastructure required for smart grids are critical to the implementation of seamless communication and data analysis. The security for these systems must be tight to avoid any malicious attacks. Millions of various systems and devices are integrated into smart grids. The high number of systems means high vulnerability for security breaches.

Attacks can potentially damage the infrastructure and distribution systems [122]. Two-way communication is a key characteristic of the smart grid and allows for both the power provider and the customer to exchange information that each party may value. Transitioning from conventional grids to smart grids presents unique challenges. Smart grids are vulnerable to physical and malware attacks. Manipulation through IoT attacks, falsified data injection and system faults attacks are some of the possible attacks that can disrupt smart grids and cause blackouts, imbalance in response-demand systems, incorrect load management, tripping and faults in equipment. Blockchain technology offers promising solutions to these problems, since it is designed in such a way that it can be used to protect the smart grid during authentication and to assess real-time energy consumption data. The real-time data is collected from smart metering that can provide the required useful information regarding the hardware. The collection of data is vital to ensure the security of smart meters. Physical Unclonable Functions (PUFs) are used to protect hardware such as smart metering. PUFs act as a fingerprint to any device that enhances the security of the device significantly [7, 123, 124].

The use of PUFs for verification along with blockchain technology can prevent the smart grid from providing falsified data and protect it from malware attacks. The combination of these two technologies can prevent Trojans and malware from accessing sensitive data and solve security vulnerabilities. Moreover, these technologies can easily be integrated with smart metering and grid infrastructures. Modern systems and networking channels are more sophisticated and advanced with various applications. At the same time, these modern systems are more vulnerable to both physical and software attacks. The traditional system architecture is not enough to provide the required security from such attacks. Therefore, the latest systems utilize Zero Trust Architecture (ZTA) in networks to protect sensitive data from security breaches. Blockchain technology and PUFs are integrated with ZTA to form a secure communication channel to transfer the data [125]. The main advantages of ZTA are enhanced security and universal authentication for computational resources and relevant data [126]. The fundamental requirements for ZTA are shown in Figure 6-1.

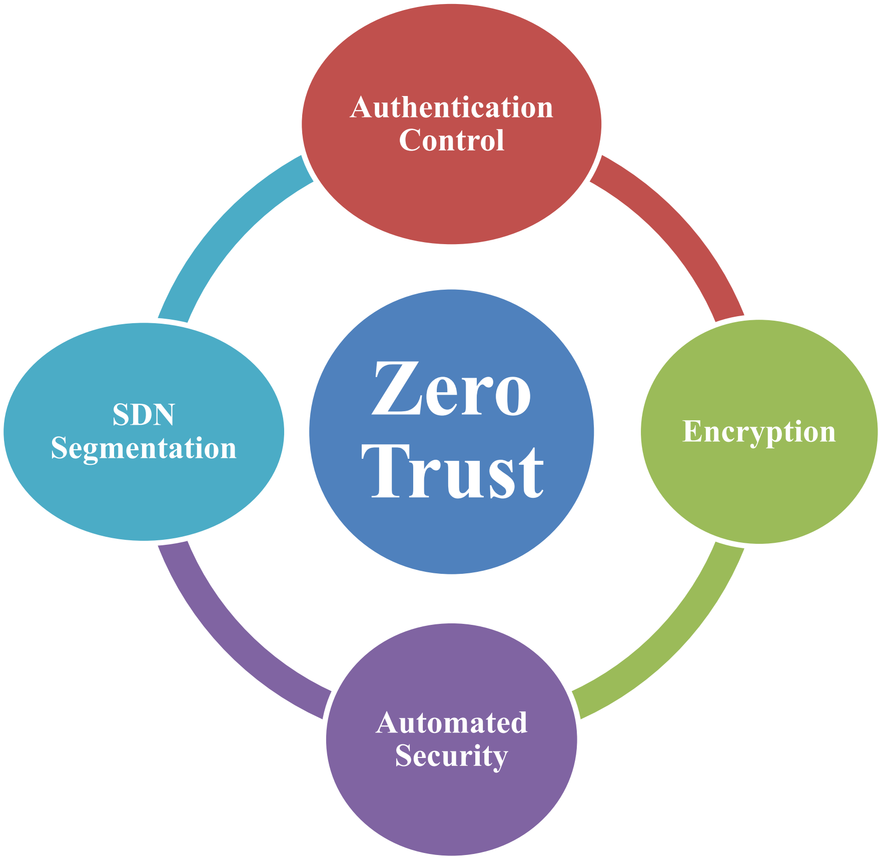


Figure 6-1: The fundamental to achieve Zero Trust Infrastructure.

At the core of this smart grid is the Advanced Metering Infrastructure (AMI), which consists of the Smart Meters (SMs), Data Collectors (DCs) and the data management systems running in the Utility Company (UC) which control all the communicating and the exchanging of data. Due to the AMI's use of networking, there has been a growing concern regarding the security of the system. Any security system that attempts to defend the vulnerable parts of the system must optimize availability, integrity, and confidentiality as its primary objectives [127]. Concisely, the system should have the ability for each entity in the network to allow for timely, yet secure access, whilst not forgoing privacy. Failure to secure the AMI in this way may lead to drastic consequences. The interaction of actors in different Smart Grid domains through secure communication is shown in Figure 6-2, reproduced from NISTIR [128].

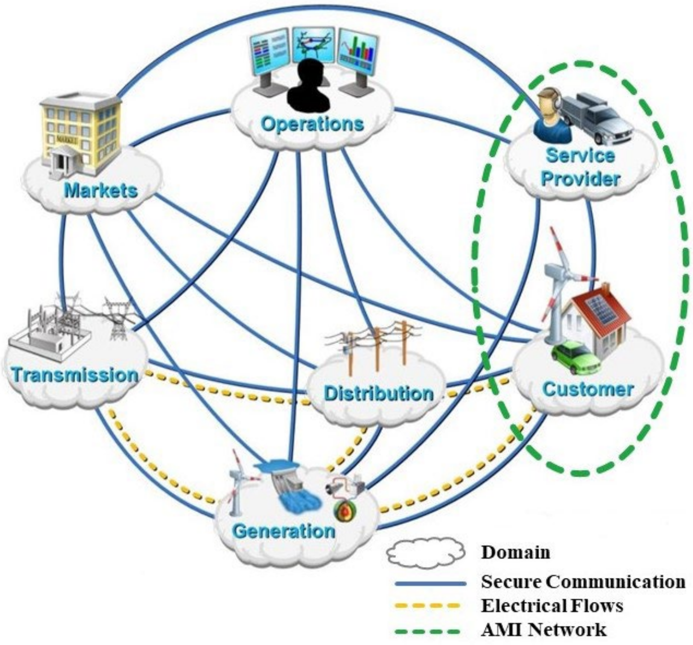


Figure 6-2: Smart Grid network model [128].

The AMI consists of different networking channels and systems that gather and analyze the data transmitted via smart grids. Moreover, various power service applications are attached to AMI to gather the relevant data from smart grids and meters. AMI plays an important role in the analysis and functions of smart grids. Malicious attacks target the vulnerabilities in AMI infrastructure. Therefore, it is essential to provide AMI with the necessary tools and systems to protect sensitive data against adversaries that can cause significant damage to the smart grid and metering infrastructure [124, 129]. A large portion of known methods of attack on the AMI focus on exploiting the entities within the network. A masquerade attack is an example of an exploitation attack, in which an illegitimate user may attempt to gain greater privileges than they should have to perform unauthorized actions on devices in the AMI [130]. Many current methods of security do not defend against such attacks, as it is assumed that, since the user appears to be legitimate based on everything except intention, the user is trustworthy and can be given access to any information or actions that are within their level of access. It is for this reason that this paper proposes a novel protocol for the verification of the AMI.

This protocol implements a Zero-Trust Architecture (ZTA) that is enabled by blockchain for monitoring and Physical Unclonable Functions (PUFs) on Field Programmable Gate Arrays (FPGAs) for authentication. Due to PUFs' ability to replicate outputs unique to the device they are located on, such a protocol allows for the removal of the requirement for any entity that is not the Utility Company (UC) to have any secure nonvolatile memory to keep track of secret keys. The implementation of ZTA allows for the nullifying of many attacks that rely on access being maintained by a malicious actor and offers complete traceability of the transaction of any data that is sent between all devices in the network due to the blockchain.

The contributions of this chapter are as follows:

- Building a novel authentication protocol for securing AMI using a combination of PUFs, Blockchain, and ZTA.
- Implementing a Zero Trust Architecture in the AMI to ensure heightened security.
- Developing a blockchain system to ensure traceability and accountability between participants of the AMI.

6.2 Related Work

Many authentication schemes for the AMI have been used previously for key authentication, communication networks, smart metering, and data collection. Current technologies used for smart metering usually include cryptography that is based on electrically erasable memory programs or uses random access memory [131-133]. These techniques are suspectable to malicious attacks [134].

Proposed authentication schemes come in a wide variety of implementations, though they can be classified into two groups: those which utilize existing hardware and those that use software only. Sellitto et al.[135] implement ZTA in this paradigm through the use of a digital twin. In the paper, they propose a dynamically aligned digital twin to reflect the state of the real-world network. The twin is then used as an enforcement agent for provided policies, however this design is applied broadly to the smart grid as a whole and focuses on the addition and removal of entities from the network. Kindervag et al.[136] first introduced “Zero Trust” in mid-2010. The security issues and networking problems have led DeCusatis et al.[137] to come up with a solution to employ the architecture that uses the zero-trust-based approach for authentication purposes, though not explicitly for the AMI. The stenographic overlay was used to induct the authentication tokens. Rose et al.[138] explained how the inclusion of ZTA improves the security structure for various systems. ZTA is proven to be more reliable to prevent any future malware attacks. Embrey et al.[139] explained the main drivers for the implementation of ZTA. ZTA offers a better solution to enhance security and control at the device level.

Gope et al.[140] proposed an authentication process with the use of PUFs to securely transmit data from smart grids and prevent any future malware attacks. Cao et al.[141] proposed a new privacy authentication scheme (PAC) for the smart grid that is based on PUFs. Experimental results suggested the high efficiency of this scheme; however, neither [140] nor [141] discuss internal breach and traceability within the system. There are also numerous authentication schemes implemented using blockchain. Kim and Huh [142] put forth a security scheme using Rainbowchain. Rainbowchain uses dual chains using seven different authentication algorithms. The implementation of the Rainbowchain in this manner is to assist in the decision-making regarding access. Wang et al.[143] propose a mutual authentication protocol using blockchain to act as the register authority of the network. However, this paper does not describe how the SMs and UCs are meant to authenticate each other, and instead focuses on the registration of the entities within the blockchain. The second group of authentication schemes fall under hardware security. For example, the authentication scheme proposed by [124] and [144] uses a PUF-based authentication method, meaning no data are stored on the vulnerable SMs, but there is no mention of a way to log the transactions between entities which can be realized using blockchain technology.

6.3 Preliminary Concepts

In this section, we introduce some concepts that are integral to understanding both the functional behaviors and the security of the proposed protocol.

6.3.1 Advanced Metering Infrastructure

The AMI is one of the 4 subsystems of the smart grid. In the AMI, there are two primary goals: to establish communications with customers, and to provide timestamped information to the other 3 elements of the smart grid. The AMI uses a variety of technologies to achieve these goals, such as Meter Data Management Systems, communication networks, and SMs [145].

At the core of the AMI is a utility network through which the customers indirectly communicate with the UC. This begins with a Home Area network that communicates to its own SM. The SM then communicates with a backhaul link that acts as a bridge to a Data Collector (DC). The DC is indirectly connected to the UC through a core backbone. For the purposes of this paper, this description of the utility network can be further abstracted to simply include the UC, DC, and SM, in which the DC acts as a middle-man and aggregation point for the data, as seen in Figure 6-3.

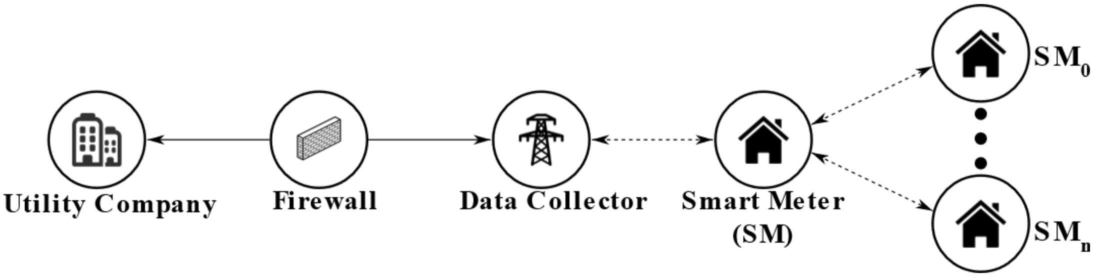


Figure 6-3: AMI network in smart grid [128].

Given the complex nature of the AMI, the network is inherently vulnerable to attacks of many forms. Thus, there are 4 key factors that any proposed security protocol for the communication network must satisfy [146]:

1. **Confidentiality** –This refers to the privacy of the customers metrology and consumption data. In the case of an attack in any form, it is vital that the customers' data are not accessed. Access to this data is to only be given to authorized system, such that a malicious actor is never able to view the information..

2. **Integrity** – This is the network's ability to guarantee that data sent and received between any pairs of entities in the network is from the entity that is claimed and not from a malicious actor masquerading as an authorized entity. Therefore, an SM, DC, or the UC must be able to ignore any requests coming from unauthorized entities.

3. **Availability** –While some data are not time-sensitive, it is expected for all data to be transferred in a timely manner. This is particularly the case for data that are taken at short intervals, which relay vital information regarding the health of components.

4. **Accountability** –Metadata regarding aspects of a message, such as a timestamp, must be kept so there is a level of traceability for vulnerabilities should an attack take place. This also means that, so long as both entities have shown themselves to be authorized entities through the applied authorization protocol and the request is of a valid security level, communication from one entity to another should not be denied.

While these factors are unique to the AMI layer of the smart grid, generalized forms of these factors may also apply to the other layers.

6.3.2 PUF

A PUF is a physical, one-way function designed to take in a challenge Ci Є C input and output a response Ri Є R unique to that challenge. PUFs take advantage of hardware manufacturing variances to generate the response, which provides the advantage of the PUF being unique to a specific device and making it impossible for an identical copy to be made using the same design [147]. An ideal PUF is expected to output a unique response for each unique challenge. PUFs offer the inherent advantage of not requiring any memory space, which can be vulnerable to a multitude of attacks.

In this work, a Ring Oscillator PUF (ROPUF) is implemented. A ROPUF is a PUF that extracts the irregularities of the chip using ROs. These ROs are positioned identically on each IC allowing for the differences in the oscillation frequencies to become apparent. Thus, by having two ROs compared with each other, a response bit can be generated. The challenge is input through a multiplexor that selects which ring oscillators to compare. The ROs are then sent a clock and their outputs are sent to ripple counters. After a specified time, the counters outputs are compared using a comparator, and the response bit is then generated from the comparator depending on how the response is meant to be generated from the algorithm, meaning that N comparisons result in N response bits. The function provided by a PUF can therefore be mathematically as C → R, in which C is the challenge and R is the response.

6.3.3 Blockchain

Blockchain is a decentralized distributed ledger system used for storing transactions. A blockchain is composed of a series of blocks, each respectively used to store data for a specific transaction. Furthermore, each block contains a hash pointer to a previous block, meaning it is difficult for a malicious actor to alter the previous data. Upon the addition of a block to the blockchain, it is propagated through the network; meaning that, hypothetically, changing the ledger with any less than the majority of the hashing power in the network would have no effect. While there are other types of attacks on blockchain, blockchain has been shown to be resilient and has been used to secure many other systems, such as vehicular edge computing [148] and Internet of Things communication [149]. There are three primary types of blockchain [143]:

1. **Public** –This is a decentralized, practically immutable form of blockchain. It is characterized by allowing all nodes to participate in the consensus process, allowing all users to read from the blockchain, and being highly scalable since any node can join or leave the network. This comes with the disadvantage of having higher latency and limited throughput.
2. **Private** –This form of blockchain is controlled entirely by a central authority, meaning it is more vulnerable to tampering by the authority and that the authority is allowed to make a decision regarding who may be able to read the data. It tends to have better performance and energy efficiency than a public blockchain since there are fewer nodes.
3. **Consortium –** Similar to the private blockchain, in a Consortium blockchain, there is a limited number of nodes allowed to validate the blockchain and have elective consensus. However, there is no single authority and the blockchain is partially centralized around a few selected nodes, meaning that it is not quite as prone to tampering as a private blockchain, but also not as immutable as a public blockchain.

In this chapter, the Ethereum network is used. While the other types of blockchain have their respective advantages, this decision revolves around the immutability and security offered by using a public blockchain. In the real-world, a different type of blockchain could be used. A consortium or private blockchain using a Proof-of-Stake consensus mechanism in which each entity in the network acts as a node was considered; however, this may come at the cost of security since the SMs and DCs are out in the field. While such a system would also completely remove gas fees, it also makes the system as a whole less secure since the blockchain loses immutability by being controlled by a single or only a few entities.

6.3.4 Zero Trust Architecture

ZTA is a set of paradigms focused on the implementation of zero trust principles in an attempt to create a secure system. The concept behind the zero trust principles is that there is no implicit trust granted to any specific device on the basis of their location, previous access, or any other characteristic [138]. This is in contrast to the traditional perimeter-based model in which a machine local to the network may be granted special access.

At the core of any implementation of ZTA are the seven tenets of zero trust. In order for a system to truly be considered ZTA, it is to satisfy the following tenets:

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.

4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

6.4 Proposed Model

6.4.1 Potential Threats

Any AMI authentication scheme may face a multitude of potential security threats with a variety of objectives. Ultimately, however, all of these attacks aim to disrupt at least one of the key factors of the AMI's security. These attacks can be categorized based on which of the three layers of the AMI is being targeted: the data layer, the hardware layer, or the communication layer [150]. This paper attempts to secure the transfer of data anywhere between the SM and the UC in the data layer, though consequently the model solves problems in both the hardware and the communication layers also.

The data layer is focused on the storage and transfer of data, which are vulnerable to manipulation, insertion, and hijack attacks. [150]. One fear is of a malicious actor manipulating the firmware of the SM (smart meter) or DC (data collector) that could modify data or limit the functionality of the device. Since this authentication model would require any file transfers to come from authenticated entities, meaning the SM or DC would never accept files from some unauthenticated entity. The limiting of such file unauthorized file transfers, whether transferring to an AMI entity or taking data from an AMI entity, is at the core of the proposed model. Another possible attack in the data layer relates to internet protocol (IP) based systems, in which an actor may be able to spoof an IP, use a teardrop attack, or simply use a Denial of Service attack to harm AMI functionality or steal data. Again, due to the limiting of unauthorized communication, such attacks should not be possible since any communication would simply be denied. Furthermore, logs regarding data of the attack would be placed on the blockchain, allowing for the UC to begin an investigation on such instances should it be deemed necessary.

In the hardware layer, one of the primary problems is the lack of onboard storage for the SM, meaning that there may not be enough space for the chip to perform cryptographic calculations, and any storage added retroactively would increase the chip's vulnerability to physical and cyber-attacks [150]. Both of these problems are solved by the proposed authentication scheme, as a PUF requires no onboard storage, meaning the SM is capable of using all of its storage for metering purposes. While PUFs may be vulnerable to machine learning attacks, this can be minimized depending on the PUF's design, such that the PUFs become resistant to such attacks [151-153]. It is also possible for these attacks to be launched against the DC, though since the DC is to be treated no different from an SM, there is no more risk for one than the other. There is also the possibility of malicious code being sent to an SM or DC, but this should not have any impact on the devices due to the authentication required. Lastly, many of the same problems are relevant in the communication layer, such as a malicious firmware update. Nevertheless, fears of a man-in-the-middle attack can be avoided through the authentication mechanism and traced due to the implementation of blockchain in the scheme.

On top of attacks specific to these three layers, there are also more generalized attacks that may impact multiple layers. One possibility is an attacker inserting their own node to act as a DC, rerouting all traffic through itself so that it can manipulate the data before sending it onward. However, since someone at the UC would first need to take note of each device's CPBPs and add them to a list in the UC before allowing any communication with a device, an attacker attempting to insert a new device into the AMI would need to have full access to the UC, itself, before doing so. There is also a possibility of an attacker masquerading as the UC, though this attack is dealt with somewhat trivially due to the authentication scheme and would be entirely traceable because of the implementation of the blockchain. Another attack may be if a user manages to somehow bypass the entire authentication scheme due to poor implementation. While this would certainly impact the system, due to the blockchain, any such attack would be entirely traceable, and it would be very simple to discover all details on the attack and deal with it accordingly.

6.4.2 Procedure

The ROPUF used in this work is a 3-stage ROPUF, shown in Figure 6-4 [101]. The stage of the ROPUF is defined by the number of inverters inherent in its circuitry. The 3-stage ROPUF mapped on 10 different Artix-7 FPGA boards. A total of 256 ring oscillators (ROs) are used in this design. Each RO is manually mapped using the FPGA Editor tool in order to have identical ROs placed at different spatial locations of the FPGA. Figure 6-5 shows the floorplan layout of the RO hard macros on four different CLBs taken from the Xilinx FPGA Editor. In the figure, the four ROs are shown in green, red, purple, and blue color with small circles inscribed on them. It is important to note that the correct placement of the ROs within the FPGA is of critical importance for obtaining accurate results. In our design, challenges for choosing the ROs are produced through a 10-bit challenge generator. After the challenge is applied, the frequency counter is switched on for 0.4 ms to measure the frequency response. A 0.1 ms delay is used between challenges to select the next RO.

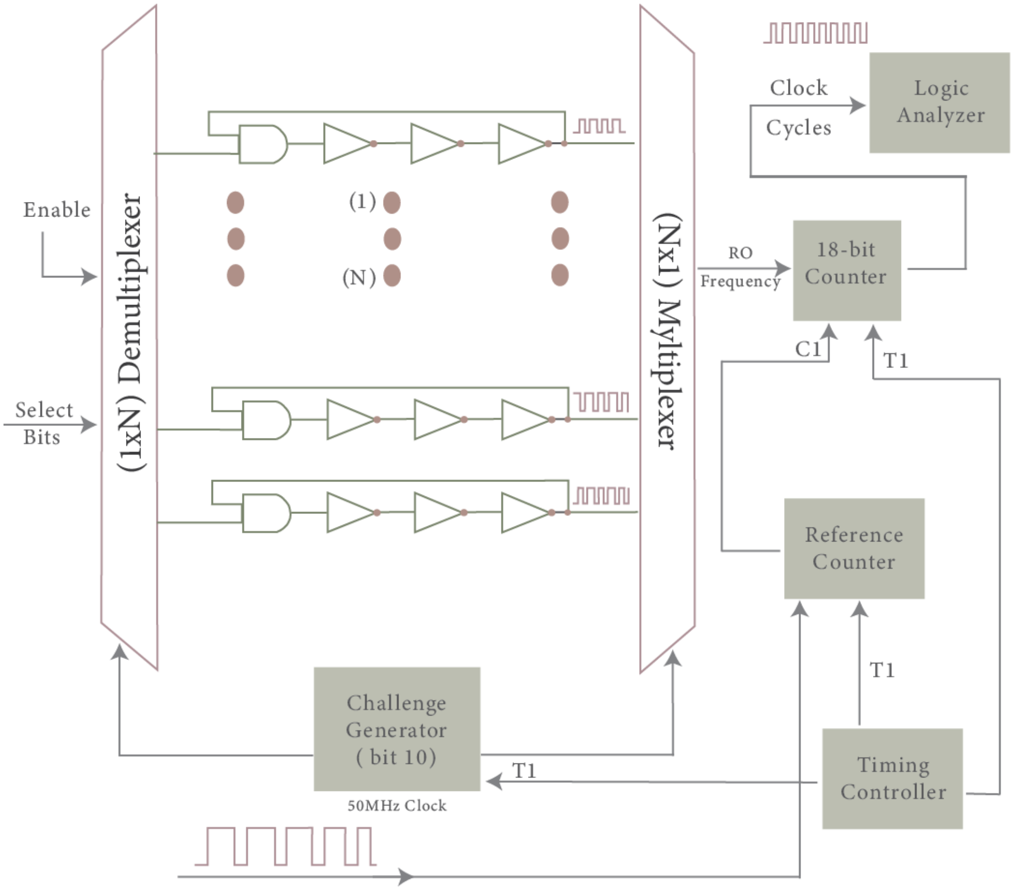


Figure 6-4: Block Diagram of 3-Stage ROPUF design.

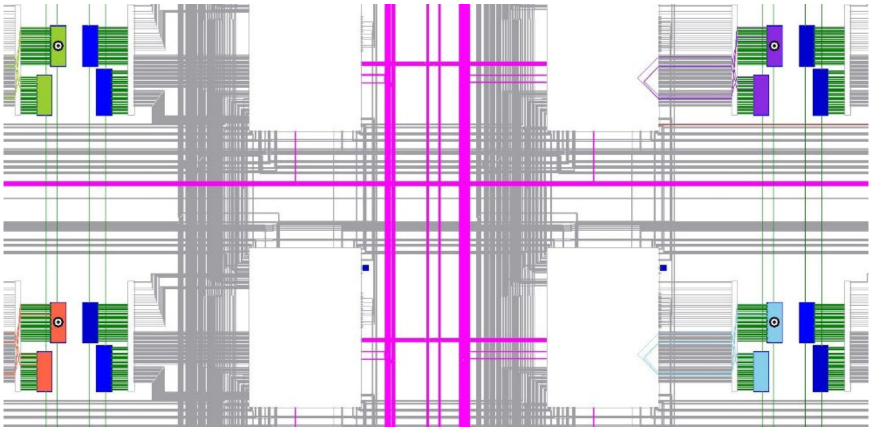
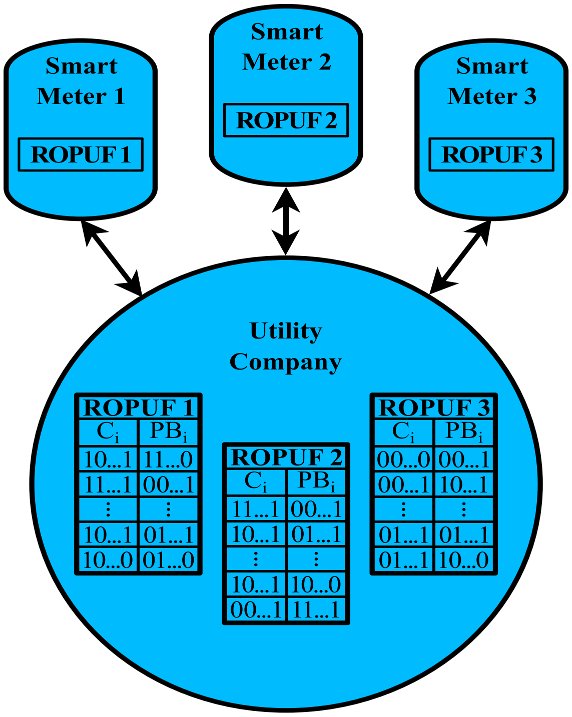


Figure 6-5: Floorplan layout of the RO hard macros on four different CLBs from Xilinx FPGA Editor.



ROPUF 1

C_i	PB_i
10...1	11...0
11...1	00...1
⋮	⋮
10...1	01...1
10...0	01...0

ROPUF 2

C_i	PB_i
11...1	00...1
10...1	01...1
⋮	⋮
10...1	10...0
00...1	11...1

ROPUF 3

C_i	PB_i
00...0	00...1
00...1	10...1
⋮	⋮
01...1	01...1
01...1	10...0

Figure 6-6: ROPUF registration with UC.

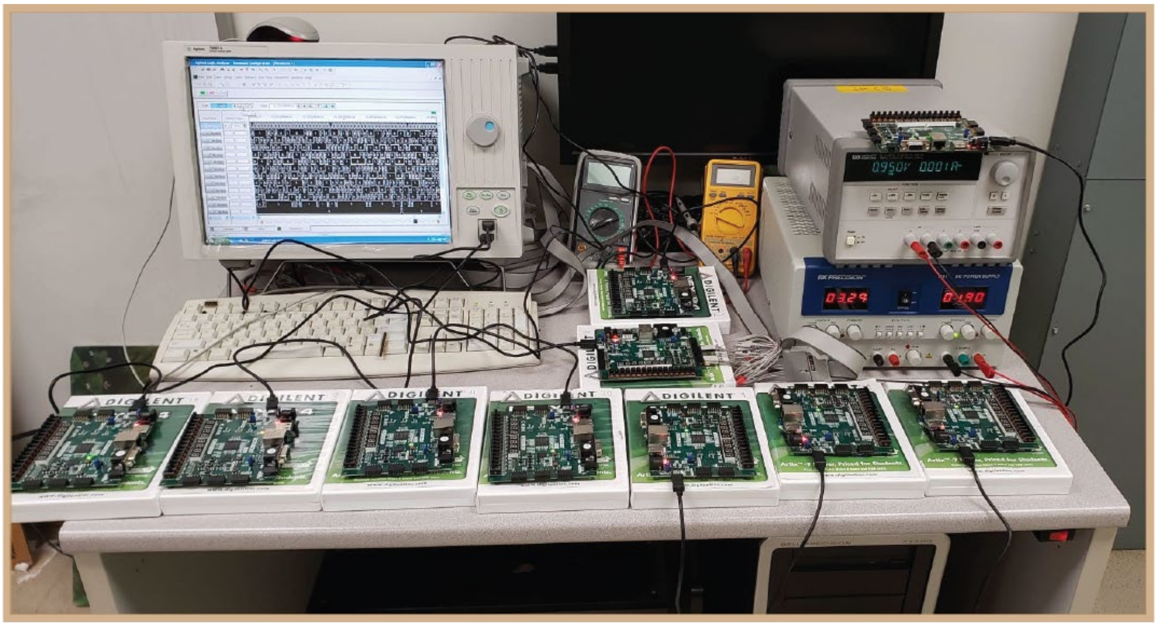


Figure 6-7: Experimental setup for the collection of data samples from ROPUFs.

There are three primary entities within the AMI: the UC, the SM, and the DC. In the AMI, all data collected from an SM must go through a series of other SMs until reaching a DC and finally being forwarded to the UC. Likewise, though the UC is never considered trusted by any of the SMs, the UC is to store the Hamming code parity bits pairs (CPBPs) that have been generated by each ROPUF, as seen in Figure 6-6. Figure 6-7 represents the actual ROPUFs implemented in different FPGAs. The UC is assigned this task since it has a much greater capacity for storage than a single SM. Furthermore, the UC is less vulnerable to physical attacks than the SMs since it is not in the field, and it is also less vulnerable to cyberattacks due to the firewall it should have in place. Nevertheless, this does mean that the security of the UC is of the utmost importance.

From a security standpoint, a DC should be treated as an SM by the UC in all aspects. It is proposed that every SM be retroactively outfitted with a ROPUF. The ROPUF does not require the devices to be outfitted with any extra memory, though it should be connected via a serial connection and necessitates the updating of the devices' firmware to support the new ROPUF. These ROPUFs' CPBPs and their respective challenges are to be registered with the UC before being integrated into the network. It is therefore necessary that the Ci for each ROPUF is provided by the manufacturer. The UC is then to record the Ri for each Ci from 128 bits to 2048 bits for use depending on the security level necessitated by a given task. The UC is not required to have a PUF, since it is able to be authenticated by showing that it knows what a given SM's CPBP would be, something an attacker would not be able to know without access to the UC's system. Table 6-1 shows list of abbreviations.

Table 6.1: Abbreviation.

Abbreviation	
REQ	Request
AUTH	Authenticate
VER()	Verify
CPBP	Challenge & Parity Bits Pair
Ci	Challenge (i)
PBi	Parity Bits (i)
ACK	Acknowledge

The use of PB_i over simply using R_i as the authentication mechanism for C_i is to improve the security of the system against attacks that aim to model the ROPUF from its responses. The advantage of using the CPBP rather than the challenge-response pairs is that an adversary would not be able to match a response to a specific challenge [154]. In the case that the UC is hacked it is possible to reconfigure the system. This is done by replacing the ROs, and therefore R_i and PB_i.

In order to add an SM to the network, the new SM and its ROPUF's CPBPs are to be register with the UC. It is important to note that this does not mean the UC is a "trusted party" as this would violate ZTA; instead, this is to provide the UC the ability to authenticate the entity it is communicating with and for the UC to authenticate itself to a secondary entity. Upon registration, the SM can be added to the network for initial authentication to begin. The initial authentication is to verify to the UC that the SM is legitimate. First, the SM is to send a request to the UC, with which the UC is to respond with a challenge. The SM is then to generate the CPBP and send it back to the UC. Upon receiving the SM's response, the UC will then acknowledge or not acknowledge the SM based on whether the response is consistent with what was given in the registration process. This process is shown in Figure 6-8. Upon acknowledgement, the SM is to authenticate the UC, as seen in Figure 6-9. This is done by the UC requesting high-level access to the SM. Included in this request is a challenge C_i and CPBP PB_i. The SM then challenges itself with C_i and verifies PB_i. The SM then either acknowledges or does not acknowledge the UC based on this verification. After acknowledgement is made, the connection is closed, and the SM is to call a function on the blockchain which will store details on the transaction. This ensures the satisfaction of the ZTA tenets regarding the monitoring of the system and the collection of information regarding the network.

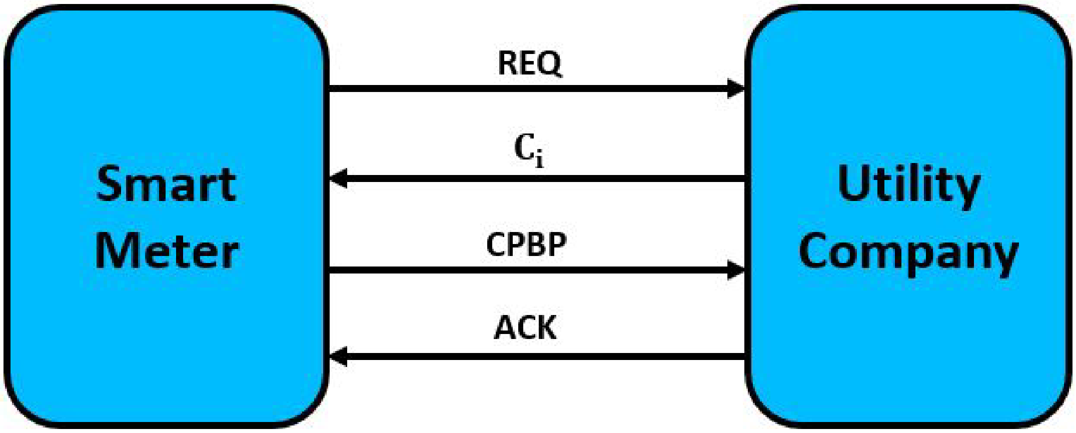


Figure 6-8: SM to UC authentication.

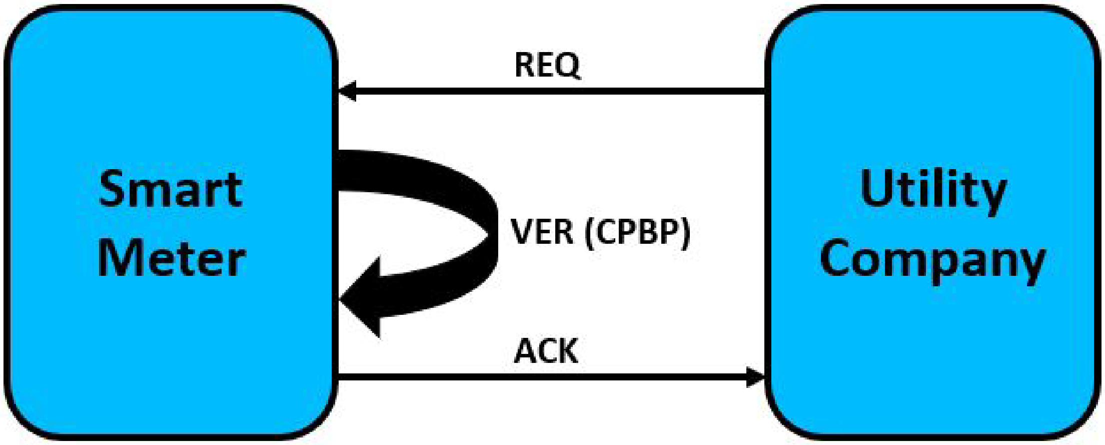


Figure 6-9: UC to SM authentication.

Due to the zero-trust nature of the proposed model, authentication by both the UC and SM is required for each session. Upon a need to exchange data, the entities are to authenticate each other in a similar manner as when the SM was first added to the network. The process of mutual authentication is shown in Figure 6-10. The UC must first authenticate the SM by sending a challenge to the SM and verifying the CPBP, then acknowledging or not acknowledging the SM based on whether the CPBP is consistent with what the known response should be. Likewise, the SM is to authenticate the UC in the same manner as when it was added to the network, though limiting the access of the UC only to the minimum level access required, in accordance with the tenets of zero-trust. The UC will posit a request with the access needed and send a challenge C_i and a CPBP PB_i to the SM. The SM will then generate its own CPBP and compare it with PB_i. Based on this comparison, it will either acknowledge or not acknowledge the UC. After both the UC and SM have acknowledged each other, data can be exchanged. Once the exchange is complete, the connection is closed. After that point, authentication will be required again to exchange any more data. The SM then documents the exchange on the blockchain.

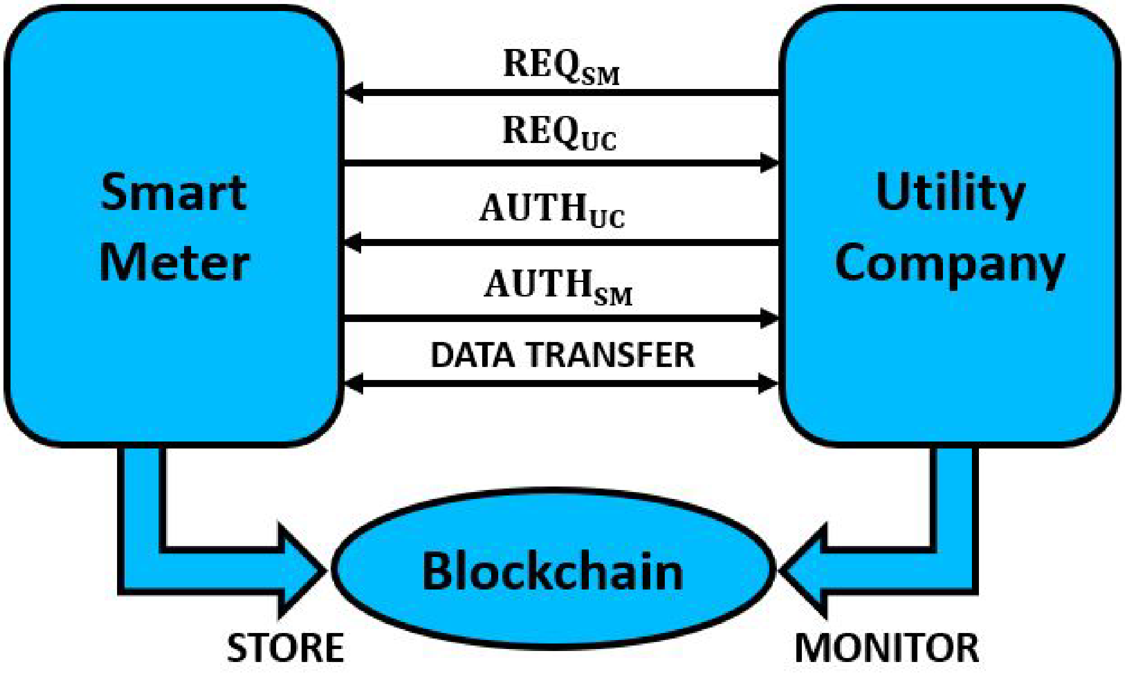
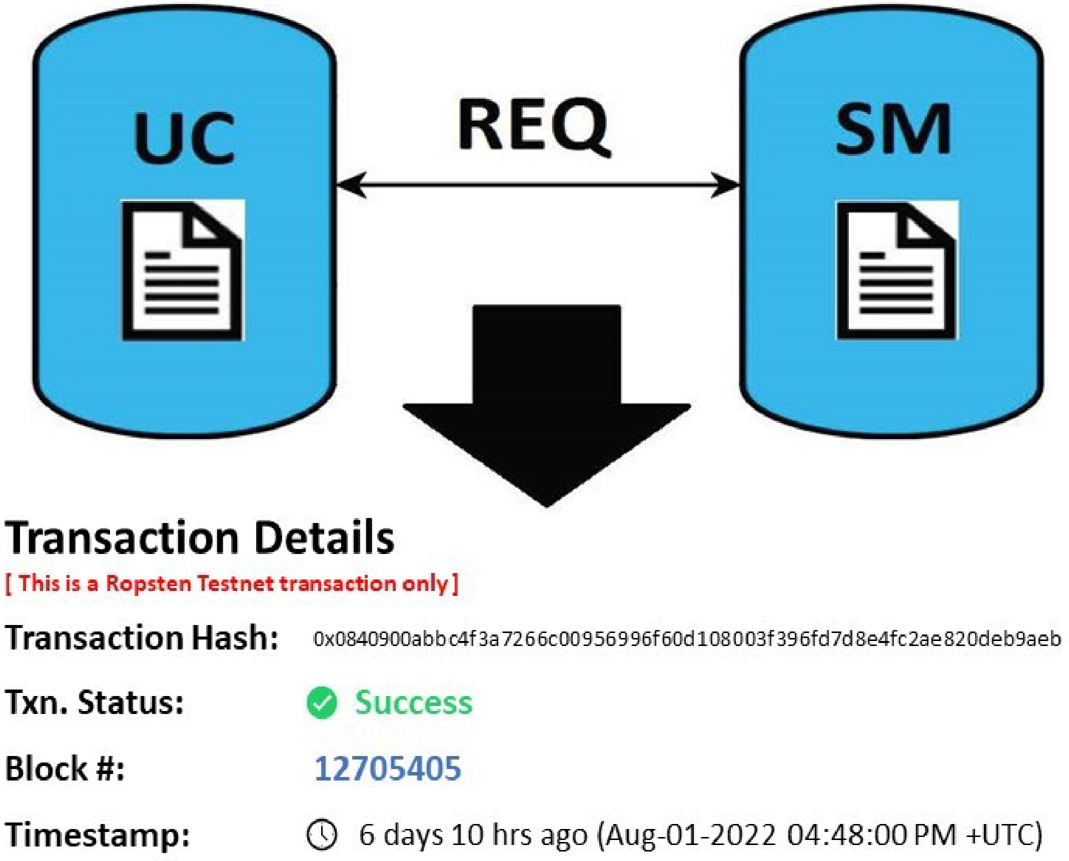


Figure 6-10: Data Exchange Protocol.

The blockchain provides traceability and accountability within the system. For successful implementation of the blockchain, smart contracts were developed using Solidity and were used to perform the communication between the UC and SM and finally authenticate it. All the transactions are recorded on the distributed ledger with a timestamp, ensuring no wrongdoings within the AMI system as depicted in Figure 6-11, which shows the ‘request’ transaction between the UC and SM. The smart contracts developed were tested on a locally built private Ethereum test network, implemented using a Geth client.

The test network is very similar to the Ethereum Mainnet, only it does not require real Ether to execute transactions. Also, the test network, uses Proof-of-Work (PoW) as consensus algorithm, which the same as Mainnet.



Transaction Details

[This is a Ropsten Testnet transaction only]

Transaction Hash: 0x0840900abbc4f3a7266c00956996f60d108003f396fd7d8e4fc2ae820deb9aeb

Txn. Status: ✓ Success

Block #: 12705405

Timestamp: 6 days 10 hrs ago (Aug-01-2022 04:48:00 PM +UTC)

Figure 6-11: Example of a blockchain transaction between UC and SM.

It is expected for the UC to act as a watchdog for the blockchain in the case that any requests are made from an unauthorized source. In the case that the UC recognizes a suspicious request for a blockchain entry, it should throw a warning. Physical investigation is then required of a party at the UC to find the reason behind the request and decide the correct course of action. Such a warning will be placed on the blockchain, so that any consistent suspicious requests from the same party or demonstrating some other pattern may be looked at. This is to further enhance the traceability and accountability of the system, thereby assisting in any future investigations, regardless of if past warnings have turned up little evidence.

It may be possible for a malicious actor to model a ROPUF using machine learning, in which case they can predict the R_i for a respective C_i. This would give them the ability to exchange data with a UC. Though this attack would eventually be caught due to the implementation of the blockchain, temporary damage may still be possible. To prevent such an attack, the authentication scheme instead uses the Hamming code parity bits PB_i as shown in Figure 6-12. This scheme utilizes the (8,4) Hamming code, a linear error correcting code, as a one-way function to create a consistent output for the ROPUF and to make it impossible to model the ROPUF using machine learning [154]. While a hash function may also have the same effect of preventing machine learning attacks, if even a single bit of the R_i suffers a bit-flip, the hash cannot be recovered. However, the use of the PBs allows for a predefined level of discrepancy, such that the authentication can still take place even under anomalous circumstances. Furthermore, the Hamming code algorithm is trivial and require very little computational power, meaning it is far more efficient than a hash, without any decrease in security. While it may be possible for an attacker to gather the PB_i and C_i, that information becomes immediately useless since a new challenge is used for every session of communication.

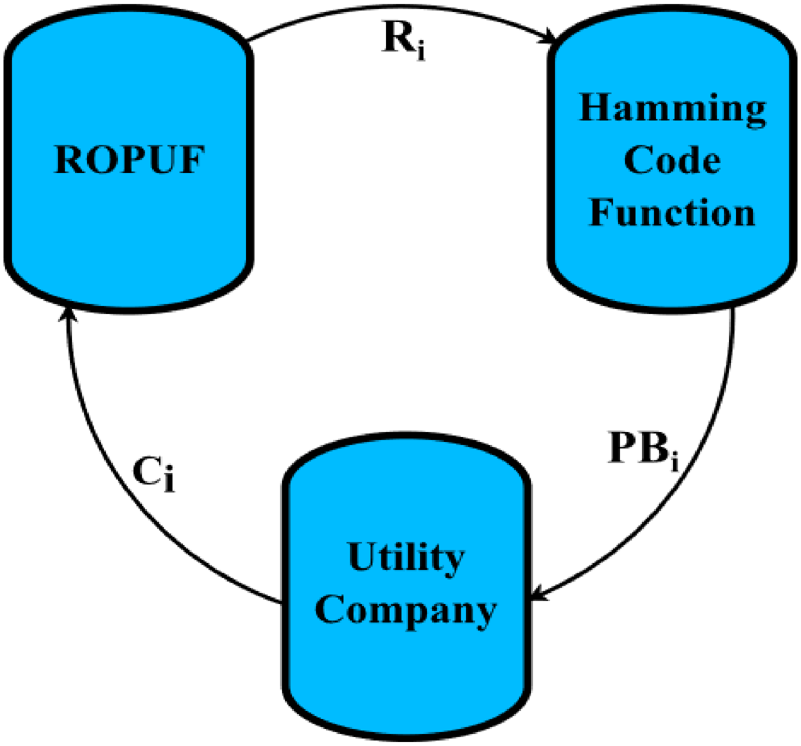


Figure 6-12: Parity Bits PBi generator.

The (8,4) Hamming code produces x=n parity bits, where x is the number of parity bits and n is the number of response bits. This means that the number of authentication bits being sent using the PB_i does not increase overusing the R_i, as seen in Figure 6-13. By using the same number of bits for the PBs as for the Rs, security is maximized without an increase in transfer time. Therefore, there are three advantages to using the PB_i over the R_i. First, it is not possible for a malicious attacker to model the ROPUF through the PBs. Second, the function is lightweight compared to alternative forms of encryption or hashing. Lastly, this method allows for a level of discrepancy to be accounted for, allowing devices to continue functioning in old age, when experiencing a voltage spike, or some other anomaly.

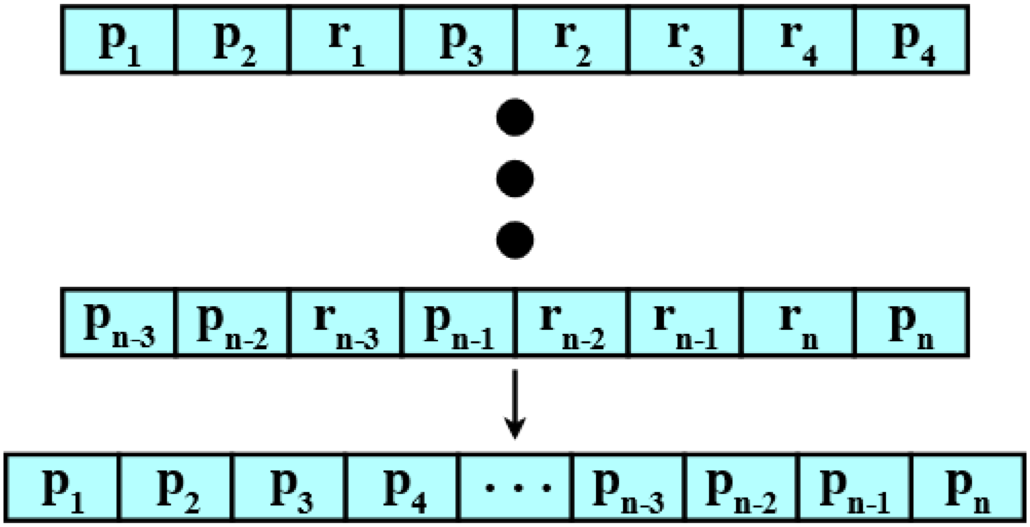

p_1 p_2 r_1 p_3 r_2 r_3 r_4 p_4
p_{n-3} p_{n-2} r_{n-3} p_{n-1} r_{n-2} r_{n-1} r_n p_n
p_1 p_2 p_3 p_4 . . . p_{n-3} p_{n-2} p_{n-1} p_n

Figure 6-13: Parity bits for n bit authentication.

6.5 Proof of Concept

This section discusses different aspects of the methodology including performance, storage requirements, and robustness. As seen in Table 6-2, there are 3 elements of the PUF that must be analyzed to evaluate the time taken to generate the parity bits PB_i and transfer the challenge bits C_i. Since the parity bits PB_i are generated using the Hamming code function, the response R_i that is generated by the PUF is used as an input. While this does come with the advantage of being more secure and requiring less data to be transferred, this also means the transferring of the calculation of the parity bits takes longer than simply using the response bits generated directly by the PUF. Nevertheless, the generation of the response bits and the calculation of the parity bits meets the requirements of the smart grid and can still be achieved in real-time. The number of bits used for the challenge C_i is 16 times (example: 16x128 = 2048) that of the response bits and, consequently, 16 times that of the parity bits. Since the transfer time of the challenge can be expected to scale linearly along with the number of bits in the challenge, the challenge typically takes 16 times as long to transfer, as seen in Table 6-2, which discusses the different levels of security defined by ANSI C12.22. Despite this increase in transfer time, it maintains real-time responses. Furthermore, the flat overhead created by implementing the blockchain, has no impact in the responsiveness of the communication, since this is done after the communication takes place.

Table 6.2: Authentication time for each level

Security Level	**R_i**	**PB_i**	**C_i**	**PB_i Generation Time (ms)**	**PB_i Transfer Time (ms)**	**Ci Transfer Time (ms)**	**Total PB_i and Ci time (ms)**	**Blockchain Transaction Time (ms)**	**Total Time (ms)**
1	128	128	2048	76.8	0.094	1.50	76.80	50	126.80
2	256	256	4096	153.6	0.0188	3.01	153.60	50	203.60
3	512	512	8192	307.2	0.0376	6.02	307.20	50	357.20
4	1024	1024	16384	614.4	0.0753	12.04	614.41	50	664.41
5	2048	2048	32768	1228.8	0.1506	24.08	1228.82	50	1278.82

The PUF implemented in this design is done so on an FPGA. This comes with the advantage of the PUF being easily reconfigurable. In the case of an attack, the PUF can simply be altered such that any predictive model is useless after reconfiguring. Furthermore, due to the volatile nature of the response bits generated by the PUF, it is difficult to launch an invasive attack on this aspect of the scheme, despite being in the most vulnerable of positions. Even in the case that the PUF on the FPGA is perfectly modeled, it would still be nearly impossible to fully infiltrate even a single SM without having complete access to that specific PUF's CPBPs. Assuming such an attack was able to succeed, it would still only give the malicious actor control of that single SM until the PUF is reconfigured.

Thus, the securing of the database containing all the challenges and their respective parity bits should be the highest priority. There are many obstacles any attacker would have to overcome before becoming a threat to the UC. While the database should inherently be more secure due to its firewall and physical location, attacks are theoretically possible. Fortunately, the system is reconfigurable such that any attacks may be rendered ineffective. Furthermore, due to the nature of the database, it is expected that it is easier to address problems in the case of a system failure, an attack, or some other fault.

The storage calculated in Table 6-3 is made by assuming that level 1 security exchanges take place every 15 minutes, as this is the most frequent communications are typically found, and that higher level security exchanges are made 5 times per day. However, the size of this changes based on the frequency of communications, such that the longer time between data exchanges, the less storage capacity required to authenticate over a similar period of time. If the devices exchange data every 15 minutes, there will need to be 35,064 CPBPs on average for each year. This means that one year of low-level authentications would take only 9.3 MB of storage. While this is low, since the storage is dependent upon the frequency of communications, it is possible to make this even lower by simply increasing the amount of time between communications. Assuming a 50-year lifespan of the AMI, one device will take a total of 1.187 GB of storage, as seen in Table 6-4. Thus, if the AMI contains a total of 2000 devices, the total storage required is only 2374.852 GB. However, this is also heavily impacted by communication frequency, and it may be realistic for this to be halved by limiting communication frequency. Nevertheless, even if the 15-minute period is maintained, the storage capacity is low for the entirety of the AMI's lifespan, meaning the protocol is efficient regarding storage requirements.

Table 6.3: Data storage size for each authentication level.

CPBP authentication level	**Year(s)**	**Data size (megabytes)**
First	1	9.257
	10	92.569
	20	185.138
	30	277.707
	40	370.276
	50	462.845
Second	50	48.213
Third	50	96.624
Fourth	50	193.248
Fifth	50	386.496

Table 6.4: Data storage size needed based on number of devices on the AMI.

Number of devices	**Data size (gigabytes)**
1	1.187
100	118.743
200	237.485
300	356.228
400	474.9704
500	593.713
600	712.456
700	831.198
800	949.941
900	1068.683
1000	1187.426
2000	2374.852

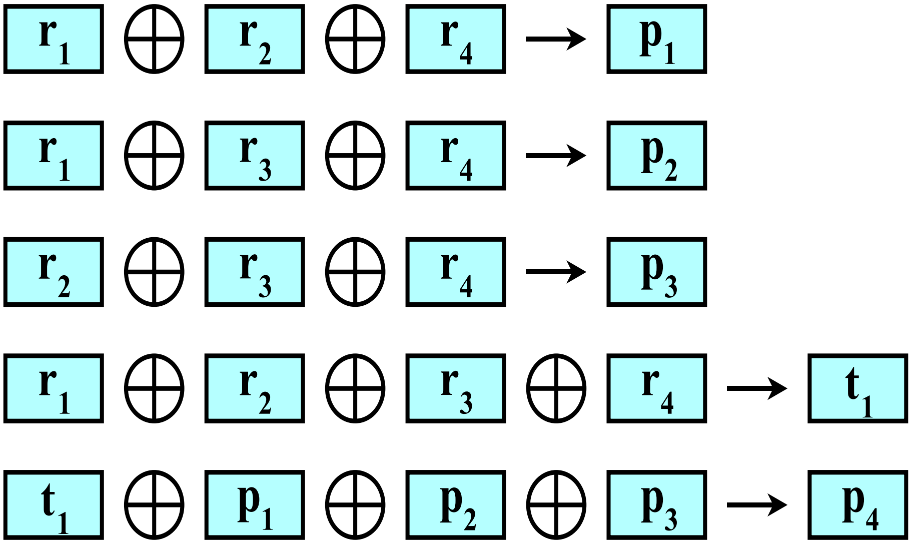

$r_1 \oplus r_2 \oplus r_4 \rightarrow p_1$
$r_1 \oplus r_3 \oplus r_4 \rightarrow p_2$
$r_2 \oplus r_3 \oplus r_4 \rightarrow p_3$
$r_1 \oplus r_2 \oplus r_3 \oplus r_4 \rightarrow t_1$
$t_1 \oplus p_1 \oplus p_2 \oplus p_3 \rightarrow p_4$

Figure 6-14: Parity Bit Generation.

To test the ROPUF security level, an ANN-based modeling attack is used to model the ROPUF based on the challenges (Ci) and parity bits (PBi). The parity bits are derived from ROPUF responses (R_i) using (8,4) parity bit generation as shown in Figure 14. The attack is performed based on the assumption that an adversary somehow manages to acquire a small set of Ci and PBi and tries to predict the parity bits for the remaining challenges. A sample of 10% of the available Ci and PBi is considered stolen. With this 10% of the data, ANN-based models have been trained using three different optimizations, namely, RMSprop, Adam, and Nadam.

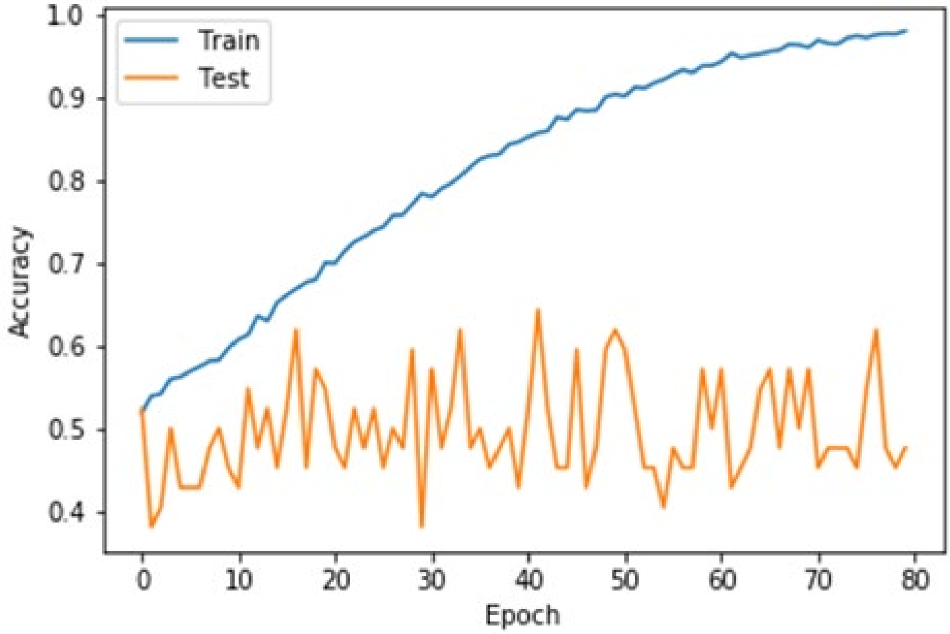


Figure 6-15: Training and Testing accuracy of (Ci, PBi) for RMSprop optimization.

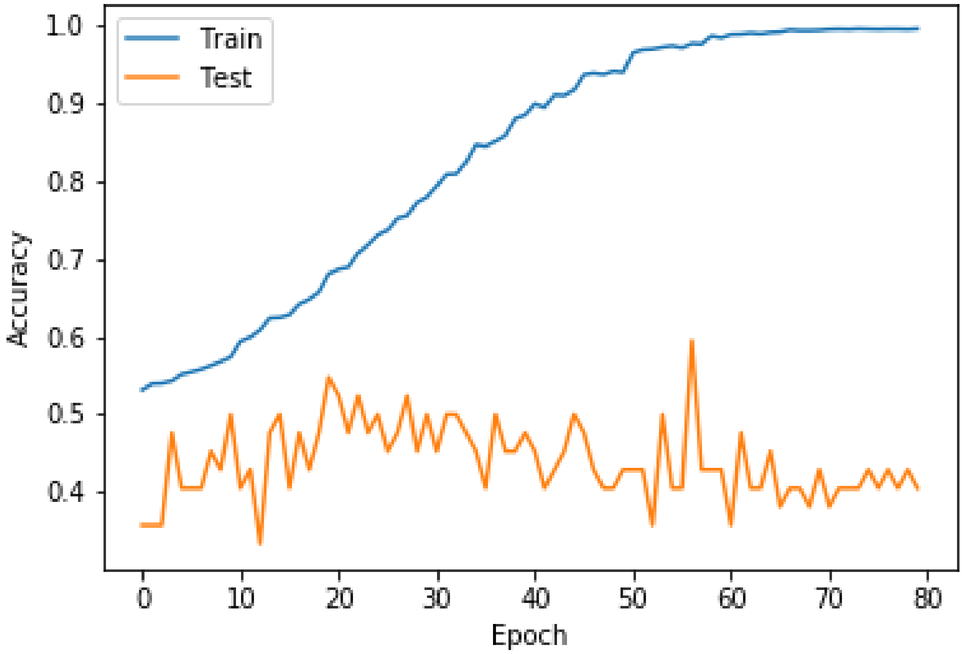


Figure 6-16: Training and Testing accuracy of (Ci, PBi) for Adam optimization.

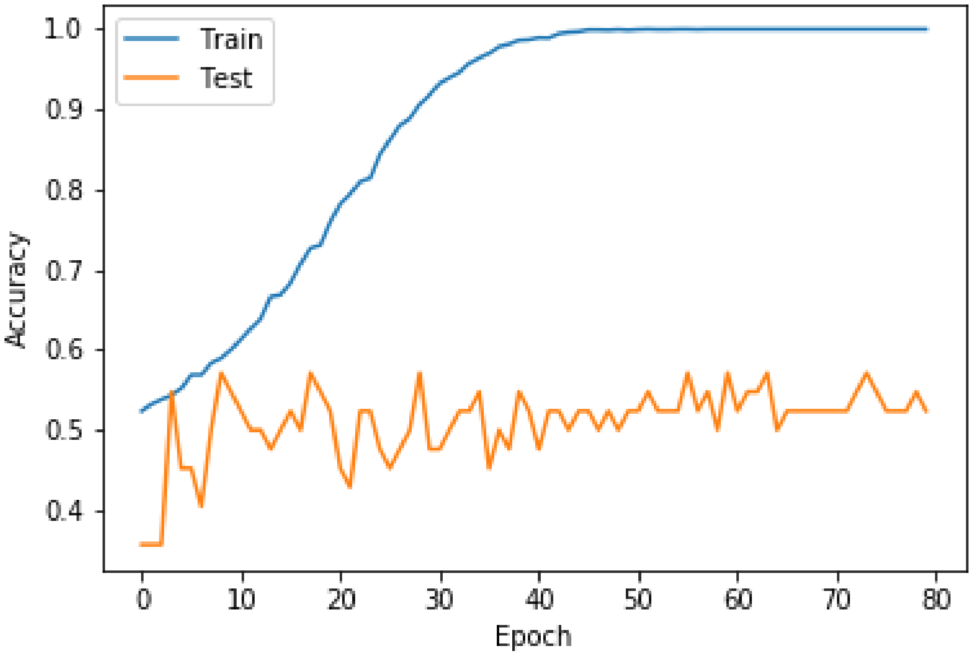


Figure 6-17: Training and Testing accuracy of (Ci, PBi) for Nadam optimization.

Figures 6-(15-17) show the training and prediction accuracy for ANN-based modeling using RMSprop, Adam and Nadam optimizers. Though the training accuracy reaches close to 100%, the prediction accuracy stays between 59-60.5%. The best accuracy is obtained for RMSprop optimization, which is 60.25%, showing that the Ci and PBi data cannot be used for predicting the remaining parity bits (PBi) from the remaining responses. This experiment justifies the use of ROPUF with PBi so that the AMI system is not harmed by modeling attacks on ROPUF.

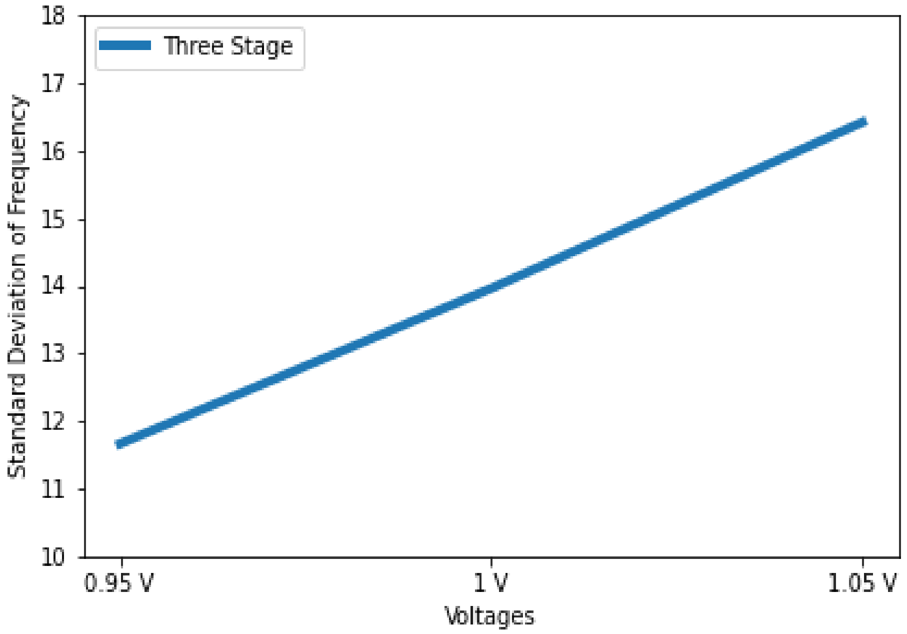


Figure 6-18: The standard deviation of frequency results for three-stage ROPUF under different voltages.

The authentication system is constructed using ROPUFs with comparison pairs that have a difference in frequency of 5 MHz or more [124]. This is because the closer two ROPUFs frequencies are to each other, the higher the chance of a bit flip scenario. Figure 18 illustrates the standard deviation of frequency for three-stage ROPUF of 16.41 MHz, which means there is a lower chance of a bit flip occurring. By increasing the minimum frequency between two ROPUFs, the chance of a bit flip caused by voltage spikes, advanced ROPUF age, or anomalous temperatures is heavily diminished. To further solidify against such scenarios, the system is built to tolerate up to a 10% discrepancy in PBi.

Table 6.5: Comparison of AMI layer of the smart grid with previous research on concepts implemented

Concepts/Previous Work	[122]	[124]	[125]	[135]	[142]	[143]	[144]	This work
Physically Unclonable Functions (PUFs)	✓	✓	✓	✗	✗	✗	✓	✓
Blockchain Technology	✗	✗	✓	✗	✓	✓	✗	✓
Zero Trust	✗	✗	✗	✓	✗	✗	✗	✓

Table 6-5 shows the different elements incorporated into the various authentication and permission systems in related literature. While there are many papers attempting to secure the AMI, no prior literature proposes an authentication scheme that is fully traceable while simultaneously fulfilling the ZTA tenets, which are discussed in Table 6-6. By creating a system that satisfies ZTA tenets, lateral movement can be entirely halted, and masquerade attacks are made much more difficult. Furthermore, the reconfigurability of the PUF and the usage of blockchain means that, even in the case of an attack, the damage can be quickly noticed and the system can be reconfigured, limiting the damage and making it easier for action to be taken that may repair or even nullify the damage caused. While individual literatures may support pieces of these capabilities using one or two of the three concepts, this is the first work to support all three concepts, and thus, combine the advantages that come with each.

Table 6.6: Implementation of ZTA tenets in the proposed work

Zero Trust Tenets (as defined by NIST)	**How each tenet is met**
All data sources and computing services are considered resources.	Every device within the AMI network is held accountable, and is only used for a specified task after requested
All communication is secured regardless of network location.	The data is completely encrypted by the sender and is not decrypted until received by the receiver in the AMI network
Access to individual enterprise resources is granted on a per-session basis.	All data transfers require initial authentication of both parties (UC and SM) and provides least privilege access to the data
Access to resources is determined by dynamic policy including the observable state of client identity, application/service, and the requesting asset and may include other behavioral and environmental attributes.	The access granted to either party (UC or SM) is least privilege for each individual session provided by the modifier and event functions of the smart contract.
The enterprise monitors and measures the integrity and security posture of all owned and associated assets.	Every data exchange is monitored and stored on the shared ledger of the blockchain
All resource authentication and authorization are dynamic and strictly enforced before access is allowed.	Both ends (UC and SM) of the data transfer are authenticated to each other using CPBP from ROPUF, and thereby the AMI network, every time some data is transferred
The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.	The implementation of the blockchain and the logging of every transaction allows for complete transparency of the AMI system

6.6 Summary

A novel authentication scheme and network security measures are proposed in this work. Utilizing ROPUFs for the authentication and blockchain for traceability, the scheme ensures a system that fulfills the ZTA tenets and minimizes the impact of any unforeseen attacks on the AMI. The use of ROPUFs rather than typical cryptography limits the effectiveness of physical attacks and the use of Hamming code parity bits over the response bits limits the effectiveness of machine learning attacks. The authentication times for L1 and L2, the most common security levels, are 126.80 ms and 203.603 ms, respectively, satisfying the real-time requirements of such a system. In addition, due to the scheme's use of FPGAs, new design and technology can be retroactively fitted into current smart meters making them future proof.

Furthermore, through the implementation of blockchain technology, communications are fully traceable, allowing for ease in investigation and establishing the trustworthiness of the AMI network. Not only the proposed scheme satisfy the requirements of ZTA, but by making the transaction data on the blockchain available to all nodes, the data becomes immutable and secure.

Chapter 7

Hardware Trojan detection using power side channel analysis and ROPUF

7.1 Introduction

Due to the rapid globalization of the supply chain, the use of integrated chips (ICs) has increased exponentially. Expensive IC fabrication is outsourced to save costs, but it gives the window for Trojan intrusion. Hardware Trojans are inserted into the circuit through physical modifications made during the fabrication process. Third-party manufacturers are responsible for designing, testing and final fabrication of these chips [155]. Trojans are more susceptible to intrude during the rather complex design and testing stages of fabrication and supply chain of IC manufacturing. ICs are widely used in many different vital systems and any attack on ICs can cripple the whole infrastructure of hardware and software systems.

To avoid and detect malware various post-processing tests such as structure, functional testing and brute force testing are designed, however, hardware Trojans are hard to detect and usually evade these tests. Similarly, reverse engineering can be used for the detection of Trojans in ICs but, again, this process lacks the capabilities to detect Trojans efficiently. Different types of Trojans can have different functionalities, such as data leaks and power consumption, that lead to changes in the intended functionalities and reduced reliability for system hardware.

Hardware-based Trojans are activated through a two-stage mechanism: trigger and payload. The trigger part in hardware Trojan signals to activate the payload. Once the payload is activated, the functionality of Trojans comes into play. Hardware Trojans can remain dormant and undetectable if the Trojan is not activated through trigger and payload. Hardware Trojans are classified based on functionalities and other features such as location, payload, trigger, abstraction capability and insertion phase. Trojans could be activated through these mechanisms and once activated, Trojans can severely disrupt military, financial, education, health, transportation systems, and daily-use appliances. Hardware Trojans can leak sensitive information and data, posing a serious threat to modern systems [156].

Various research studies analyzed methods and modifications of system hardware to insert Trojans. Techniques such as the alteration of open-sourced Lean processor and wear out of silicon material were analyzed by research studies [157, 158]. Trojan detection methods range from restructuring to non-destructive nature. Destructive testing methods are based on taking apart the components in circuit to physically examine the parts and chips. While non-destructive methods do not involve taking apart the components, these tests examine different system parameters such as in the side channel analysis.

A side channel analysis is a non-destructive and effective approach used in the detection of hardware Trojans. Side channel analysis considers the side channel parameters that include change in current, power consumption, and other response delays for a chip. This is a straightforward approach to avoid extensive Trojan detection methods. Any alteration in the side channel behavior due to the activation of malware in IC can detect the presence of Trojans. Noise and Other variations in the environment are important factors influencing the efficiency of side channel attacks. These factors can mask the variations in the side channel parameters, making it difficult to detect Trojans. Another important influencing factor in the detection of Trojan is the process variation. This affects the side channel measurements that can significantly reduce the sensitivity of Trojan detection [159]. Moreover, the sensitivity of the Trojan detection is also affected with the increase in circuit size. Narasimhan et al. offered a unique non-invasive, multiple-parameter side-channel analysis-based Trojan detection technique. The inherent link between a dynamic current along with the maximum operating frequency for a circuit was exploited to isolate the influence of a Trojan circuit from process noise. A vector-generating strategy and multiple design/test techniques were presented to boost detection sensitivity. Results from simulations using two big circuits, a 32-bit unit with integer execution and a 128-bit advanced encryption standard (AES) algorithm, indicated a detecting resolution of around 1.12 percent despite parameter variability of 20%. Experimental findings were also used to validate the strategy. Finally, it was demonstrated that using a combined side-channel analysis and logic testing technique provides effective detection accuracy for hardware Trojan circuits of various sorts and sizes [159].

Authors in [160] analyze the hardware Trojan testing using a unique test approach that combines logic and side-channel testing. As a golden circuit, an 18-bit CORDIC IP core was used, while a 2-bit counter was used for a Trojan circuit. The automated testing platform included a LabVIEW software, Xilinx FPGA, and a higher-accuracy oscilloscope. Moreover, the power traces of FPGA power supply VCCINT and VCCAUX were also monitored to improve detection sensitivity for hardware Trojans. When the principal component analysis methodology was used for the data processing algorithm, the experimental findings showed that the innovative test method may easily reach around 0.1% Trojan detection sensitivity [160].

This research proposes power consumption and ROPUF frequency-based Trojan detection techniques. For each technique, three different design configurations are analyzed. These configurations include the Trojan-free design (or the golden design), the design with an inactive Trojan, and the design with an active Trojan. This approach monitors the channel parameters of RO delay paths through power side-channel analysis and ROPUF frequency-based detection.

7.2 Related Work

A hardware Trojan is a malicious circuit alteration made by the adversary. The system's creator was unaware that it could have unfavorable impacts on the system, such as incorrect operation or the loss of confidential information. During wars, adversaries employed the Hardware Trojan to eavesdrop on each other's communication signals [161]. Another instance is that the chips might be hacked, equipped with the ability to turn off a missile in the case of a war, or simply waiting to break down [162]. The detection of Trojans has been divided into two categories. One uses non-destructive techniques and the other uses destructive ones.

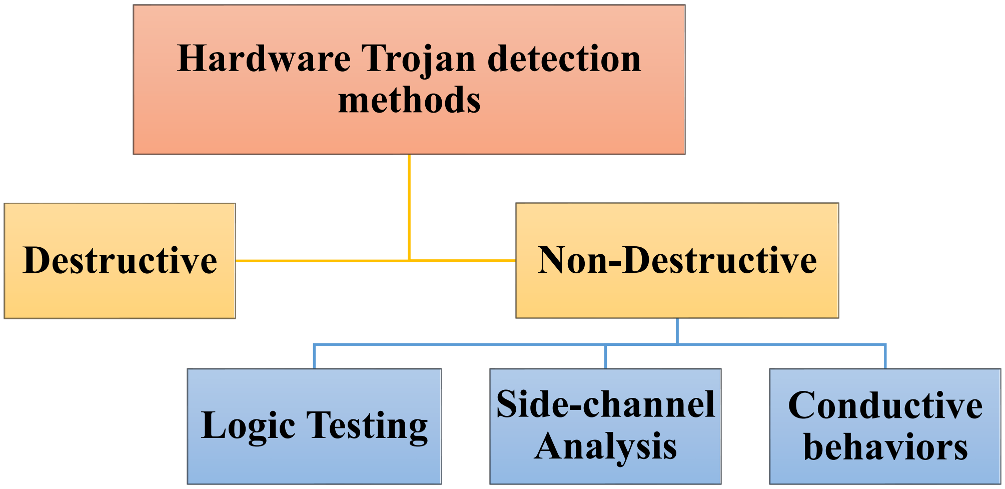


Figure 7-1: Hardware Trojan detection methods category.

7.2.1 Destructive

IC that is examined by the destructive methods for the identification of malicious circuitry and destroyed, which reduces the applicability of such procedures. Numerous ways of solving this critical problem of detecting the hidden Trojan have been discussed earlier. Long-term transistor aging was proposed, where overclocking and aging produce enough combinations of output bit abnormalities to identify the Trojans [156]. The work in [163] discusses short-term aging, where voltage scaling is used to generate aging at sustainable levels and overcome the problems that can occur with long-term aging of transistors, which have a negative effect on the circuit and cause permanent damage . To locate known good ICs, authors in [164] apply reverse engineering using destructive techniques and discuss that it is possible to create reliable fingerprints for a family of ICs to find Trojan ICs.

7.2.2 Non-Destructive

Non-destructive approaches for Hardware Trojan detection are either intrusive or non-intrusive depending on whether they damage the IC being examined. While invasive techniques alter the design to embed elements that help with Trojan detection, non-invasive strategies leave the design intact.

7.2.2.1 Logic testing

Trojan detection with multiple parameters used in the side channel analysis uses a technique to uncover small Trojans, which are challenging to detect. It is done by exploiting the inherent link between dynamic current and the maximum operating frequency of a circuit to separate the impact of a Trojan circuitry from process noise [159]. A different methodology has been used for Trojan detection with multiple parameters where a logical testing approach, a run-time approach, and a side channel analysis method are employed [165]. These techniques are categorized into functional behavior analysis and finding hidden features based on investigating the IC's logic structures [166]. In [162], the researchers discuss a comprehensive solution where a Trojan-aware design is presented with post-silicon validation, including logical testing, online observation of crucial circuit functions, and side channel analysis analyzed with supply current. The approaches to logic testing and side channel analysis are non-intrusive. In contrast, the run-time process necessitates using on-chip digital sensors to find unanticipated differences in the IC's layout. Logic testing, as used in [167], is one technique that can be used with side channel analysis. In this technique, test patterns are obtained using numerous infrequent logic value excitations at internal nodes, which can trigger and detect hidden Trojans.

7.2.2.2 Side Channel Analysis

Ring oscillator-based side-channel analysis with analysis of variating frequencies was discussed in [87], where the Nand-based oscillator’s frequency comparison is used to detect the Trojan. They have a more significant effect on the frequency of neighboring ROs. Also, a circuit partitioning technique is employed to increase the Trojan's power consumption ratio to the host circuit's power consumption. A side-channel backscattering approach was proposed in [168], which is produced by a signal being transmitted in the direction of the IC. A novel technique for the non-invasive detection of Trojans outside of the chip was discussed. In the simulation scenario, a hardware Trojan is inserted into 8 of the 16 circuits to find the Trojan in the infected circuit using techniques like spectrogram and neural networks [169].

The researchers of [170] attempt to identify the hardware Trojan by calculating the time difference between the gates on the circuit. The described method generates a probabilistic fingerprint based on the calculated delay between the circuit's gates and compares it to the two results of other circuits. Authors in [171] propose a way of observing Trojan activity in the circuit using current integration and a method for isolating the Trojan using localized current analysis. If the current integration results fall outside the golden chip, the Trojan can be detected by comparing the results obtained for golden chips against the chip-under-authentication.

7.2.2.3 Conductive behaviors

In this approach, an additional structure is introduced to the circuit before the manufacturing step is complete in order to detect the Hardware Trojan. Most frequently, this additional component is a miniature circuit, or a component of the circuit known as Design for Hardware. In [172], the researchers suggest adding dummy flip-flops to the circuitry to enhance Hardware Trojan activity, which will facilitate side-channel techniques and increase the possibility of Trojan detections. [172].

7.3 Experimental Setup

7.3.1 Implementation on FPGA

Xilinx Artix-7 XC7A100T boards are used in this research to implement the ROPUF and the Trojan.

7.3.1.1 Architecture of the Xilinx Artix-7 FPGA

The layout of the Xilinx Artix-7 FPGA XC7A100T chip is shown in Figure 7-3. This FPGA uses 28 nm technology and contains 101,440 gates in 15,850 configurable logic blocks (CLBs) [102]. The CLBs are distributed across 200 rows and 82 columns, as shown in Figure 7-3. Each CLB in this FPGA consists of four identical slices. Each slice comprises of four look up tables (LUTs) and flip-flops. Hence, there are four 6-input LUTs in each CLB, along with eight flip-flops.

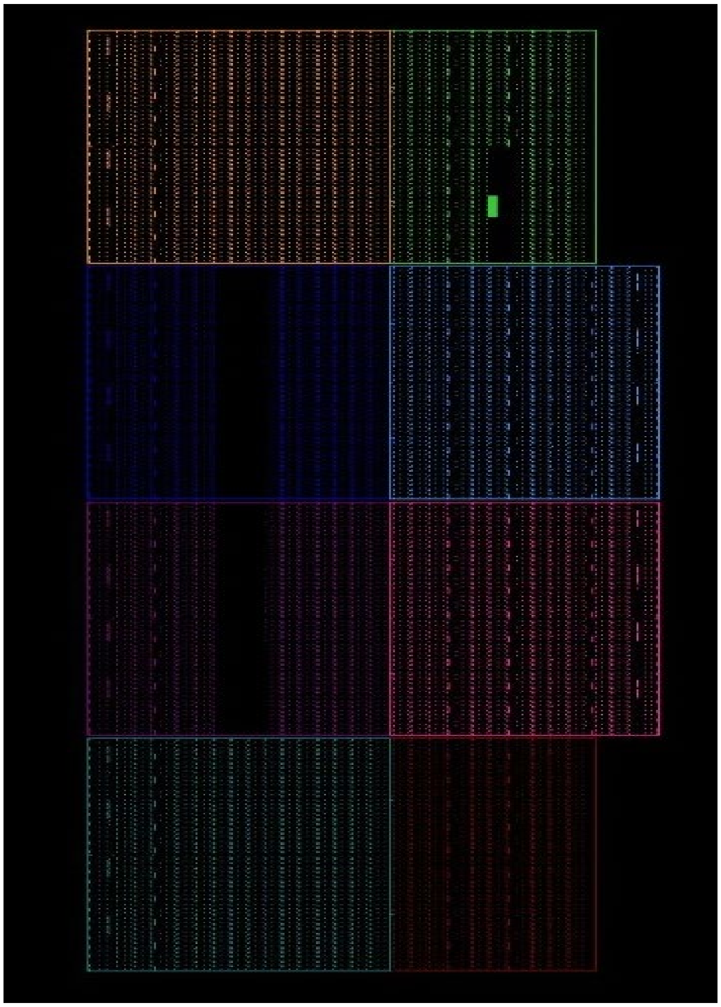


Figure 7-2: Xilinx Artix-7 FPGA architecture.

7.3.1.2 Ring Oscillator PUF Structure

For a given challenge, a ring oscillator generates a one-bit response by comparing the frequencies received from two oscillators. The proposed design consists of a single AND gate and an odd number of inverter gates. A three stage ROPUF consists of one AND gate and three inverter gates. Figure 7-3 shows the component level layout of the three stage ROPUF mapped on an Artix-7 FPGA. The three stage ROPUF utilizes 4 LUTs. A total of 512 Ring Oscillators are used in this design as shown in Figure 7-5. Each RO is manually mapped using the FPGA Editor tool in order to have identical ROs placed at different spatial locations of the FPGA. Figure 7-4 shows the floorplan layout of the RO hard macros on one CLB taken from the Xilinx FPGA Editor. In the figure, the RO is shown in red color with small circles inscribed on it. It is important to note that the correct placement of the ROs within the FPGA is of critical importance for obtaining accurate results. In our design, challenges for choosing the ROs are produced through a 10-bit challenge generator. After the challenge is applied, the frequency counter is switched on for 0.4 ms to measure the frequency response. A 0.1 ms delay is used between challenges to select the next RO.

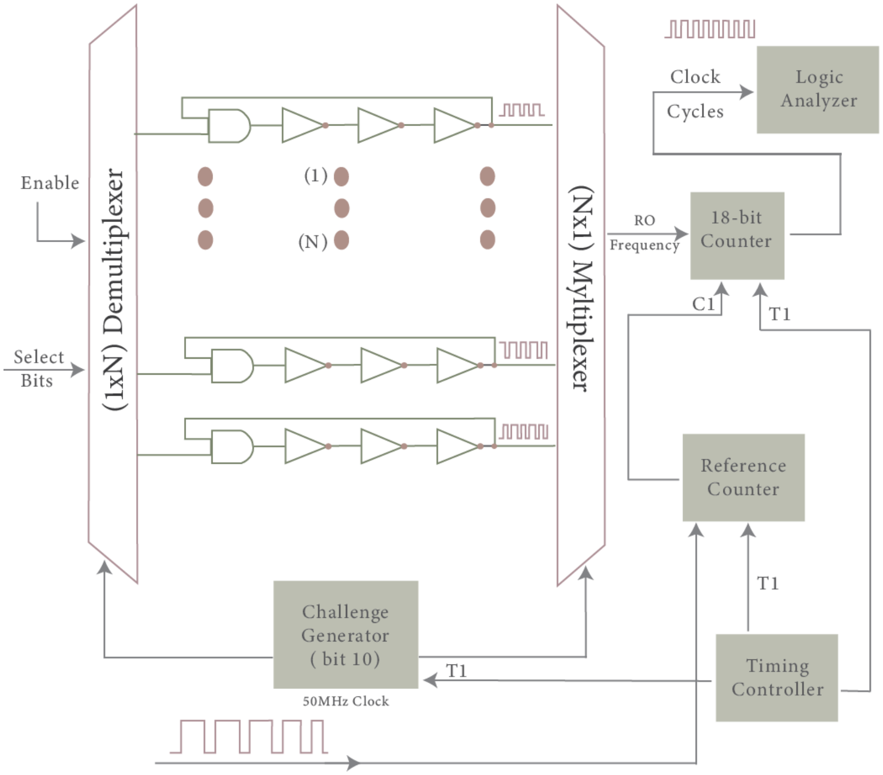


Figure 7-3: Block Diagram of 3-Stage ROPUF.

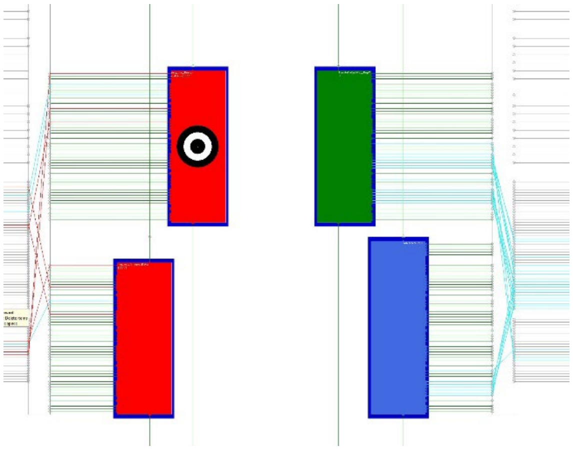


Figure 7-4: Floorplan layout of the RO hard macros on one CLB.

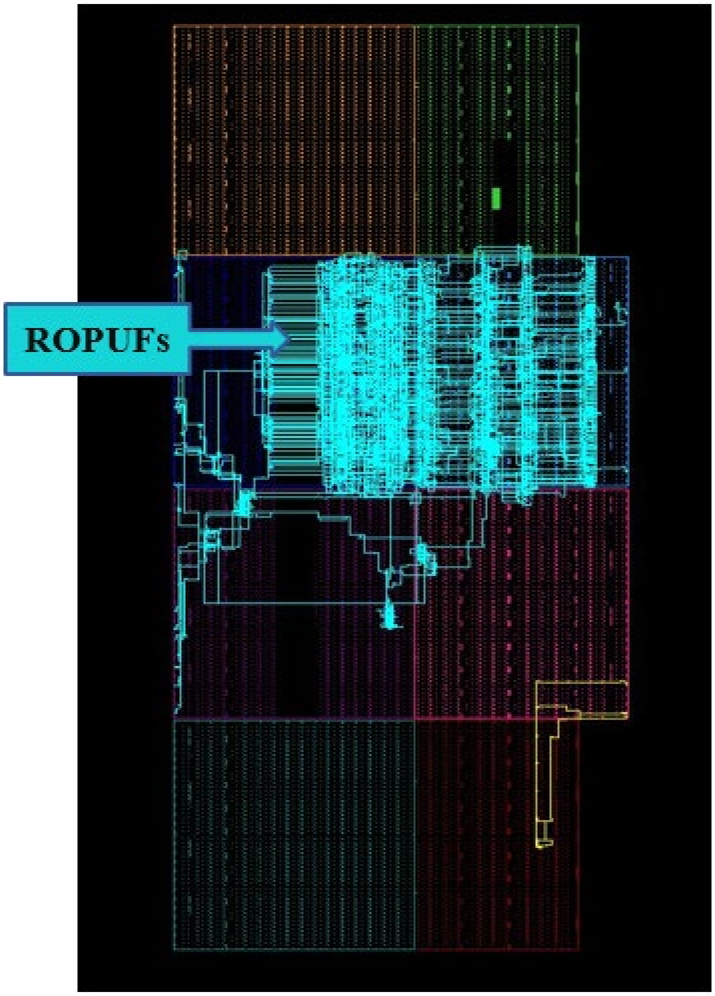


Figure 7-5: 512 Ring Oscillators mapped on an Artix-7 FPGA board.

7.3.2 Trojan Design

The Trojan design has five logic gates: three AND gates, one NOT gate, and one XOR gate as shown in Figure 7-6. The Trojan gates are manually placed at six different locations on the FPGA as shown in Figure 7-7. These Trojan gates are manually placed in the 2 empty slices that were kept empty in the Trojan Free version of the design. The functionality of the Trojan is such that it adds delays in the circuit when enabled. Any malicious hardware Trojan placed into a trusted design will consume leakage power, the amount of which is typically proportional to the Trojan's size. It will also add to the Trojan's dynamic power if any switching activities are conducted. Therefore, power analysis techniques can be utilized to discover the differences in side-channel information between trusted and untrusted integrated circuits [173].

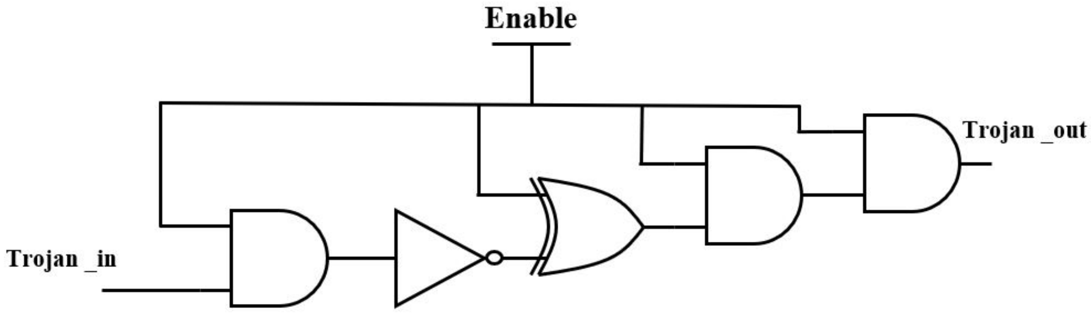


Figure 7-6: Proposed Trojan design.

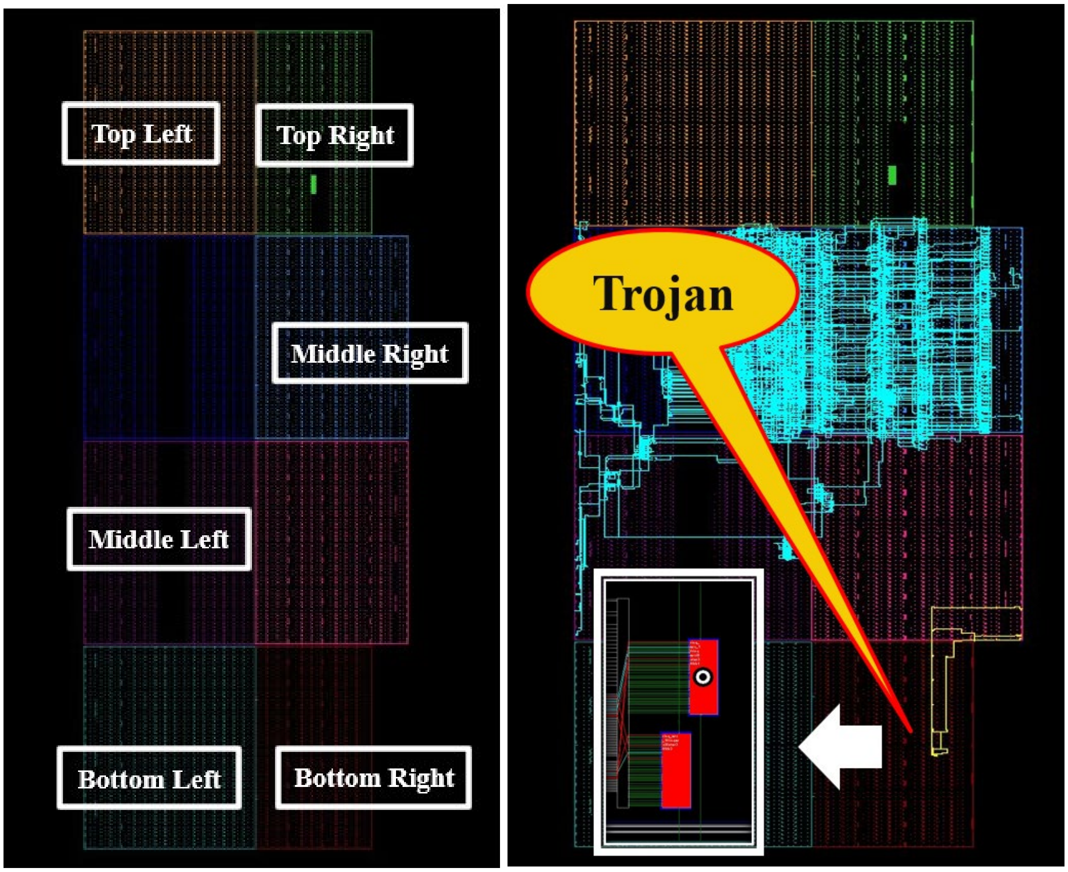


Figure 7-7: The Trojan is placed at six different locations on the FPGA.

7.4 Measurement Flow

Our approach is to detect the trojan using two different methods: 1) analyzing the power consumption and 2) ring oscillator PUF frequency based on three configurations of the design.

- Trojan Free Design
- Design while Trojan is inactive
- Design with Active Trojan

First, we analyzed the Trojan-free design (or the golden design), the design while the Trojan is inactive, and the design with an active Trojan. In this experiment, the ROPUFs are programmed on ten different FPGA boards, and a power analyzer is used to record the power consumption pattern. At the same time, the logic analyzer is used to record its frequency response, as shown in Figure 7-8. After performing this experiment for the three design configurations for board 1, the experiment is repeated with the other nine FPGA boards.

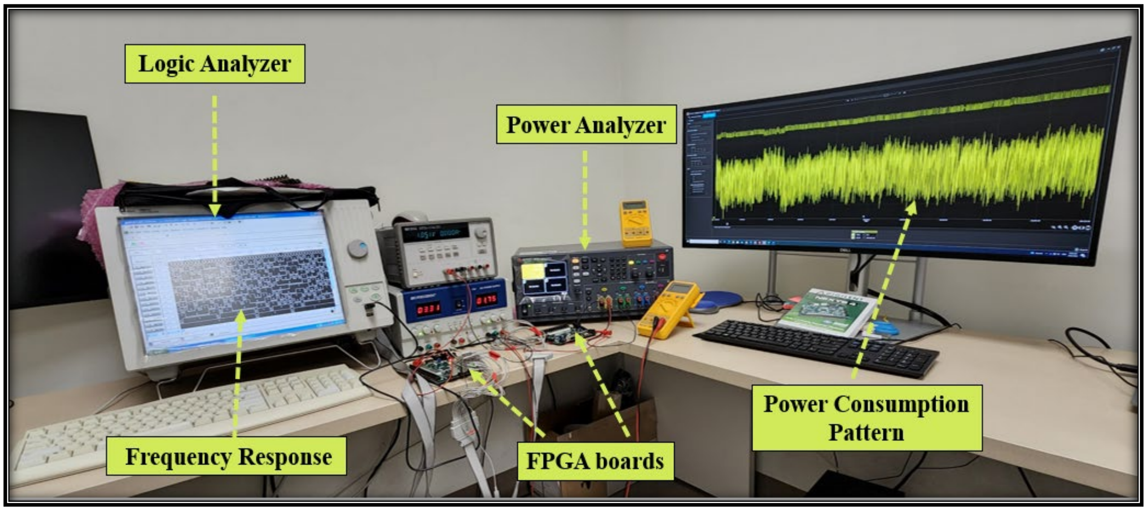


Figure 7-8: Our experimental setup for power consumption patterns and frequency response data collection.

7.5 Experimental Results

In this section, the impact of a hardware Trojan on a specific RO of an FPGA is evaluated by comparing it to the same reference RO of the same FPGA's Trojan-free version. We use two approaches for hardware Trojan based detection by comparing the same ROs between the Trojan and Trojan free versions of FPGA. The first approach is based on side channel analysis and the second is based on a ring oscillator PUF frequency based detection approach.

7.5.1 Side Channel Analysis based approach

In the side channel analysis based approach, we have taken three case studies. The first case involves a circuit that contains no Trojans at all. The second contains a Trojan, but it is inactive. The third circuit contains an active Trojan. From Figure 7-9, we can see that the current and voltage behavior are nearly uniform when the Trojan is not present in the circuit. On the other hand, Figure 7-10 shows the fluctuation of the current drawn by the design when we include the Trojan in the circuit, indicating that the Trojan is active. Based on this information, we can conclude that a Trojan is present in the circuit, and this is how we detect the Trojan's presence in the circuit.

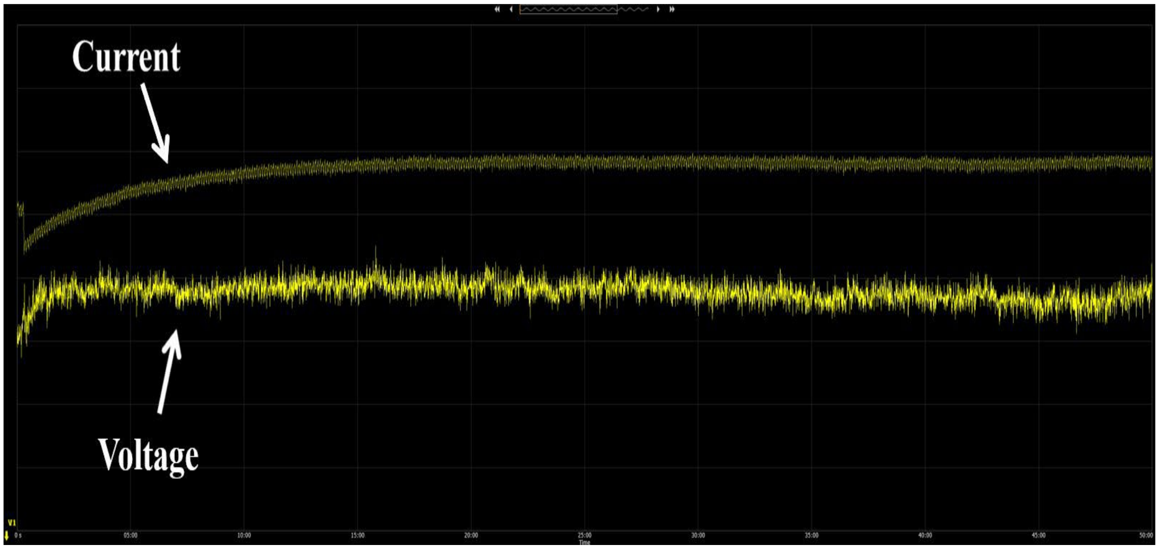


Figure 7-9: Voltage and current measurements for the ROPUF during operation with No Trojan in the logic.

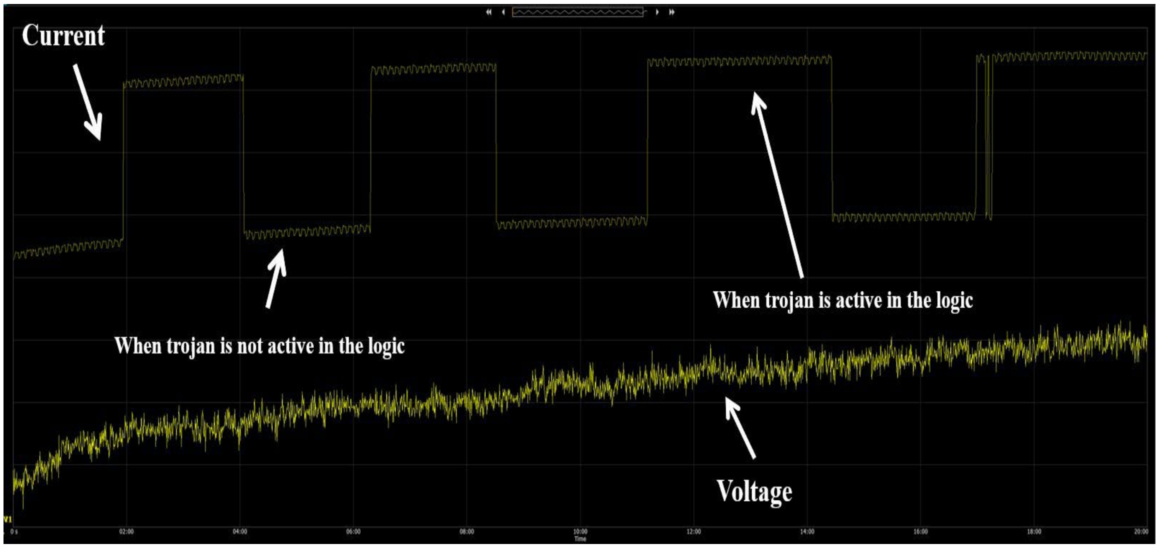


Figure 7-10: Voltage and current measurements for the ROPUF during operation with Trojan in the logic not active and active.

7.5.2 Ring Oscillator PUF frequency based detection approach

For the Ring Oscillator PUF frequency based detection approach, we have done a similar three case studies. The first case involves a circuit that contains no Trojans at all. The second contains a Trojan, but it is inactive. The third circuit contains an active Trojan. Figure 7-11 shows that when the Trojan is not present in the circuit, the ring oscillator frequency is almost identical with a few variations, but it ranges from 48,309 to 50,855. However, Figure 7-12 shows the Trojan is inserted but not activated; we can see that the frequency output of the ring oscillator varies greatly. This is due to the Trojan being in the circuit, mapped but not active, and still causing output delays. For the third study case, the Trojan creates increased delays when the Trojan is inserted and activated. In this frequency-based detection approach, the difference between the Trojan being active and not active is observed from a different set of data. Figure 7-13 represents the additional frequency variation delays, which are denoted by red circles.

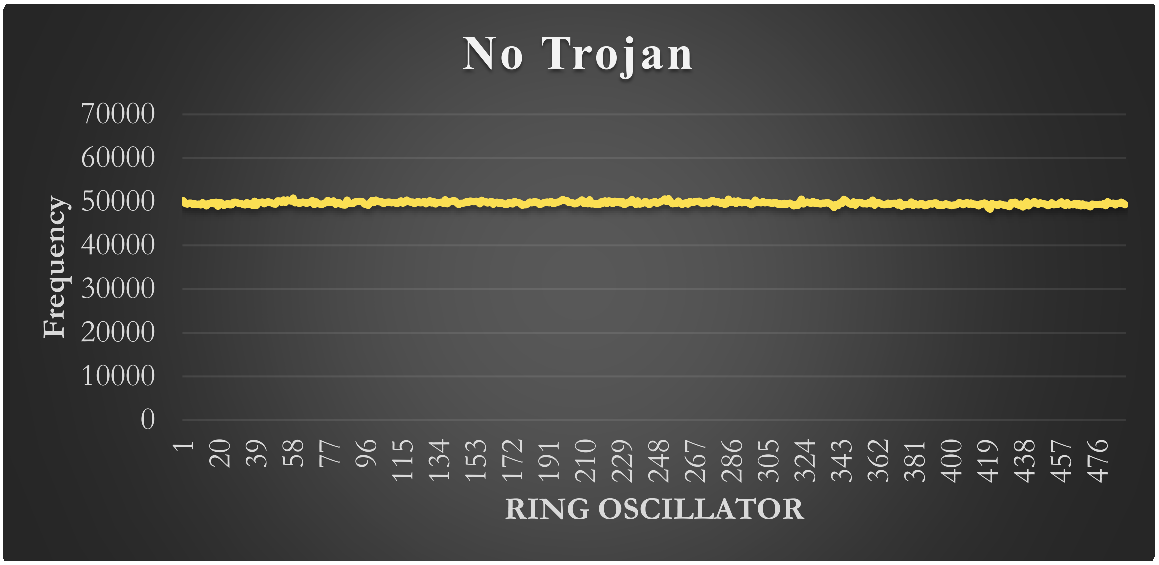


Figure 7-11: Frequency for the ROPUF from the Logic Analyzer with No Trojan in the logic.

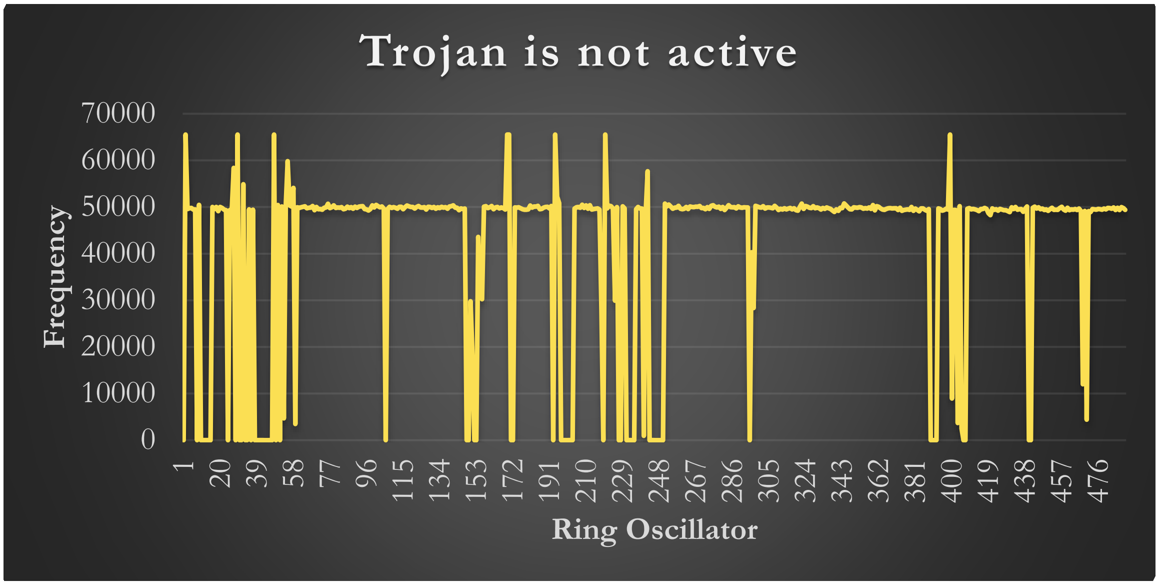


Figure 7-12: Frequency for the ROPUF from the Logic Analyzer with Trojan in the logic not active.

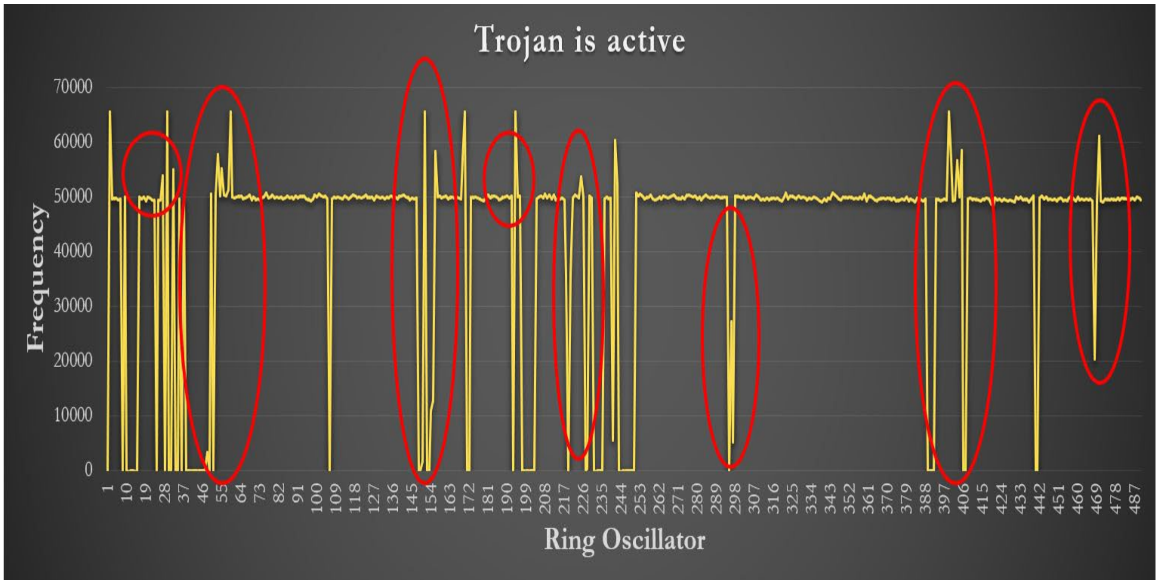


Figure 7-13: Frequency for the ROPUF from the Logic Analyzer with Trojan in the logic is active.

Based on the results of the power side channel analysis approach, we are unable to locate the Trojan. However, using the frequency-based detection approach, we are able to locate the Trojan while it's present in the circuit if it is close to or far from the ROPUF design. The frequency has fluctuated significantly more in Figures 7-14 and 7-15, which indicates Trojan designs that are close to the ROPUF design, than in Figures 7-16, 7-17, 7-18, and 7-19, which show Trojan designs that are far away from the ROPUF design.

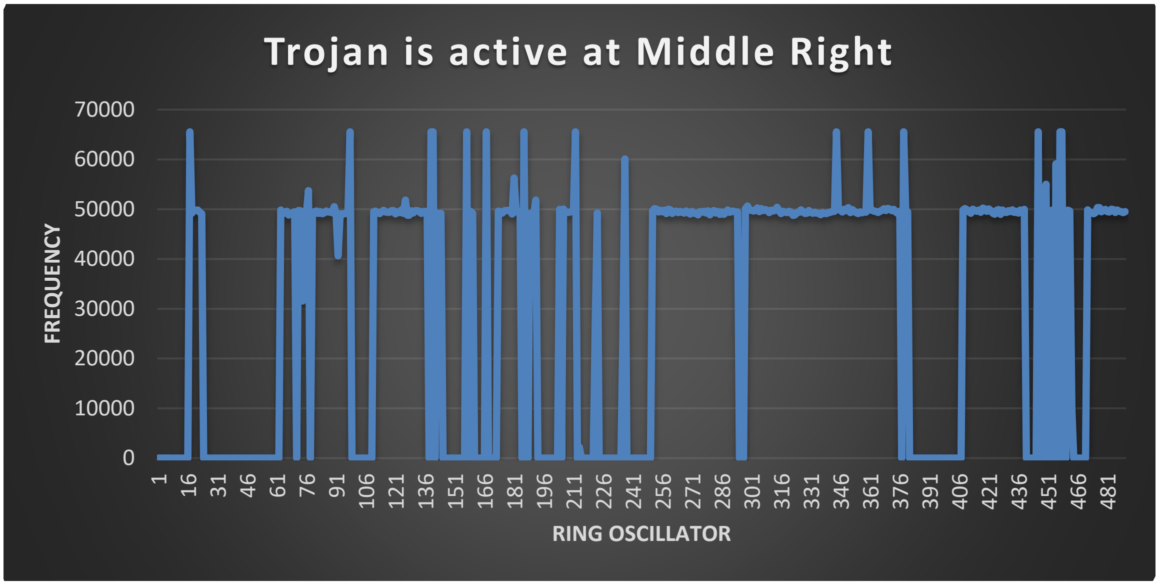


Figure 7-14: When the Trojan is placed on the middle right region of the Artix-7 chip which is the closest to the ROPUF design.

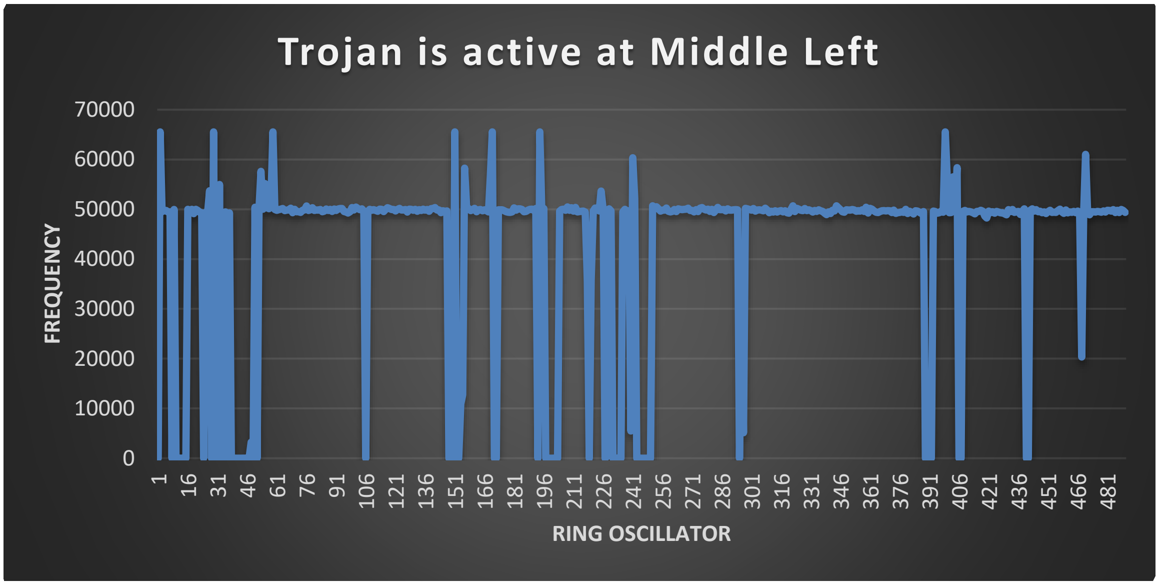


Figure 7-15: When the Trojan is placed on the middle left region of the Artix-7 chip which is the close to the ROPUF design.

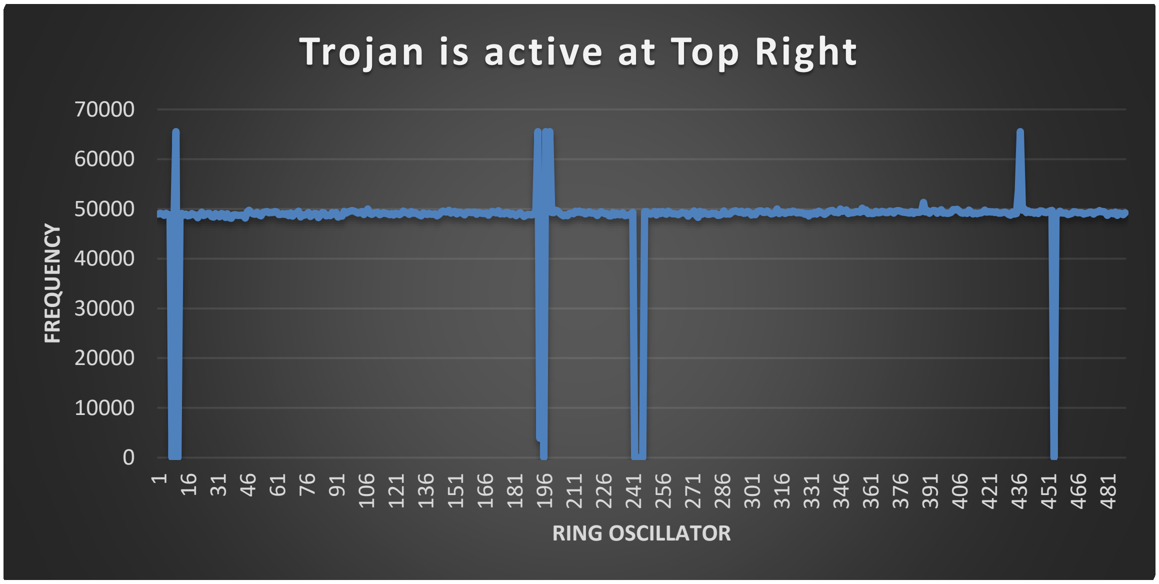


Figure 7-16: When the Trojan is placed on the top right region of the Artix-7 chip.

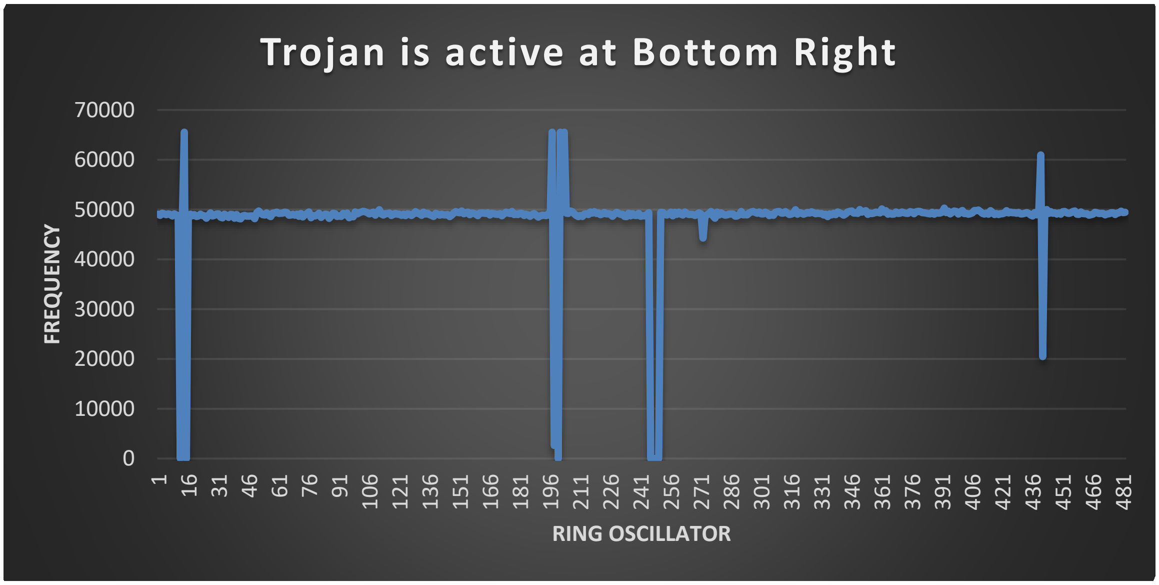


Figure 7-17: When the Trojan is placed on the bottom right region of the Artix-7 chip.

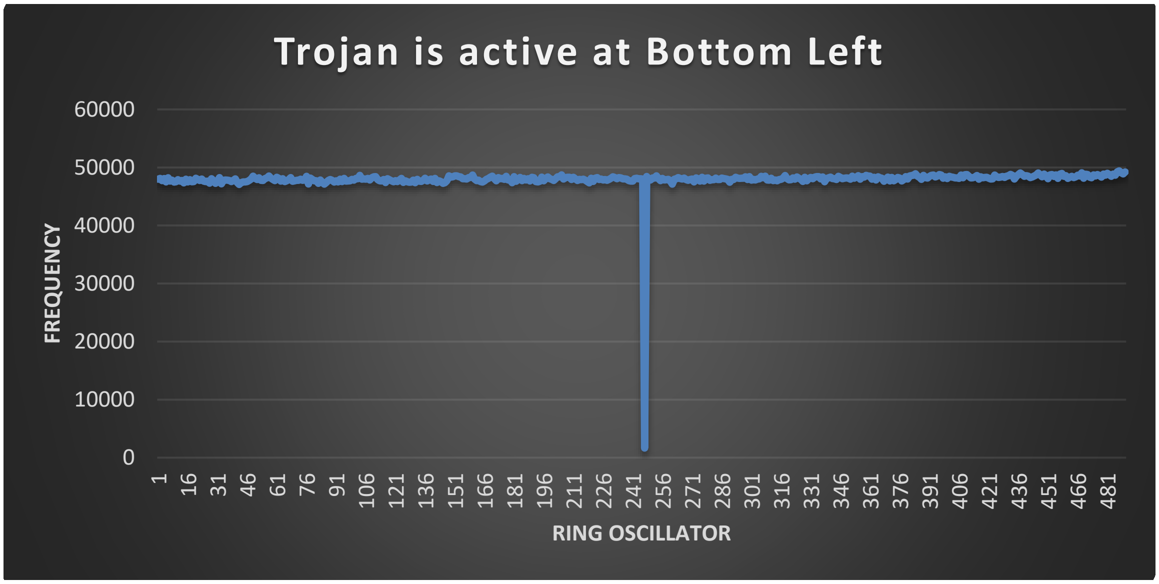


Figure 7-18: When the Trojan is placed on the bottom left region of the Artix-7 chip which is the farthest from the ROPUF design.

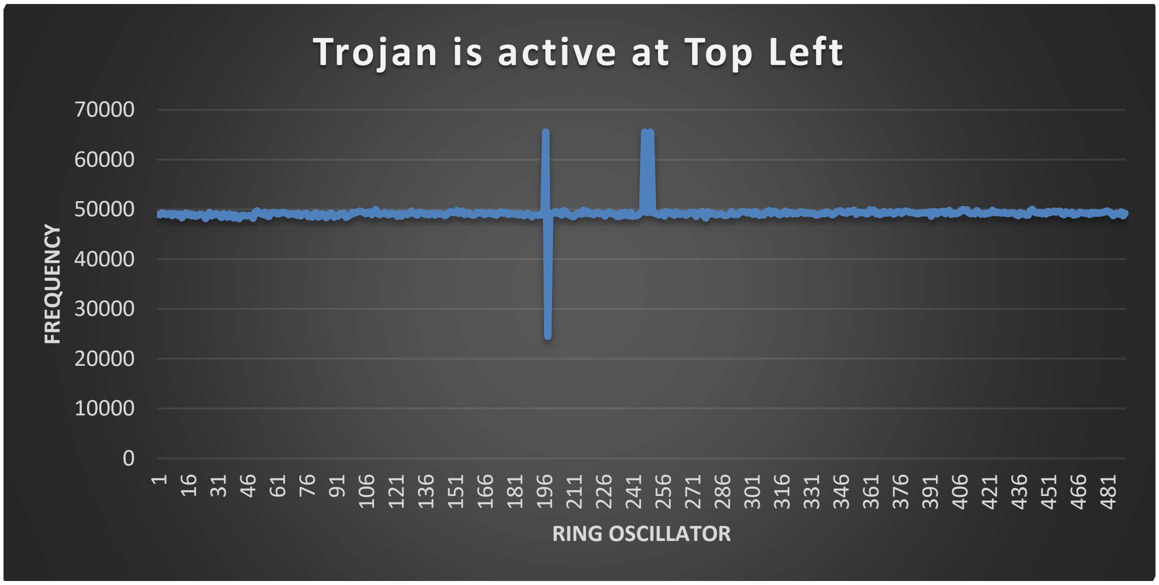


Figure 7-19:When the Trojan is placed on the top left region of the Artix-7 chip which is the farthest from the ROPUF design.

7.6 Summary

In this chapter, we presented techniques for the detection of hardware Trojans. These techniques are based on side channel analysis and Ring Oscillator PUF frequency-based detection approach. The proposed technique not only detects the Trojan but also facilitates in determining its location. The results show that both our proposed side channel analysis and the Ring Oscillator PUF frequency based detection techniques are visible. The experimental results show that the frequency-based Ring Oscillators near the Trojan have a higher frequency variation than the other Trojan locations.

Chapter 8

Conclusions

8.1 Summary and Conclusions

Hardware security is becoming an important part of the latest technologies employing integrated circuit chips. The hardware supply chain's complexity makes them more vulnerable to malicious attacks and Trojans. Different research publications have pointed out the use of old components disguised as new, making them vulnerable to sensitive private and public data systems. In 2011, Boeing informed the US navy regarding a possible Trojan in an FPGA chip being used in various sensitive hardware in military installations [174]. The specific chip was being used in P-8A aircraft. It was concluded that a third party that was responsible for manufacturing these chips made it possible for Trojans to penetrate the hardware and chips. It was found that a Chinese company supplying these parts was using re-used parts. As FPGA is becoming vital for various industrial and military applications, it is important to enhance the security of these systems to avoid future attacks [175]. Therefore, trust and hardware security vulnerabilities must be overcome with the implementation of appropriate security systems. The 2011 incident highlighted the extensive use of FPGA and other programmable chips along with the vulnerabilities of these chips in a global supply chain. These vulnerabilities lead to some very alarming security and safety concerns in sensitive systems. It is increasingly important to improve the security of these devices. Various techniques are used to overcome the issues of security. Unique IDs are used for verification and secret keys in PUFs. ROPUFs are used in the encryption and decryption of data through cryptography techniques [176].

The dissertation explains and analyzes various effects of temperature, voltage, and aging on the Ring Oscillator PUF. Aging factors cause some irreversible changes for components in the circuit that result in permanent changes in circuit behavior and parameters [177]. ROPUFs are sensitive to voltage and temperature variations. It is easy to get randomness and uniqueness for well-designed PUF systems. However, it is a challenge to achieve higher reproducibility for responses.

Physical implementations and various performance measurement approaches for three, five, and seven-stage configurations of AND-Inverter ROPUFs are analyzed. The performance is studied using uniformity, reliability, bit-aliasing, uniqueness, and randomness. The impact of voltage, temperature variation, and aging are evaluated in depth for these metrics. It is found that the lower number of stages in the Ring Oscillator (RO) promises better security. The high number of CRPs significantly enhances the overall security of PUF systems. Furthermore, this work analyzes two simultaneous environmental variation factors, namely, aging and voltage variations, and temperature variations with voltage variations. To our knowledge, the impact of aging with varying voltages has not been studied before. The results show that ROPUF performance is sensitive to changes in operating temperature and voltage. From the experimental data, it can be concluded that the impact of temperature with voltage variations increases for all metrics for each configuration of the ROPUF. For the three stage ROPUF, the impact of aging is minimal, whereas aging is more evident in five stage and seven stage ROPUFs. It is observed that the three stage ROPUF performs better and is suitable for different applications than the five and seven stage ROPUFs.

A novel authentication scheme for the Advanced Metering Infrastructure (AMI) employed in a smart grid is also proposed in this dissertation. Utilizing ROPUFs for authentication and blockchain technology for traceability, the scheme ensures a system that fulfills the ZTA tenets and minimizes the impact of any unforeseen attacks on the AMI. The use of ROPUFs rather than typical cryptography limits the effectiveness of physical attacks, and the use of Hamming code parity bits over the response bits limits the effectiveness of machine learning attacks. The authentication times for the most common security levels L1 and L2, are found to be 126.80 ms and 203.603 ms, respectively, satisfying the system's ANSI real-time requirements. In addition, the scheme's use of FPGAs allows for retrofitting new designs and technology into current smart meters, making them future-proof. Further, by utilizing blockchain technology, communications are fully traceable, allowing for ease of investigation and establishing the AMI network's trustworthiness. The proposed scheme not only enhances the requirements of ZTA but also makes the transaction data on the blockchain immutable and secure by making it available to all nodes.

Finally, this work presents techniques for the detection of hardware Trojans. These techniques are based on side channel analysis, and Ring Oscillator PUF frequency-based detection approach. The proposed technique not only detects the Trojan but also facilitates in determining its location. The experimental results show that the frequency-based Ring Oscillators near the Trojan have a higher frequency variation than the other Trojan locations.

8.2 Contributions

The contributions of this research are summarized as follows:

- Design and implementation of a new AND-Inverter based ROPUF. Experimental results show that the ROPUF exhibits improved performance parameters when compared to previous ROPUF designs.
- Use of Artix-7 Xilinx FPGA family to explore ROPUF. Various stages of ROs are studied and compared based on five parameters: uniqueness, reliability, uniformity, bit-aliasing, and randomness.
- A comprehensive analysis of the environmental impact on the proposed ROPUF, including temperature, voltage variations, and aging.
- Analysis of two simultaneous environmental variation factors; namely, aging and voltage variations, and temperature variations with voltage variations. To the best of our knowledge, the impact of aging with varying voltages has not been studied before.
- Development of a novel authentication scheme for the Advanced Metering

Infrastructure (AMI) of the smart grid using a combination of ROPUFs for authentication, and blockchain for traceability, in a Zero Trust Architecture (ZTA) design to maximize the security of the AMI. The design provides security for communications between the utility company and the smart meters. Experimental results show that the authentication times for level 1 and level 2, the most common security levels, are 126.80 ms and 203.603 ms, respectively, satisfying the system's real-time requirements.

- Development of two novel techniques that can detect hardware Trojans based on power side-channel analysis and frequency response of the ROPUF. The proposed technique not only detects the Trojan but also facilitates in determining its location. The experiment results show that the Ring Oscillators closest to the Trojan have a higher percentage of frequency variation than the other Trojan locations.

References

[1] Potlapally, N. Hardware Security in Practice: Challenges and Opportunities. In Proceedings of the 2011 IEEE International Symposium on Hardware-Oriented Security and Trust; June 2011; pp. 93–98.

[2] Lipp, M.; Schwarz, M.; Gruss, D.; Prescher, T.; Haas, W.; Fogh, A.; Horn, J.; Mangard, S.; Kocher, P.; Genkin, D. Meltdown: Reading Kernel Memory from User Space. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18); 2018; pp. 973–990.

[3] Kocher, P.; Horn, J.; Fogh, A.; Genkin, D.; Gruss, D.; Haas, W.; Hamburg, M.; Lipp, M.; Mangard, S.; Prescher, T. Spectre Attacks: Exploiting Speculative Execution. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP); IEEE, 2019; pp. 1–19.

[4] Tang, A.; Sethumadhavan, S.; Stolfo, S. CLKscrew: Exposing the Perils of Security-Oblivious Energy Management, Usenix 2018 (Distinguished Paper Award). 2018.

[5] Forte, D.; Bhunia, S.; Karri, R.; Plusquellic, J.; Tehranipoor, M. IEEE International Symposium on Hardware Oriented Security and Trust (HOST):

Past, Present, and Future. In Proceedings of the 2019 IEEE International Test Conference (ITC); November 2019; pp. 1–4.

[6] Joshi, S.; Mohanty, S.P.; Kougianos, E. Everything You Wanted to Know About PUFs. IEEE Potentials 2017, 36, 38–46, doi:10.1109/MPOT.2015.2490261.

[7] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," *in Design Automation Conference (DAC).* New York, New York, USA: ACM, 2007, pp. 9–14.

[8] Gao, Y.; Al-Sarawi, S.F.; Abbott, D. Physical Unclonable Functions. Nat Electron 2020, 3, 81–91, doi:10.1038/s41928-020-0372-5.

[9] Gassend, B.L.P. Physical Random Functions. PhD Thesis, Massachusetts Institute of Technology, 2003.

[10] Tehranipoor, M.; Wang, C. Introduction to Hardware Security and Trust; Springer Science & Business Media, 2011;

[11] Sklavos, N.; Chaves, R.; Di Natale, G.; Regazzoni, F. Hardware Security and Trust. Cham, Switzerland: Springer 2017.

[12] Hu, W.; Chang, C.-H.; Sengupta, A.; Bhunia, S.; Kastner, R.; Li, H. An Overview of Hardware Security and Trust: Threats, Countermeasures, and Design Tools. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 2020, 40, 1010–1038.

[13] Bhunia, S.; Hsiao, M.S.; Banga, M.; Narasimhan, S. Hardware Trojan Attacks: Threat Analysis and Countermeasures. Proceedings of the IEEE 2014, 102, 1229–1247.

[14] Becker, G.T.; Regazzoni, F.; Paar, C.; Burleson, W.P. Stealthy Dopant-Level Hardware Trojans. In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems; Springer, 2013; pp. 197–214.

[15] Becker, G.T.; Regazzoni, F.; Paar, C.; Burleson, W.P. Stealthy Dopant-Level Hardware Trojans: Extended Version. Journal of Cryptographic Engineering 2014, 4, 19–31.

[16] Hamburg, M.; Kocher, P.; Marson, M.E. Analysis of Intel's Ivy Bridge Digital Random Number Generator. Online: http://www. cryptography. com/public/pdf/Intel_TRN G_Report_20120312. pdf 2012.

[17] Dubrova, E.; Näslund, M.; Carlsson, G.; Smeets, B. Keyed Logic BIST for Trojan Detection in SoC. In Proceedings of the 2014 International Symposium on System-on-Chip (SoC); IEEE, 2014; pp. 1–4.

[18] Hughes, L.A.; DeLone, G.J. Viruses, Worms, and Trojan Horses: Serious Crimes, Nuisance, or Both? Social science computer review 2007, 25, 78–98.

[19] Katzenbeisser, S.; Kocabaş, Ü.; Rožić, V.; Sadeghi, A.-R.; Verbauwhede, I.; Wachsmann, C. PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions (PUFs) Cast in Silicon. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems; Springer, 2012; pp. 283–301.

[20] Herder, C.; Yu, M.-D.; Koushanfar, F.; Devadas, S. Physical Unclonable Functions and Applications: A Tutorial. Proceedings of the IEEE 2014, 102, 1126–1141.

[21] Zhang, J.-L.; Qu, G.; Lv, Y.-Q.; Zhou, Q. A Survey on Silicon PUFs and Recent Advances in Ring Oscillator PUFs. Journal of computer science and technology 2014, 29, 664–678.

[22] Maes, R.; Verbauwhede, I. Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions. In Towards hardware-intrinsic security; Springer, 2010; pp. 3–37.

[23] Gassend, B.; Clarke, D.; Van Dijk, M.; Devadas, S. Silicon Physical Random Functions. In Proceedings of the Proceedings of the 9th ACM Conference on Computer and Communications Security; 2002; pp. 148–160.

[24] Yan, W.; Chandy, J. Phase Calibrated Ring Oscillator PUF Design and Application. Computers 2018, 7, 40.

[25] Portal, J.M.; Aziza, H. EEPROM Memory: Threshold Voltage Built in Self Diagnosis. In Proceedings of the International Test Conference, 2003. Proceedings. ITC 2003.; IEEE Computer Society, 2003; pp. 23–23.

[26] Rührmair, U.; Devadas, S.; Koushanfar, F. Security Based on Physical Unclonability and Disorder. In Introduction to Hardware Security and Trust; Springer, 2012; pp. 65–102.

[27] Maes, R.; Herrewege, A.V.; Verbauwhede, I. PUFKY: A Fully Functional PUF-Based Cryptographic Key Generator. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems; Springer, 2012; pp. 302–319.

[28] Devadas, S.; Suh, E.; Paral, S.; Sowell, R.; Ziola, T.; Khandelwal, V. Design and Implementation of PUF-Based" Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications. In Proceedings of the 2008 IEEE international conference on RFID; IEEE, 2008; pp. 58–64.

[29] Zheng, J.X.; Potkonjak, M. A Digital PUF-Based IP Protection Architecture for Network Embedded Systems. In Proceedings of the 2014 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS); IEEE, 2014; pp. 255–256.

[30] Gu, C.; Hanley, N.; O'neill, M. Improved Reliability of FPGA-Based PUF Identification Generator Design. ACM Transactions on Reconfigurable Technology and Systems (TRETS) 2017, 10, 1–23.

[31] Maiti, A.; McDougall, L.; Schaumont, P. The Impact of Aging on an FPGA-Based Physical Unclonable Function. In Proceedings of the 2011 21st International Conference on Field Programmable Logic and Applications; IEEE, 2011; pp. 151–156.

[32] Danger, J.-L.; Guilley, S.; Nguyen, P.; Rioul, O. PUFs: Standardization and Evaluation. In Proceedings of the 2016 Mobile System Technologies Workshop (MST); IEEE, 2016; pp. 12–18.

[33] Herkle, J. Becker and M. Ortmanns, "Exploiting Weak PUFs From Data Converter Nonlinearity—E.g., A Multibit CT $\Delta\Sigma$ Modulator," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 63, no. 7, pp. 994-1004, July 2016, doi: 10.1109/TCSI.2016.2555238.

[34] Kumar, A.; Sahay, S.; Suri, M. Switching-Time Dependent PUF Using STT-MRAM. In Proceedings of the 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID); IEEE, 2018; pp. 434–438.

[35] Chen, A. Utilizing the Variability of Resistive Random Access Memory to Implement Reconfigurable Physical Unclonable Functions. IEEE Electron Device Letters 2014, 36, 138–140.

[36] Gao, Y.; Ranasinghe, D.C.; Al-Sarawi, S.F.; Kavehei, O.; Abbott, D. Emerging Physical Unclonable Functions with Nanotechnology. IEEE access 2016, 4, 61–80.

[37] Marconot, J.; Hely, D.; Pebay-Peyroula, F. Conception and Evaluation of Secure Circuits for Strong Digital PUF. SN COMPUT. SCI. 2020, 1, 259, doi:10.1007/s42979-020-00274-0.

[38] Rührmair, U.; Sölter, J. PUF Modeling Attacks: An Introduction and Overview. In Proceedings of the 2014 Design, Automation & Test in Europe Conference & Exhibition (DATE); IEEE, 2014; pp. 1–6.

[39] Chien, W.-C.; Chang, Y.-C.; Tsou, Y.-T.; Kuo, S.-Y.; Chang, C.-R. STT-DPSA: Digital PUF-Based Secure Authentication Using STT-MRAM for the Internet of Things. Micromachines 2020, 11, 502.

[40] “What Are Logical Tags in HTM” GeeksforGeeks, 15 Mar. 2021, https://www.geeksforgeeks.org/what-are-logical-tags-in-

html/#:~:text=Logical%20tags%20are%20used%20to,any%20information%20about%20the%20text.

[41] J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls, “FPGA intrinsic PUFs and their use for IP protection,” in International workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer-Verlag, Sep. 2007, pp. 63–80.

[42] S. S. Kumar, J. Guajardo, R. Maes, G. J. Schrijen, and P. Tuyls, “The Butterfly PUF Protecting IP on every FPGA,” in International Workshop on Hardware-Oriented Security and Trust, 2008, pp. 67–70.

[43] Pappu, R.; Recht, B.; Taylor, J.; Gershenfeld, N. Physical One-Way Functions. Science 2002, 297, 2026–2030.

[44] Tuyls, P.; Skoric, B.; Stallinga, S.; Akkermans, T.; Ophey, W. An Information Theoretic Model for Physical Uncloneable Functions. In Proceedings of the International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.; IEEE, 2004; p. 141.

[45] Tuyls, P.; Škorić, B.; Stallinga, S.; Akkermans, A.H.; Ophey, W. Information-Theoretic Security Analysis of Physical Uncloneable Functions. In Proceedings of the International Conference on Financial Cryptography and Data Security; Springer, 2005; pp. 141–155.

[46] Ignatenko, T.; Schrijen, G.-J.; Skoric, B.; Tuyls, P.; Willems, F. Estimating the Secrecy-Rate of Physical Unclonable Functions with the Context-Tree Weighting

Method. In Proceedings of the 2006 IEEE International Symposium on Information Theory; IEEE, 2006; pp. 499–503.

[47] Vrijaldenhoven, S. Acoustical Physical Uncloneable Functions [Master Thesis]. TU Eindhoven 2004.

[48] Buchanan, J.D.; Cowburn, R.P.; Jausovec, A.-V.; Petit, D.; Seem, P.; Xiong, G.; Atkinson, D.; Fenton, K.; Allwood, D.A.; Bryan, M.T. 'Fingerprinting'Documents and Packaging. Nature 2005, 436, 475–475.

[49] DeJean, G.; Kirovski, D. RF-DNA: Radio-Frequency Certificates of Authenticity. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems; Springer, 2007; pp. 346–363.

[50] Jiang, D.; Chong, C.N. Anti-Counterfeiting Using Phosphor Puf. In Proceedings of the 2008 2nd International Conference on Anti-counterfeiting, Security and Identification; IEEE, 2008; pp. 59–62.

[51] Holcomb, D.E.; Burleson, W.P.; Fu, K. Power-up SRAM State as an Identifying Fingerprint and Source of True Random Numbers. IEEE Transactions on Computers 2008, 58, 1198–1210.

[52] G. T. Becker and R. Kumar, "Active and passive side-channel attacks on delay based PUF designs," IACR Cryptology ePrint Archive, vol. 287, 2014

[53] Chang, Z.; Shi, S.; Song, B.; Fan, W.; Wang, Y. Modeling Attack Resistant Arbiter PUF with Time-Variant Obfuscation Scheme. In Proceedings of the 2021 31st International Conference on Field-Programmable Logic and Applications (FPL); IEEE, 2021; pp. 60–63.

[54] Gassend, B.; Dijk, M.V.; Clarke, D.; Torlak, E.; Devadas, S.; Tuyls, P. Controlled Physical Random Functions and Applications. ACM Transactions on Information and System Security (TISSEC) 2008, 10, 1–22.

[55] S. M. Trimberger, "Three Ages of FPGAs: A Retrospective on the First Thirty Years of FPGA Technology", Proceedings of the IEEE, vol. 103, no. 3, pp. 318-331, March 2015

[56] M. Tehranipoor and F. Koushanfar , “A survey of Hardware Trojan Taxonomy and Detection,’’ IEEE Design Test Comput., vol. 27, no. 1, pp. 10–25, Jan. 2010

[57] S. Drimer, "Volatile FPGA design security-a survey," IEEE Computer Society Annual, pp. 292-297, 2008.

[58] N. A. Hazari, F. Alsulami and M. Niamat, " FPGA IP Obfuscation Using Ring Oscillator Physical Unclonable Function," 2018 IEEE National Aerospace and Electronics Conference (NAECON), pp. 105-108, July 2018.

[59] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," 44th ACM/IEEE Design Automation Conference, San Diego, CA, 2007, pp. 9-14.

[60] S. Gören et al., "Partial bitstream protection for low-cost FPGAs with physical unclonable function obfuscation and dynamic partial self reconfiguration", Elsevier Computers &Electrical Engineering, vol. 39, no. 2, pp. 386-397, Feb. 2013.

[61] M. Tehranipoor, H. Salmani, and X. Zhang.,“Integrated Ciruit Authentication,” New York: Springer, 2015.

[62] F. Amsaad, T. Hoque, and M. Niamat, “Analyzing the Performance of a Configurable ROPUF controlled by Programmable XOR Gates,”in Midwest Symposium on Circuits and Systems, pp. 1-4, 2015.

[63] A. Maiti and P. Schaumont, ‘‘Improving the quality of a physical unclonable function using configurable ring oscillators,’’ in Proc. IEEE Int. Conf. Field Program. Logic Appl., Aug./Sep. 2009, pp. 703–707.

[64] M. Mustapa, “ PUF based FPGAs for Hardware Security and Trust,” PhD. Dissertation, Department of Electrical Engineering and Computer Science, University of Toledo, Ohio, 2015.

[65] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions" in Embedded Systems Design with FPGAs., New York, NY, USA: Springer-Verlag, pp. 245-267, Nov. 2012.

[66] Yamamoto D, Sakiyama K, Iwamoto M, Ohta K, Ochiai T, Takenaka M, and Itoh K, “Uniqueness enhancement of puf responses based on the locations of random outputting rs latches,” Proceedings of the 13th international conference on Cryptographic hardware and embedded systems, CHES 2011. Springer, Berlin, Heidelberg, pp 390–406.

[67] Majzoobi M., Koushanfar F., and Potkonjak M., “Testing techniques for hardware security,” IEEE international test conference, ITC 2008, pp 1–10.

[68] Su Y, Holleman J and Otis B., “A digital 1.6 pj/bit chip identification circuit using process variations,” IEEE J Solid-State Circ 43(1):69–77.

[69] Tuyls, Pim; Šcorić, Boris; Kevenaar, Tom (2007). Security with Noisy Data: Private Biometics, Secure Key Storage and Anti-counterfeiting. Springer. doi:10.1007/978-1-84628-984-2. ISBN 978-184628-983-5.

[70] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs," International Conference on Reconfigurable Computingand FPGAs (ReConFig) 2010, pp 298-303, December 2010.

[71] Gu, C.; Hanley, N.; O'neill, M. Improved reliability of FPGA-based PUF identification generator design. ACM Trans. Reconfigurable Technol. Syst. (TRETS) 2017, 10, 1–23.

[72] A. Aloseel, H. He, C. Shaw and M. A. Khan, "Analytical Review of Cybersecurity for Embedded Systems," in IEEE Access, vol. 9, pp. 961-982, 2021, doi:10.1109/ACCESS.2020.3045972.

[73] B. Chen and F. M. J. Willems, "Secret Key Generation Over Biased Physical Unclonable Functions With Polar Codes," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 435-445, Feb. 2019, doi: 10.1109/JIOT.2018.2864594.

[74] R. Helinski, D. Acharyya and J. Plusquellic, "Quality metric evaluation of a physical unclonable function derived from an IC's power distribution system," Design Automation Conference, 2010, pp. 240-243, doi: 10.1145/1837274.1837336

[75] J. W. Lee, Daihyun Lim, B. Gassend, G. E. Suh, M. van Dijk and S. Devadas, "A technique to build a secret key in integrated circuits for identification and

authentication applications," 2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525), 2004, pp. 176-179, doi: 10.1109/VLSIC.2004.1346548.

[76] Müelich, H. Mandry, M. Ortmanns and R. F. H. Fischer, "A Multilevel Coding Scheme for Multi-Valued Physical Unclonable Functions," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3814-3827, 2021.

[77] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas,“ Silicon Physical Random Functions,” in Proc. 9th ACM Conf. on Comp. and Commun. Secur. (CCS), 2002, pp. 148 160.

[78] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", Proceedings IEEE, vol. 102, no. 8, pp. 1207-1228, Aug 2014.

[79] P. Samarin and K. Lemke-Rust, "Detection of counterfeit ICs using public identification sequences," 2017 IEEE Int. Symposium on Hardware Oriented Secur. and Trust (HOST), 2017, pp. 163-163, doi: 10.1109/HST.2017.7951827.

[80] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware Trojan attacks: Threat analysis and countermeasures", Proc. IEEE, vol. 102, no. 8, pp. 1229-1247, Aug. 2014

[81] M. Tehranipoor, H. Salmani, and X. Zhang, “Hardware Trojan detection: Untrusted manufactured integrated circuits,” in Integrated Circuit Authentication. Switzerland: Springer, 2014, pp. 31–38.

[82] S. M. Trimberger and J. J. Moore, "FPGA Security: Motivations, Features, and Applications," in Proc. IEEE, vol. 102, no. 8, pp. 1248-1265, Aug. 2014.

[83] N. A. Hazari, F. Alsulami and M. Niamat, "FPGA IP obfuscation using ring oscillator physical unclonable function," in Proc. Nat. Aerosp. Electron. Conf. (NAECON), Dayton, OH, USA, Jul. 2018, pp. 105–108.

[84] B. Gassend, D. E. Clarke, M. van Dijk, and S. Devadas, "Controlled physical random functions," in Proc. 18th Annu. Comput. Security Appl. Conf. (ACSAC), Las Vegas, NV, USA, 2002, pp. 149–160. [Online]. Available: https://doi.org/10.1109/CSAC.2002.1176287

[85] X. Xin, J.-P. Kaps, and K. Gaj, ''A configurable ring-oscillator-based PUF for xilinx FPGAs,'' in Proc. 14th Euromicro Conf. Digit. Syst. Design, Aug. 2011, pp. 651–657.

[86] K. Kursawe, A. Sadeghi, D. Schellekens, B. Skoric, and P. Tuyls, ''Reconfigurable physical unclonable functions-enabling technology for tamperresistant storage,'' in Proc. IEEE Int. Workshop Hardw.-Oriented Secur. Trust, Jul. 2009, pp. 22–29.

[87] T. Hoque, F. Amsaad, and M. Niamat, ''Assessment of NAND based ring oscillator for hardware trojan detection,'' in Proc. IEEE 58th Int. Midwest Symp. Circuits Syst. (MWSCAS), Aug. 2015, pp. 1–4.

[88] M. Barbareschi, G. D. Natale, F. Bruguier, P. Benoit, and L. Torres, "Ring oscillators analysis for security purposes in Spartan-6 FPGAs," Microprocessors and Microsystems, vol. 47, Part A, pp 3-10, Nov. 2016.

[89] N. Hazari, F. Alsulami, A. Oun, and M. Niamat, ‘‘Performance analysis of XOR-inverter based ring oscillator PUF for hardware security,’’ in Proc. IEEE Nat. Aerosp. Electron. Conf. (NAECON), Dayton, OH, USA, Jul. 2019, pp. 253–256.

[90] M. Mustapa and M. Niamat, "Temperature, Voltage, and Aging Effects in Ring Oscillator Physical Unclonable Function," in Proc. IEEE 17th Int. Conf. on High Performance Computing and Commun., IEEE 7th Int. Symposium on Cyberspace Safety and Secur., and 2015 IEEE 12th Int. Conf. on Embedded Software and Systems, 2015, pp. 1699-1702.

[91] A. Maiti and P. Schaumont, ‘‘Improving the quality of a physical unclonable function using configurable ring oscillators,’’ in Proc. Int. Conf. Field Program. Log. Appl., Prague, Czech Republic, Aug. 2009, pp. 703–707.

[92] P. Sedcole and P. Y. K. Cheung, "Within-die delay variability in 90nm FPGAs and beyond," in Proc. IEEE . Int. Conf .on Field Programmable Technology, 2006, pp. 97-104.

[93] N. Karimi, T. Moos, and A. Moradi, ‘‘Exploring the effect of device aging on static power analysis attacks,’’ in Proc. TCHES, vol. 2019, no. 3, 2019, pp. 233–256.

[94] E. Boemo and S. López-Buedo, “Thermal monitoring on FPGAs using ring-oscillators,” in Proc. Int. Conf. Field Program. Logic Appl. (FPL), 1997, pp. 69–78.

[95] H. Yu, P. H. W. Leong, and Q. Xu, “An FPGA chip identification generator using configurable ring oscillator,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 20, 2012, pp. 2198-2207.

[96] X. Wang and M. Tehranipoor, “Novel physical unclonable function with process and environmental variations,” in Design, Automation Test in Europe Conference Exhibition (DATE), 2010, pp. 1065 –1070.

[97] P. Koeberl, J. Li, R. Maes, A. Rajan, C. Vishik, and M. Wojcik, “Evaluation of a PUF device authentication scheme on a discrete 0.13 μm SRAM,” in Trusted Systems. Berlin, Germany: Springer-Verlag, 2012, pp. 271–288.

[98] A. Maiti and P. Schaumont, “The impact of aging on a physical unclonable function,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 22, no. 9, pp. 1854–1864, Sep. 2014.

[99] M. T. Rahman, D. Forte, F. Rahman, and M. Tehranipoor, “A pair selection algorithm for robust RO-PUF against environmental variations and aging,” in Proc. 33rd IEEE Int. Conf. Comput. Design (ICCD), New York, NY, USA, Oct. 2015, pp. 415–418.

[100] P. Tuyls, B. Skoric, and T. Kevenaar, Security with noisy data on private biometrics, secure key storage and anti-counterfeiting. London, UK: Springer-Verlag, 2007. [Online]. Available: https://doi.org/10.1007/978-1-84628-984-2

[101] F. Alsulami and M. Niamat, "Performance study of FPGA based AND-inverter ring oscillator PUFs," 2020 IEEE International Conference on Electro

Information Technology (EIT), 2020, pp. 194-199, doi: 10.1109/EIT48999.2020.9208341.

[102] Xilinx Datasheet. Artix-7 FPGAs Data Sheet: DC and AC Switching Characteristics. Available online: http://www.xilinx.com/support/documentation/data_sheets/ds181_Artix_7_Data_Sheet.p df (accessed on 20 January 2021).

[103] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, S. D. Leigh, M. Levenson, M. Vangel, N. A. Heckert, and D. L. Banks, ‘‘A statistical test suite for random and pseudorandom number generators for cryptographic applications,’’ NIST, Gaithersburg, MD, USA, Tech. Rep. SP 800-22 Rev 1a, Apr. 2010.

[104] Y. Luo, W. Wang, S. Best, Y. Wang, and X. Xu, “A high-performance and secure TRNG based on chaotic cellular automata topology,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 67, no. 12, pp. 4970–4983, Dec. 2020.

[105] B. Khaleghi and T. S. Rosing, “Thermal-aware design and flow for FPGA performance improvement,” in Design Automation & Test in Europe Conf . & Exhibition (DATE). 2019, pp. 342– 347.

[106] J. Zhang, X. Tan, Y. Zhang, W. Wang and Z. Qin, "Frequency Offset-Based Ring Oscillator Physical Unclonable Function," in IEEE Transactions on Multi-Scale Computing Systems, vol. 4, no. 4, pp. 711-721, 1 Oct.-Dec. 2018, doi: 10.1109/TMSCS.2018.2877737.

[107] W. Yan, C. Jin, F. Tehranipoor and J. A. Chandy, "Phase calibrated ring oscillator PUF design and implementation on FPGAs," 2017 27th International Conference on Field Programmable Logic and Applications (FPL), 2017, pp. 1-8, doi: 10.23919/FPL.2017.8056859.

[108] A. Maiti, V. Gunreddy, and P. Schaumont, “A systematic method to evaluate and compare the performance of physical unclonable functions,” Proc. Embedded System Design FPGAs, 2013, pp. 245-267.

[109] G. Brussenskiy, and J. S. Yuan, “Robust PUF Circuit Design against Temperature Variations and Aging Effects,” International Conference on Security and Management (SAM), 2015, pp. 211-216.

[110] T. Bryant, S. Chowdhury, D. Forte, M. Tehranipoor, and N. Maghari, “A Stochastic Approach to Analog Physical Unclonable Function,” In IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS), 2016, pp. 1-4.

[111] A.S. Chauhan, V. Sahula and A.S. Mandal, " Novel Randomized Placement for FPGA Based Robust ROPUF with Improved Uniqueness," in Journal of Electronic Testing, vol. 35, pp. 581-601, 2019, doi: https://doi.org/10.1007/s10836-019-05829-5.

[112] R. Hesselbarth, F. Wilde, C. Gu and N. Hanley, "Large scale RO PUF analysis over slice type, evaluation time and temperature on 28nm Xilinx FPGAs," 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2018, pp. 126-133, doi: 10.1109/HST.2018.8383900.

[113] A. Maiti and P. Schaumont, “Improved ring oscillator PUF: an FPGA friendly secure primitive,” Journal of cryptology, vol. 24, no. 2, pp. 375–397, 2011.

[114] S. U. Hussain, M. Majzoobi, and F. Koushanfar, “A Built-in-Self-Test Scheme for Online Evaluation of Physical Unclonable Functions and True Random Number Generators,” IEEE Transactions on Multi-scale Computing Systems, vol. 2, no. 1, 2016.

[115] J. R. Celaya, P. Wysocki, V. Vashchenko, S. Saha and K. Goebel, "Accelerated aging system for prognostics of power semiconductor devices," 2010 IEEE AUTOTESTCON, 2010, pp. 1-6, doi: 10.1109/AUTEST.2010.5613564.

[116] Chi-En Yin and Gang Qu, "Temperature-aware cooperative ring oscillator PUF," 2009 IEEE International Workshop on Hardware-Oriented Security and Trust, 2009, pp. 36-42, doi: 10.1109/HST.2009.5225055.

[117] A. S. Chauhan, V. Sahula and A. S. Mandal, "Novel Randomized & Biased Placement for FPGA Based Robust Random Number Generator with Enhanced Uniqueness," 2019 32nd International Conference on VLSI Design and 2019 18th International Conference on Embedded Systems (VLSID), 2019, pp. 353-358, doi: 10.1109/VLSID.2019.00079.

[118] C. Gu, N. Hanley, and M. O’Neill, “FPGA-based strong PUF with increased uniqueness and entropy properties,” 2017 IEEE International Symposium on Circuits and Systems (ISCAS), 2017, pp. 1-4.

[119] Jim Ledin. 2021. Architecting High-Performance Embedded Systems (1st. ed.). Packt Publishing, Birmingham, UK.

[120] M. Mustapa and M. Niamat, “Relationship between number of stages in ROPUF and CRP generation on FPGA,” in Proc. Int. Conf. Security Manag. (SAM) Steering Committee World Congr. Comput. Sci. Comput. Eng. Appl. Comput. (WorldComp), Las Vegas, NV, USA, 2014, pp. 120–126.

[121] W. Wang, Z. Lu, “Cyber security in the Smart grid: Survey and challenges”, Computer Networks, vol. 57, no. 5, pp. 1344-1371, April 2013.

[122] V. C. Patil and S. Kundu, "Realizing Robust, Lightweight Strong PUFs for Securing Smart Grids," in IEEE Transactions on Consumer Electronics, vol. 68, no. 1, pp. 5-13, Feb. 2022, doi: 10.1109/TCE.2021.3139356.

[123] W. Yan, F. Tehranipoor and J. A. Chandy, "PUF-Based Fuzzy Authentication Without Error Correcting Codes," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 36, no. 9, pp. 1445-1457, Sept. 2017, doi: 10.1109/TCAD.2016.2638445.

[124] M. Mustapa, M. Y. Niamat, A. P. Deb Nath and M. Alam, "Hardware-Oriented Authentication for Advanced Metering Infrastructure," in IEEE Transactions on Smart Grid, vol. 9, no. 2, pp. 1261-1270, March 2018, doi: 10.1109/TSG.2016.2582423

[125] S. Ghosh, U. Chatterjee, D. Chatterjee, R. Masburah, D. Mukhopadhyay, S. Dey, “Demand Manipulation Attack Resilient Privacy Aware Smart Grid Using PUFs and Blockchain”, in Applied Cryptography and Network Security Workshops (ACNS): Lecture Notes in Computer Science, J. Zhou, C. M. Ahmed, L. Batina, S. Chattopadhyay, O. Gadyatskaya, C. Jin, J. Lin, E. Losiouk, B. Luo, S.

Majumdar, M. Maniatakos, D. Mashima, W. Meng, S. Picek, M. Shimaoka, C. Su, C. Wang, Eds. Cham: Springer International Publishing, 2021, pp. 252–275.

[126] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," in IEEE Access, vol. 10, pp. 57143-57179, May 2022.

[127] A. Gopstein, et al., "NIST Framework and Roadmap for Smart Grid Interoperability Standards," NIST Special Publication 1108r4, release 4.0, pp. 1-239, Feb. 2021.

[128] The Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee, Guidelines for Smart Grid Cybersecurity, NISTIR 7628 Rev. 1 (2014) 1-668.

[129] A. Ghosal and M. Conti, "Key Management Systems for Smart Grid Advanced Metering Infrastructure: A Survey," in IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2831-2848, thirdquarter 2019.

[130] Z. El Mrabet, N. Kaabouch, H. El Ghazi, H. El Ghazi, "Cyber-security in smart grid: Survey and challenges", Computers & Electrical Engineering, vol. 67, pp. 469-482, May 2018.

[131] S. Chang, T. William, W. Wu, B. Cheng, H. Chen and P. Hsu, "Design of an authentication and key management system for a smart meter gateway in AMI," 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE), 2017, pp. 1-2, doi: 10.1109/GCCE.2017.8229288.

[132] I. Parvez, A. I. Sarwat, M. T. Thai and A. K. Srivastava, "A novel key management and data encryption method for metering infrastructure of smart grid" in eprint arXiv:1709.08505, pp. 1-8, Sep. 2017.

[133] N. Liu, J. Chen, L. Zhu, J. Zhang and Y. He, "A key management scheme for secure communications of advanced metering infrastructure in smart grid", IEEE Trans. Ind. Electron., vol. 60, no. 10, pp. 4746-4756, Oct. 2013.

[134] A. S. Sani, D. Yuan, W. Bao and Z. Y. Dong, "A Universally Composable Key Exchange Protocol for Advanced Metering Infrastructure in the Energy Internet," in IEEE Transactions on Industrial Informatics, vol. 17, no. 1, pp. 534-546, Jan. 2021, doi: 10.1109/TII.2020.2971707.

[135] G. P. Sellitto, H. Aranha, M. Masi, T. Pavleska, "Enabling a Zero Trust Architecture in Smart Grids Through a Digital Twin", in Dependable Computing - EDCC 2021 Workshops: Communications in Computer and Information Science, et al., Eds. Cham: Springer International Publishing, 2021, pp. 73–81.

[136] J. Kindervag, "[Build Security into Your Network's Dna: The Zero Trust Network Architecture]," Forrester Research Inc. pp. 1-27, Nov. 2010.

[137] C. DeCusatis, P. Liengtiraphan, A. Sager and M. Pinelli, "Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication," 2016 IEEE International Conference on Smart Cloud (SmartCloud), 2016, pp. 5-10.

[138] S. Rose, O. Borchert, S. Mitchell, S. Connelly, "Zero-Trust Architecture," NIST Special Publication 800-207, pp. 1-59, Aug. 2020.

[139] B. Embrey, "The Top Three Factors Driving Zero Trust Adoption," Computer Fraud & Security, vol. 2020, no. 9, pp. 13-15, Jan. 2020.

[140] P. Gope and B. Sikdar, "A Privacy-Aware Reconfigurable Authenticated Key Exchange Scheme for Secure Communication in Smart Grids," in IEEE Transactions on Smart Grid, vol. 12, no. 6, pp. 5335-5348, Nov. 2021, doi: 10.1109/TSG.2021.3106105.

[141] Y. -N. Cao, Y. Wang, Y. Ding, H. Zheng, Z. Guan and H. Wang, "A PUF-based Lightweight Authenticated Metering Data Collection Scheme with Privacy Protection in Smart Grid," 2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), 2021, pp. 876-883, doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00124.

[142] S.-K. Kim, J.-H. Huh, “A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective,” Energies, vol. 11, no. 8, p. 1973, Jul. 2018, doi: 10.3390/en11081973.

[143] W. Wang, H. Huang, L. Zhang, C. Su, "Secure and efficient mutual authentication protocol for smart grid under blockchain," Peer-to-Peer Netw. Appl. vol. 14, pp. 2681–2693, Nov. 2020, doi: https://doi.org/10.1007/s12083-020-01020-2.

[144] M. Tahavori, F. Moazami, "Lightweight and secure PUF-based authenticated key agreement scheme for smart grid," Peer-to-Peer Netw. Appl. vol. 13, pp. 1616–1628, May 2020, doi: https://doi.org/10.1007/s12083-020-00911-8.

[145] Office of Electricity Delivery and Energy Reliability, "[The National Energy Technology Laboratory Modern Grid Strategy Powering our 21st-Century Economy: Advanced Metering Infrastructure]," U.S. Department of Energy, v. 1, Feb. 2008.

[146] R. R. Mohassel, A. Fung, F. Mohammadi, K. Raahemifar, "A survey on Advanced Metering Infrastructure," International Journal of Electrical Power & Energy Systems, vol. 63, pp. 473–484, Dec. 2014, doi: https://doi.org/10.1016/j.ijepes.2014.06.025.

[147] C. Herder, L. Ren, M. van Dijk, M. -D. Yu and S. Devadas, "Trapdoor computational fuzzy extractors and stateless cryptographically-secure physical unclonable functions," in IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 1, pp. 65-82, 1 Jan.-Feb. 2017, doi: 10.1109/TDSC.2016.2536609.

[148] J. Kang et al., "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4660-4670, June 2019, doi: 10.1109/JIOT.2018.2875542.

[149] M. Wazid, A. K. Das, S. Shetty and M. Jo, "A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of

Intelligent Things," in IEEE Access, vol. 8, pp. 88700-88716, 2020, doi: 10.1109/ACCESS.2020.2992467.

[150] M. Shokry, A. I. Awad, M. K. Abd-Ellah, and A. A. M. Khalaf, “Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision,” Future Generation Computer Systems, vol. 136, pp. 358-377, Nov. 2022, doi: https://doi.org/10.1016/j.future.2022.06.013.

[151] Y. Tanaka, S. Bian, M. Hiromoto and T. Sato, "Coin Flipping PUF: A Novel PUF With Improved Resistance Against Machine Learning Attacks," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 65, no. 5, pp. 602-606, May 2018, doi: 10.1109/TCSII.2018.2821267.

[152] Q. Ma, C. Gu, N. Hanley, C. Wang, W. Liu and M. O'Neill, "A machine learning attack resistant multi-PUF design on FPGA," 2018 23rd Asia and South Pacific Design Automation Conference (ASP-DAC), 2018, pp. 97-104, doi: 10.1109/ASPDAC.2018.8297289.

[153] E. Dubrova, O. Näslund, B. Degen, A. Gawell and Y. Yu, "CRC-PUF: A Machine Learning Attack Resistant Lightweight PUF Construction," 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2019, pp. 264-271, doi: 10.1109/EuroSPW.2019.00036.

[154] R. Maes, Physically Unclonable Functions: Constructions, Properties and Applications, New York, NY, USA: Springer-Verlag, 2013, pp. 1–172, ISBN: 978-3-642-41394-0.

[155] X. Wang, H. Salmani, M. Tehranipoor and J. Plusquellic, "Hardware Trojan Detection and Isolation Using Current Integration and Localized Current Analysis," 2008 IEEE International Symposium on Defect and Fault Tolerance of VLSI Systems, 2008, pp. 87-95, doi: 10.1109/DFT.2008.61.

[156] V. R. Surabhi et al., "Hardware Trojan Detection Using Controlled Circuit Aging," in IEEE Access, vol. 8, pp. 77415-77434, 2020, doi: 10.1109/ACCESS.2020.2989735.

[157] C. Dunbar and G. Qu, “Designing trusted embedded systems from finite state machines,” ACM Transactions on Embedded Computing Systems (TECS), vol. 13, no. 5s, pp. 1–20, 2014.

[158] S. T. King, J. Tucek, A. Cozzie, C. Grier, W. Jiang, and Y. Zhou, “Designing and implementing malicious hardware,” in Proc. 1st Usenix Workshop Large-Scale Exploits Emergent Threats, 2008, Art. no. 5.

[159] S. Narasimhan et al., "Hardware Trojan Detection by Multiple-Parameter Side-Channel Analysis," in IEEE Transactions on Computers, vol. 62, no. 11, pp. 2183-2195, Nov. 2013, doi: 10.1109/TC.2012.200.

[160] C. He, B. Hou, L. Wang, Y. En and S. Xie, "A novel hardware Trojan detection method based on side-channel analysis and PCA algorithm," 2014 10th International Conference on Reliability, Maintainability and Safety (ICRMS), 2014, pp. 1043-1046, doi: 10.1109/ICRMS.2014.7107362.

[161] T. E. Levin, T. P. Sherwood, T. D. Huffmire, C. E. Irvine, R. C. Kastner, T. D. Nguyen, et al., "Superpositional Control of Integrated Circuit Processing," ed: Google Patents, 2011.

[162] S. Bhunia et al., "Protection Against Hardware Trojan Attacks: Towards a Comprehensive Solution," in IEEE Design & Test, vol. 30, no. 3, pp. 6-17, June 2013, doi: 10.1109/MDT.2012.2196252.

[163] V. R. Surabhi, P. Krishnamurthy, H. Amrouch, J. Henkel, R. Karri and F. Khorrami, "Exposing Hardware Trojans in Embedded Platforms via Short-Term Aging," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, no. 11, pp. 3519-3530, Nov. 2020, doi: 10.1109/TCAD.2020.3012649.

[164] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi and B. Sunar, "Trojan Detection using IC Fingerprinting," 2007 IEEE Symposium on Security and Privacy (SP '07), 2007, pp. 296-310, doi: 10.1109/SP.2007.36.

[165] A. P. Fournaris, L. Pyrgas and P. Kitsos, "An FPGA Hardware Trojan Detection Approach Based on Multiple Parameter Analysis," 2018 21st Euromicro Conference on Digital System Design (DSD), 2018, pp. 516-522, doi: 10.1109/DSD.2018.00091.

[166] E. Sharifi, K. Mohammadias1, M. Havasi and A. Yazdani, "Performance analysis of Hardware Trojan detection methods", International Joumal of Open Information Technologies, vol. 3, pp. 39-44, April 2015.

[167] R.S. Chakraborty, F. Wolff, S. Paul, C. Papachristou and S. Bhunia, "MERO: A Statistical Approach for Hardware Trojan Detection", Proc. 11 th Int. Conf. Cryptograph. Hardw. Embedded Syst., pp. 396-410, 2009.

[168] L. N. Nguyen, C. -L. Cheng, M. Prvulovic and A. Zajić, "Creating a Backscattering Side Channel to Enable Detection of Dormant Hardware Trojans," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 7, pp. 1561-1574, July 2019, doi: 10.1109/TVLSI.2019.2906547.

[169] S. Baktir, T. Güçlüoğlu, A. Özmen, H. F. Alsan and M. C. Macit, "Detection of Trojans in integrated circuits," 2012 International Symposium on Innovations in Intelligent Systems and Applications, 2012, pp. 1-5, doi: 10.1109/INISTA.2012.6246941.

[170] Yier Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, 2008, pp. 51-57, doi: 10.1109/HST.2008.4559049.

[171] X. Wang, H. Salmani, M. Tehranipoor and J. Plusquellic, "Hardware Trojan Detection and Isolation Using Current Integration and Localized Current Analysis," 2008 IEEE International Symposium on Defect and Fault Tolerance of VLSI Systems, 2008, pp. 87-95, doi: 10.1109/DFT.2008.61.

[172] H. Salmani, M. Tehranipoor and J. Plusquellic, "New design strategy for improving hardware Trojan detection and reducing Trojan activation time," 2009 IEEE International Workshop on Hardware-Oriented Security and Trust, 2009, pp. 66-73, doi: 10.1109/HST.2009.5224968.

[173] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi and B. Sunar, "Trojan Detection using IC Fingerprinting," 2007 IEEE Symposium on Security and Privacy (SP '07), 2007, pp. 296-310, doi: 10.1109/SP.2007.36.

[174] J. Villasenor and M. Tehranipoor, "Chop shop electronics," in IEEE Spectrum, vol. 50, no. 10, pp. 41-45, October 2013, doi: 10.1109/MSPEC.2013.6607015.

[175] A. Maiti, J. Casarona, L. McHale and P. Schaumont, "A large scale characterization of RO-PUF," 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2010, pp. 94-99, doi: 10.1109/HST.2010.5513108.

[176] Y. Gao, S.F. Al-Sarawi, D. Abbott, "Physical Unclonable Functions." Nature Electronics, 2020, 3, 81–91, doi:10.1038/s41928-020-0372-5.

[177] F. Kodýtek, R. Lórencz, and J. Buček. "Improved ring oscillator PUF on FPGA and its properties." Microprocessors and Microsystems, 2016,47, pp.55-63.