Exploring Design of Physical Unclonable Functions (PUFs) for Robust Hardware-Assisted Security

Submitted in partial fulfilment of the requirements
for the award of the degree of

Doctor of Philosophy

by

Podeti Raveendra
(Roll No: 719068)

Under the supervision of

Prof. Patri Sreehari Rao
(Supervisor)

Dr. P. Muralidhar
(Co-Supervisor)

Department of Electronics & Communication Engineering
National Institute of Technology Warangal
Telangana, India - 506004
2024

Dedicated

To

Amma & Nanna,

Uma & Karthi

Approval Sheet

This thesis entitled **Exploring Design of Physical Unclonable Functions (PUFs) for Robust Hardware-Assisted Security** by **Podeti Raveendra** is approved for the degree of **Doctor of Philosophy**.

Examiners

____

____

Research Supervisor	**Research Co-Supervisor**
______________________	______________________
Prof. Patri Sreehari Rao	**Dr. P. Muralidhar**
Department of ECE,	Department of ECE,
NIT Warangal, India-506004	NIT Warangal, India-506004
DSC Chairman	**Head of the Department**
______________________	______________________
Prof. N. Bheema Rao	**Prof. D. Vakula**
Department of ECE,	Department of ECE,
NIT Warangal, India-506004	NIT Warangal, India-506004

Place:

Date:

Declaration

This is to certify that the work presented in this thesis entitled **Exploring Design of Physical Unclonable Functions (PUFs) for Robust Hardware-Assisted Security** is a bonafied work done by me under the supervision of **Prof. Patri Sreehari Rao and Dr. P. Muralidhar** and was not submitted elsewhere for the award of any degree.

I declare that this written submission represents my own ideas and even considered others ideas which are adequately cited and further referenced the original sources. I understand that any violation of the above will cause disciplinary action by the institute and can also evoke panel action from the sources or from whom proper permission has not been taken when needed. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea or data or fact or source in my submission.

Place:

Date:

Podeti Raveendra
Research Scholar
Roll No.: 719068

NATIONAL INSTITUTE OF TECHNOLOGY

WARANGAL, INDIA-506004

Department of Electronics and Communication Engineering

CERTIFICATE

This is to certify that the thesis work entitled **Exploring Design of Physical Unclonable Functions (PUFs) for Robust Hardware-Assisted Security** is a bonafide record of work carried out by **Podeti Raveendra** submitted to the faculty of **Electronics and Communication Engineering** department, in partial fulfilment of the requirements for the award of the degree of **Doctor of Philosophy** in **Electronics and Communication Engineering, National Institute of Technology Warangal, India-506004**. The contributions embodied in this thesis have not been submitted to any other university or institute for the award of any degree.

Prof. Patri Sreehari Rao
Research Supervisor,
Department of ECE,
NIT Warangal, India-506004.

Dr. P. Muralidhar
Research Co-Supervisor
Department of ECE,
NIT Warangal, India-506004.

Place:

Date:

Acknowledgements

First, I would like to express my deepest gratitude to the exceptional individuals Prof. Patri Sreehari Rao and Dr. Pullakandam Muralidhar, who supported and guided me throughout this transformative journey with promptness and care. I am profoundly grateful for the immeasurable contributions they made to my development.

I take this privilege to thank all my Doctoral Scrutiny Committee members Prof. D. Vakula (HoD), Prof. N. Bheema Rao (Chairman), Prof. C. B. Rama Rao (Retd.), Prof. J.V. Ramana Murthy (Dept. of Mathematics), and Dr. Ekta Goel for their detailed review, constructive suggestions, and excellent advice during the progress of this research work. I would also like to thank all the faculty of the Department of ECE who helped me during the course.

I would like to convey my sincere gratitude to Prof. Sree Rama Krishna (Former HoD of Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada), Dr. Sirigiri Chittibabu (Late), Prof. M. Padmaja, Prof. Jhansi Rani, Dr. Sk. Fayaz Ahamed, RV Hanumanth Prasad, Dr. K. Vara Prasad, A Ravi Raja, K.V Ratna Prabha, Dr. P.V. Satya Narayana, Dr. Ch. Naga Raghuram, Dr. A. Vijaya Shankar, Dr. P. Phani kumar, Dr. B.L. Sirisha, Dr. G. Hema Kumar, Dr. P.S. Suhasini, Dr. A. Anitha, and Dr.N.S. Murthy, who provided exceptional guidance and unwavering support throughout my teaching endeavours.

I want to express my heartfelt appreciation to My Gurus (Intermediate) Mr. Seshu, Mr. P. Srinivasa Rao, Mr.Devanandam, Mr.Dinesh, Mr.Khan, Mr.Varaprasad, My Gurus (High school) Mr. A. Arun Kumar, Mr.Sharma, Mr.Kornel, Mr.Acharya, Mr.Vincent, Mr.Lurthiah, Mr.Baala swamy, Mr.Jnananandam, Mr.Balireddy, Mrs. Karuna, Mrs. Sandhya rani, Tuition: Mr.Ravikumar (Late), Mr. Haranath, and Mrs. Usha, who

engraved my knowledge and directed me in a positive way.

I am deeply indebted to Dr. S. Subbarao, Dr. D. Vijaya Kumar, Dr. G. Chakaravarthy, Dr. BJ Rani Deepika, and Dr. Ch. Vijayadurga by making conversations vital in inspiring me to think outside the box and also treated me as one of their family members. I'm extremely grateful to thank my co-scholars M. Praveen, Ravi shankar, Kiran, Mallaiah, Yesudasu, Laxmikanth, Hari, Mahesh, Srinivas, My friends: Dr. Praveen naidu, Srikanth, Babu, and well-wishers for sharing their knowledge and spending valuable time with me.

I would like to express my deepest appreciation to Mixed Signal Design Lab warriors: Dr. K Krishna Reddy, Dr. Mudassir Mir Bashir, Dr. A. Suresh, Dr. Pavan Kumar sharma, Dr. Mushahhid Majeed, Dr. KVBV Rayudu, Dr. LAV Sanhith Rao, Nandini, D. Baba Fayaz, Ch. Jayaram, M. Fathima, MV Krishna Reddy, Suresh Nagula, E Koti Hanuman Reddy, Nagarani, K Kamalakar for their suggestions and support regarding technical discussions about circuits and tools. I would like to thank Dr. Karthik, Dr. Asish, Dr. Srikar, Dr. Sri Ram Tej, Dr. Siva Rama Krishna, Dr. Ahadith, Ganesh, and Dr. Rambabu for their valuable suggestions during my coursework, review presentations and thesis writing with their support.

I would like to convey my heartfelt gratitude to my childhood friends Hemaraju, and S.L. Suresh, who stood by my side and helped me morally, ethically, and financially. I would like to thank my friends Naga Mallikarjun, Dr. M. Vijaya kumar and Veerababu, who supported me financially in critical times. And also convey my heartfelt appreciation to my Intermediate friends Murali krishna (late), D. Venkateswara rao, and Dhanvi.

I want to express my deepest gratitude to my family who believe in my abilities and support. Your encouragement played an integral role in my accomplishments. I would also like to extend my heartfelt appreciation to my family: Pinni, Akka, Narendra, and Tinku.

Finally, I thank my nation India, for giving me the opportunity to carry out my research work at the National Institute of Technology Warangal. A special thanks to MHRD for its financial support.

Podeti Raveendra

Abstract

Physical unclonable function (PUF) is a promising hardware that augments the security feature for Integrated Circuit (IC) identification and authentication. It is one of the reliable solutions to many security threats as it facilitates die-unique identifier features by increasing uncertainty and prediction. PUF technology, especially for compact IoT-enabled devices, makes use of inherent Process Variations (PVs) of ICs attained by chip manufacturers and transforms them into distinctive digital keys to offer a possible solution to security-related issues. Fascinatingly, Machine Learning (ML) is a relatively prominent and inexpensive method that is frequently employed to tackle PUFs. As a result of the PUF's instability due to environmental changes, additional circuits are now being explored to fix the threats that ensue.

In this thesis, we discuss different facets of PUF design with a strong emphasis on the circuit details. From basic PUF designs presented by the researchers, the ultimate design challenges are identified, and prominent solutions are offered that should satisfy the PUF evaluation metrics before contrasting different PUF core implementations. Concerning the detailed literature, we proposed an XoR Feed Arbiter PUF (XFAPUF) that minimizes vulnerabilities by introducing more complexity in the arbitration process using a relatively smaller number of challenges against conventional Arbiter PUF (APUF). It offers better uniqueness and reliability than prior works as it achieves promising results, such as uniqueness of 50.03%, diffuseness of 49.52%, and worst-case reliability of 99.81% that ranges from 10°C to 80°C, with 10% fluctuations in supply voltage (V$_{DD}$). In addition, an enhancement in reliability is achieved by a chaotic-based challenge generation mechanism introduced for feeding APUFs to increase the non-linearity in the arbitration process.

Subsequently, an automated challenge-feeding mechanism by Recursive Challenge

Feed Arbiter Physical Unclonable Function (RC-FAPUF) is proposed to generate unique, unpredictable, and reliable keys that are independent of the challenges that are generally fed by the user. The robustness of the keys is measured by an average reliability of 99.91% and also validated through a lower prediction accuracy of 48% and 52.7% with Linear Regression (LR), and ML classifiers respectively. Furthermore, to power up suitable IoT sub-systems or sensors, a Relaxation Oscillator PUF (ReOPUF) is designed to generate a 4.4MHz frequency along with key generation. The reliability of ReOPUF responses has been improved from 95.33% for the conventional Ring Oscillator (RO) PUF to 99.19%. Besides, a Schmitt-Trigger (ST) based APUF instance is introduced that uses PVs in Hysteresis Width (HW) to attain the non-linearity in the Challenge Response Pair (CRP) mechanism. Thereby, impersonation of the responses (keys) is complex perhaps various trials are performed to predict the keys. It offers reliability while achieving 0.15%, and 0.31% Bit Error Rate (BER) concerning the variations in temperature and V$_{DD}$ respectively. Finally, the proposed PUF designs are implemented in UMC180nm CMOS technology that is suitable for prominent security assistance to IoT-enabled devices and is more resilient against ML attacks.

Contents

List of Figures

List of Tables

List of Abbreviations

AES	Advanced Encryption Standard
AI	Artificial Intelligence
AMS	Analog and Mixed Signal
APUF	Arbiter Physical Unclonable Function
ASIC	Application Specific Integrated Circuit
ATM	Automated Teller Machine
CMA	Current Mirror Array
CMOS	Complementary Metal Oxide Semiconductor
CRP	Challenge Response Pair
DAPUF	Double Arbiter Physical Unclonable Function
DES	Data Encryption Standard
DLFET	Doping Less Field Effect Transistor
DRAM	Dynamic Random Access Memory
EEPROM	Electrically Erasable Programmable Read Only Memory
FFA	Feed Forward Arbiter
FIB	Focused Injection Beam
FinFET	Fin Field Effect Transistor
FPGA	Field Programmable Gate Array
HCI	Hot Carrier Injection
HRNG	Hardware Random Number Generator
HSM	Hardware Security Module
IP	Intellectual Property
IoMT	Internet of Medical Things
LDO	Low Dropout regulator
LFSR	Linear Feedback Shift register
ML	Machine Learning
MVL	Multiple Value Logic
NBTI	Negative Bias Thermal Instability

NIST	National Institute of Standards and Technology
NMOS	N-channel Metal Oxide Semiconductor
NN	Neural Networks
OP-AMP	Operational Amplifier
OTP	One Time Programmable
PBTI	Positive Bias Thermal Instability
PKI	Public Key Infrastructure
PMOS	P-channel Metal Oxide Semiconductor
PMU	Power Management Unit
PRNG	Pseudo Random Number Generator
PTAT	Positive To Absolute Temperature
PUF	Physical Unclonable Function
PV	Process Variation
RFID	Radio Frequency IDentification
RNG	Random Number Generator
RO	Ring Oscillator
RRAM	Rotating Random Access Memory
SbD	Security by Design
SCA	Side Channel Attacks
SRAM	Static Random Access Memory
ST	Schmitt Trigger
SVM	Support Vector Machine
TCRO	Temperature Control Ring Oscillator
TPM	Trust Platform Module
TRNG	True Random Number Generator
UMC	United Microelectronics Corporation
VLSI	Very Large Scale Integration
mm^2	square millimeter
nm	nanometer
ns	nanosecond
μ**m**	micrometer
μ**s**	microsecond

Chapter 1

Introduction

Security is the major concern for Internet of Things (IoT) enabled devices and is a challenging area as it is mandatory to protect our privacy concerns from various security attacks. IoT [1] is one of the fast-growing technologies that has simplified our personal lives and brought easy exposure to the outside world. It is not only limited to our personal lives but also can be advantageous for our future industrial systems to control and access devices without human intervention. It has brought revolution across all computing application domains, such as home automation, wearable electronics, Artificial Intelligence (AI) enabled services, etc [1,2]. On the other hand, IoT devices face many issues as they are susceptible to cyber-attacks and need many computational resources while consuming low power. For example, IoT devices frequently access the confidential information of the user with security attacks, which are performed by intruders from unauthorized resources. Nowadays, most of the IoT-enabled devices are equipped with Integrated circuits (ICs) to withstand malicious attacks.

ICs are witnessing great demand as they are being used to execute security-critical jobs and handle sensitive information in electronic gadgets [1]. So, secret keys are essential to identify and authenticate users in the development of the system's security. Many applications, such as intellectual property protection and software licensing, key cards to regulate access to restricted areas, smart card usage to perform financial transactions, and smartphones to store sensitive data of confidential papers, personal emails, etc., are emerging rapidly [3]. The protection of the secret keys is the main function of these applications enabling active logical controls to identify and authenticate users. However, malicious users can impersonate authorized users against various kinds of logical and physical tampering attacks when the secret key is exposed. Therefore, a common element is required to enable the aforementioned security operations, which an attacker cannot access or replicate.

To authenticate a device and secure confidential information, the existing practice is to store a secret key in memory-based techniques like fuses, Electrically Erasable Programmable Read-Only Memory (EEPROM), and cryptographic mechanisms like digital signature and encryption. Eventually, responses (secret keys) are always retained in digital form in memory-based systems. As a result, robustness decreases and cost increases as non-volatile memory systems are frequently subjected to invasive attacks. Also, it is due to the usage of battery-backed Random Access Memory (RAM), where keys can be read afterwards and stored for a long period. A high level of security is achieved when the IC must be safeguarded with costly tamper-sensing circuitry that must be continuously powered by batteries.

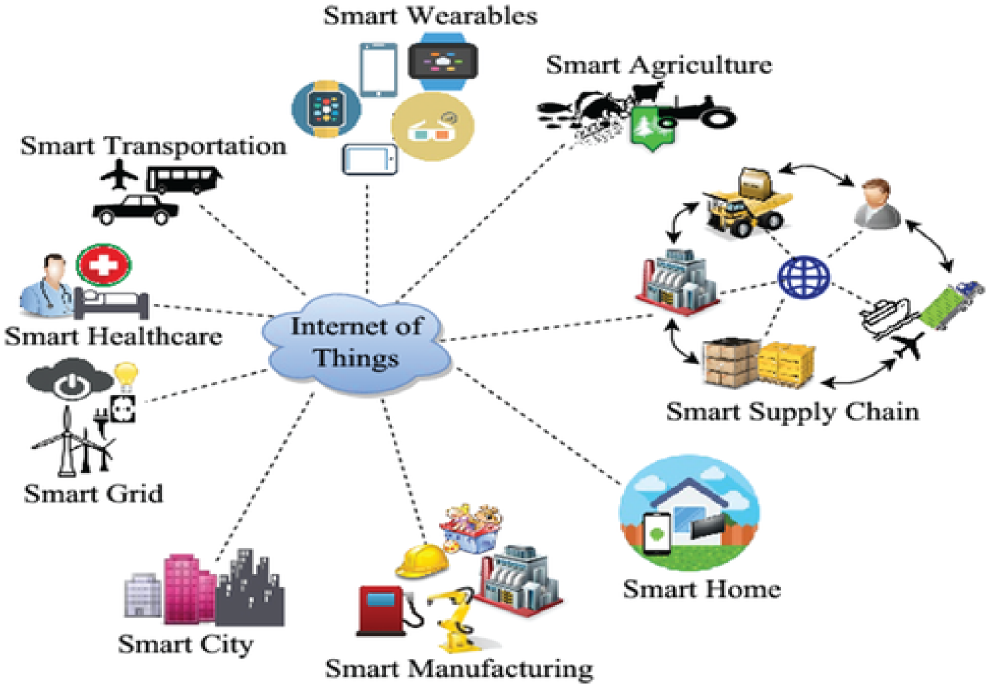


Figure 1.1 IoT in the security domain [3]

1.1 Internet of Things (IoT)

IoT is a network of interconnected physical objects or ”things” that are embedded with sensors, software, and other technologies to collect or exchange data with other devices/systems over the Internet [1]. As shown in Fig.1.1, IoT things might be anything from commonplace like domestic appliances, automobiles, and wearable devices to industrial machinery and building materials. IoT has the potential to transform firms by facilitating more connectivity, automation, and data-driven decision-making [4]. The enormous amount of data generated by connected devices must be managed, and there are issues with data security, interoperability, and management. IoT is probably going to become a bigger part of how we connect with the physical world and the digital world advances in technology.

A PUF-based device authentication scheme PMSec [112] provides a mechanism that is appropriate for the Internet of Medical Things (IoMT). This authentication scheme's primary benefit is that no information about IoMT devices is kept in server memory. It took between 1.2 and 1.5 seconds to fully authenticate the devices. An Oscillator Arbiter Hybrid Physical Unclonable Function was employed to verify the suggested authentication method. Moreover, the device information is not kept in the server's memory, which is one benefit of this technique. Although each device has a PUF module that can be used for authentication, the server RAM does not save the challenge and response from the client PUF modules. This can assist in situations where the device information is not compromised and the attacker gains access to the hacked server.

1.2 IoT Cryptographic Primitives

IoT includes a wide range of internet-connected devices, including industrial sensors and smart thermostats. Since many IoT devices collect sensitive data or control crucial activities, their immense scale and diversity present several security challenges. Cryptography is one of the key principles of IoT security that deals with security issues associated with IoT-enabled devices. The building blocks for building secure protocols and security services are known as cryptographic IoT primitives [5] that are discussed in the following sections for the provision of IC security.

1.2.1 Symmetric Key cryptography

Symmetric key cryptography [5, 6] is a sort of encryption technique where the same key is used to both encrypt and decrypt messages as illustrated in Fig.1.2. In the past, secret communications between governments and militaries have been made possible in great part by using this method of data encoding. The symmetric key is also referred to

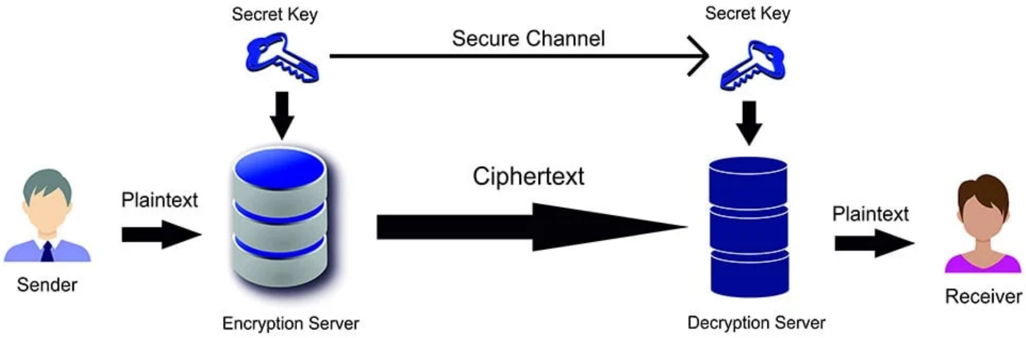


Figure 1.2 Symmetric key cryptography [5,6]

as shared-key, secret-key, one-key, and eventually private-key cryptography. It is obvious that the shared key must be known by the sender and the recipient when using this type of cryptography. The distribution of the key presents a challenge with this method.

1.2.2 Asymmetric Key cryptography

A Public Key Infrastructure (PKI) [5,6] is a cryptographic technique requiring two separate keys, one to lock or encrypt the plain text and another to unlock or decrypt the cipher text built on asymmetric keys. As represented in Fig.1.3 no key can perform both tasks. A private key is kept private, while a public key is made public. The technology enables private communication from the general public to the owner. The system functions as a signature verification for documents locked by the owner of the private key.

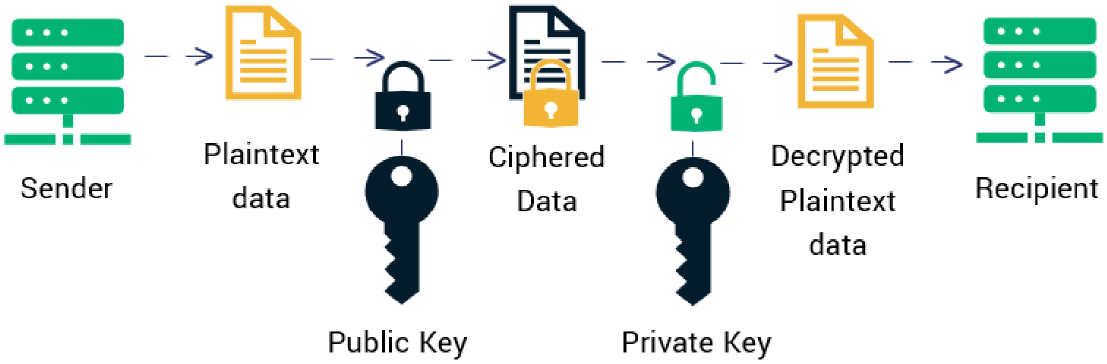


Figure 1.3 Asymmetric key cryptography [5,6]

1.2.3 Hash functions

A mathematical operation employed in cryptography is known as a hash function [5, 6] is shown in Fig.1.4. Most hash functions accept inputs with varying lengths and outputs with fixed lengths. The message-passing abilities of hash functions are combined with security features in a cryptographic hash function. Hash functions that ”map” or transform a given data set into a fixed-length bit string known as the ”hash value.” The complexity and difficulty of hash functions, which are employed in cryptography, can vary. However, for the provision of security to the messages, passwords, and cryptocurrency, hash functions are the best choice to employ.

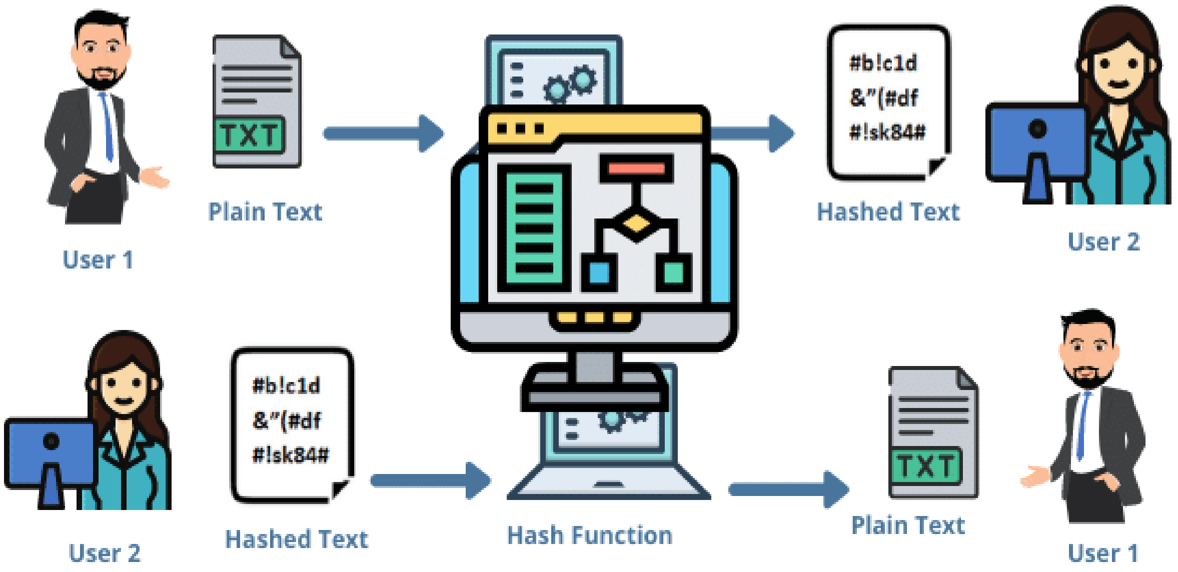


Figure 1.4 Hash functions [5,6]

1.2.4 Random Number Generators (RNGs)

Random numbers play a crucial role in cryptography applications due to their non-deterministic nature. Basically, RNGs or Random Bit Generators (RBGs) [7] shown in Fig.1.5 are preferred to generate random numbers or random bits to manipulate the system by foreseeing processes. Random numbers are essentially required in the following applications such as cashless payments, Automated Teller Machines (ATMs), online payments, e-banking, point of sale, prepaid cards, etc. In cryptography, the key protocols use random numbers to generate a secret key between the sender and receiver. Whereas, the presumption of the secret key will diminish the key rate when random numbers are generated by RBGs. A Pseudo-Random Number Generator (PRNG) [8] produces periodic or deterministic random numbers based on a mathematical formula, which is determined by the initial state called a seed. PRNGs form a strong correlation between 0’s and 1’s thereby increasing the cryptographic strength. In contrast to PRNGs, Hardware Random Number Generator (HRNG) [8] is proposed to generate random numbers through randomness extracted from physical processes that make them a better candidate for secret key generation.

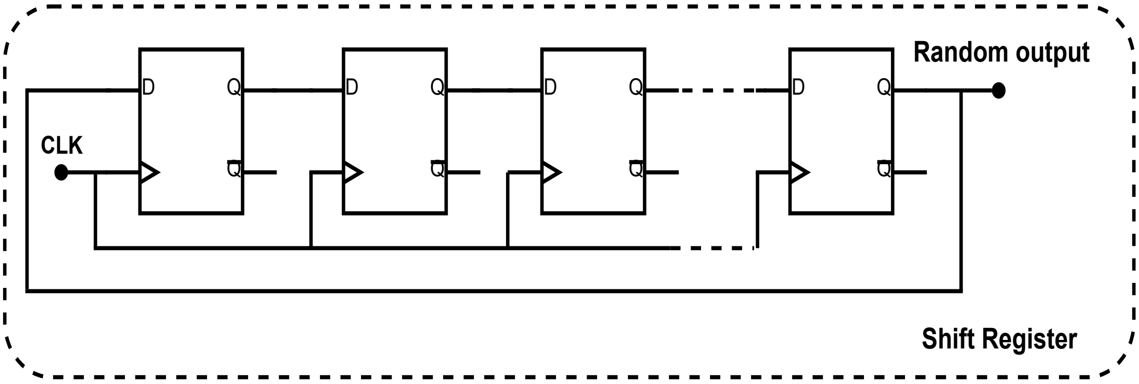


Figure 1.5 Random Number Generator

1.2.5 Lightweight cryptography

Lightweight cryptography is an encryption method that features a small footprint and/or low computational complexity. It can be measured by the execution time and the number of calculations used to estimate processing speed. Moreover, it is aimed at expanding the applications of cryptography to constrained devices [9] based on international standardization and guidelines. For the implementation of lightweight cryptography, factors like circuit size (or memory size), power consumption, and processing delay (delay, throughput) should be considered. The respective cycle of lightweight cryptography is represented in Fig.1.6.

Generally, the size is the major factor that determines whether a design can be implemented in a certain device or not. Whereas power consumption is crucial for battery-powered devices, power is particularly important for devices like Radio Frequency Identification (RFID) and energy harvesting systems. A low delay is crucial for the real-time control processing of control-based systems but a high throughput is required for devices with significant data transmissions, such as a camera or a vibration sensor.

1.2.6 Cryptographic Algorithms

The mathematical processes incorporated in cryptographic algorithms [6, 9] protect the sensible data of the user. These methods convert plain text (readable data) into cipher text (unreadable data), and vice versa. They are essential in maintaining the privacy, accuracy, and integrity of data. It is critical to take into account the unique

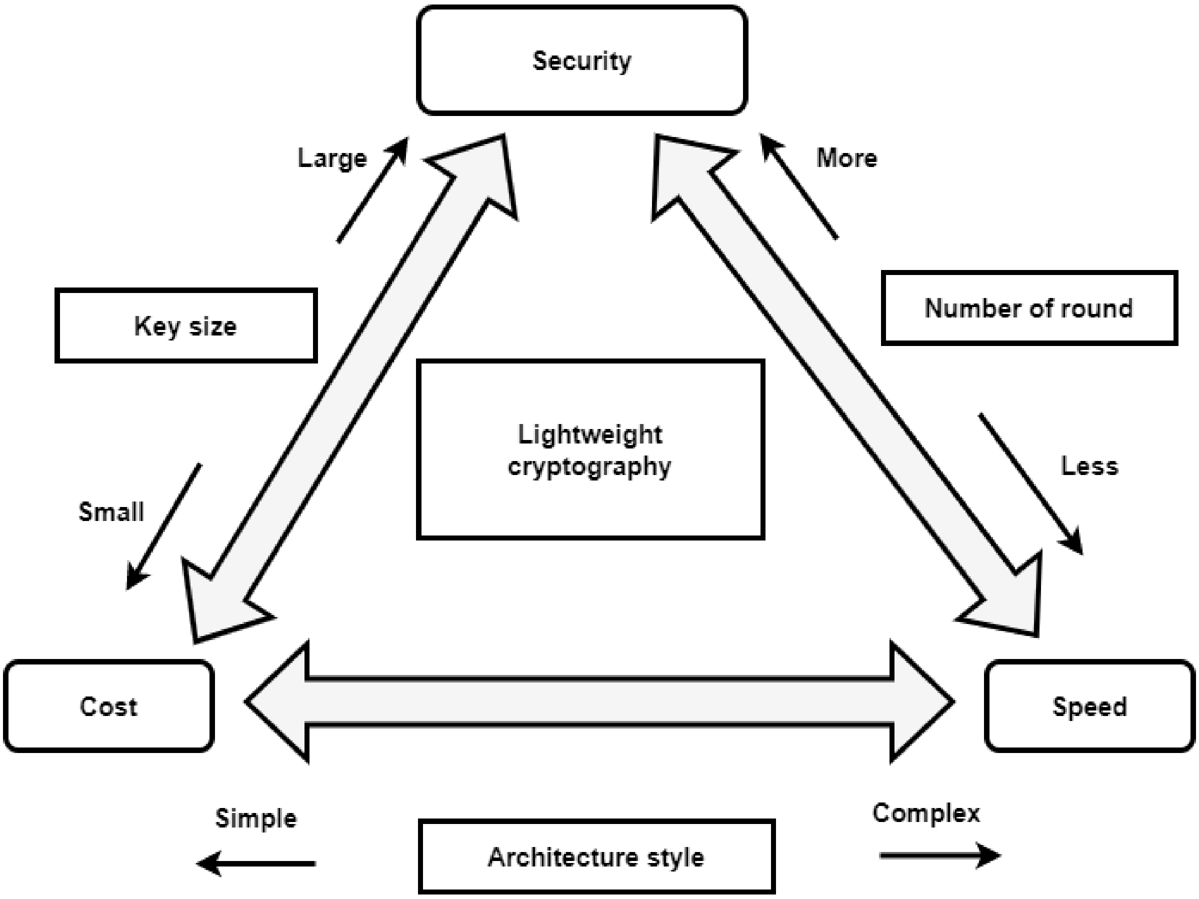


Figure 1.6 Lightweight cryptography [9]

security concerns, performance constraints, and eventual shortcomings while selecting a cryptographic algorithm. The accurate implementation of the algorithms can be ensured by well-tested and well-known cryptographic libraries that are equipped in crypto ICs to execute challenges or keys. Even though they are accurate but are not reliable due to the Process Variations (PVs) existing in the ICs that are discussed in the following section.

1.3 Process Variations (PVs)

Individual chips can differ in performance and behaviour due to variations in ICs, which can come from a variety of sources. PVs [10] are the variabilities in circuits, such as Random Dopant Fluctuations (RDFs) and process control limitations, that are challenging for any technology nodes. Additionally, there is a mismatch between the sizes set up during design and the sizes achieved during manufacture due to process variances. For instance, with a 65 nm CMOS process technology node, it is anticipated that the differences in a MOSFET's threshold voltage and channel length can reach up to 30% [107]. PVs affect the performance of circuit operation at the gate level even though the circuits are designed with identically sized gates. The design's functionality is impacted by process variances. The ability to convey current and delay can be impacted by changes in the channel length. Leakage and delay below the threshold can be impacted by changes in the threshold voltage. Variations in the process can alter the circuit and system parameters from the design specification, which could impact the yield [107].

As the technology scales down the performance and speed of the ICs may increase but result in PVs. Due to PVs, delay variations occurred and affected the frequency performance of the design and yield. This can be stated as how many chips can perform within the target frequency after fabrication. To create reliable circuits and systems with the highest possible yield and lowest possible cost, variability-tolerant design is required. To create a chip that can withstand process variations, it is crucial to include variability awareness in the early design cycles. The common PVs are,

- **Intrinsic material variability:** The characteristics of transistors and the behaviour of the entire circuit can be impacted by variations in material qualities at the atomic level.
- **Dopant fluctuations:** Transistor performance can be affected by the precise location and concentration of dopant particles during manufacture.
- **Oxide thickness:** Oxide thickness variations can affect the threshold voltage and other properties of transistors.
- **Lithography and etching:** Critical dimensions and forms of circuit elements may deviate due to variations in photolithography and etching procedures.

Possibly, either static or dynamic fluctuations in the parameter may occur [107]. Variations in the manufacturing process are the source of the static parameter variations. On the other hand, changes in workload and environmental circumstances cause dynamic parameter variations to occur over time as the circuit and system operate. There are numerous potential sources from which the process deviations can arise. Process changes can therefore be at the wafer, reticle, or local levels, and they have fairly distinct characteristics.

A novel hardware-intrinsic security mechanism, Physical Unclonable Function (PUF) [11] came into existence to utilize PVs in a proper way that is inexpensive, unique, and secured. Also, it provides reliable solutions for security issues faced by IoT devices. The PVs observed in PUF could generate unique signatures as identifications when random challenges are fed during runtime. These PVs can be a bit higher than the physical variations. Also, they are considered major side effects that occur during the manufacturing process, so circuits can be defective. Fortunately, APUF can withstand PVs since its responses depend on the difference in delays between two adjacent paths, which are fed as input to the Switch Component (SC). Due to PVs, some challenges may affect the arbiter latch with setup time violation, which leads to an unpredicted response, thus resulting in the poor reliability of the PUF. Therefore, to make the conventional logic systems unique and unclonable, their design has to be variability-aware in the implementation of PUF.

1.3.1 Sources of variances in ICs

The PVs [10] can be classified into two categories: systematic variations and random variations. Random variations are intrinsically unpredictable, whereas systematic variations are deterministic and can be predicted or controlled. The common sources of variations shown in Fig.1.7 are discussed below.

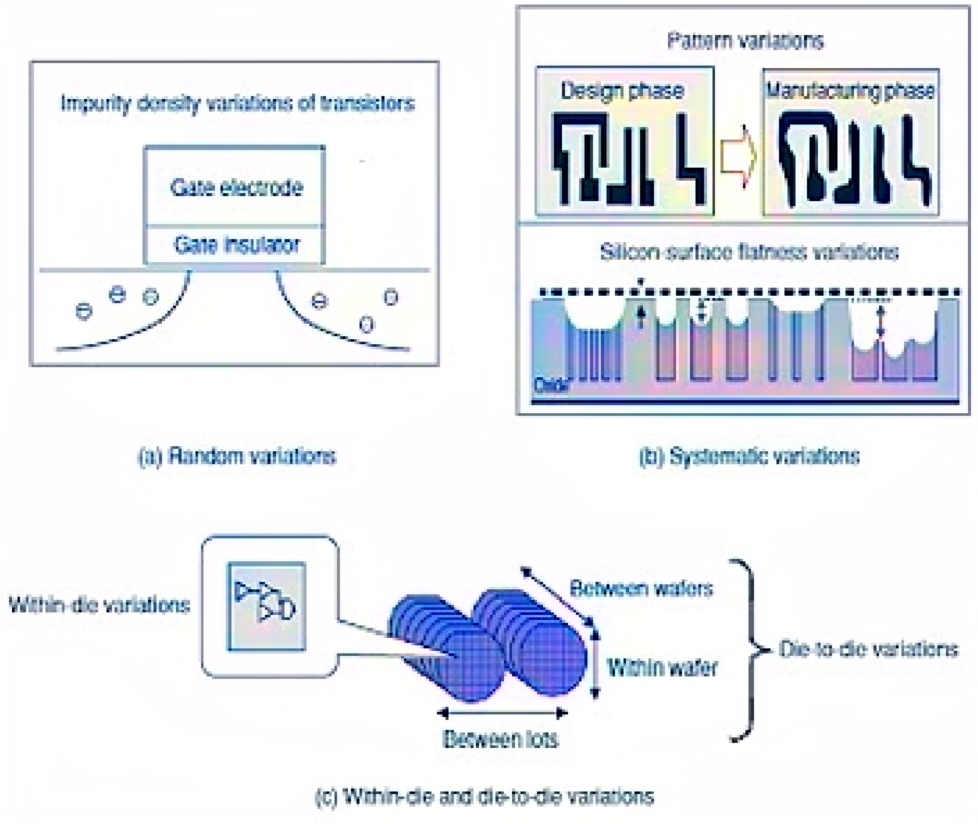


Figure 1.7 Sources of variances in ICs [10]

1.3.1.1 Layout and design variations

- Layout-Dependent Effects: Due to proximity effects, optical diffraction, and other considerations, the physical architecture of transistors and interconnects can affect performance.
- Parasitic Capacitance and Resistance: Circuit timing and signal integrity can be affected by parasitic components such as capacitance and resistance that can vary depending on the arrangement.

1.3.1.2 Thermal Variations

- Thermal Gradients: The performance of a circuit can change as a result of variances in transistor properties caused by temperature differences across the semiconductor.

1.3.1.3 Voltage and Bias Variations

- Supply voltage variation: Circuit speed, power consumption, and noise margin may be impacted by changes in the power supply voltage.
- Threshold voltage variation: The switching behaviour of digital circuits is impacted by changes in transistor threshold voltage brought on by manufacturing and bias variations.

1.3.1.4 Random Variations

- Statistical variability: Statistics-based fluctuations in parameters like carrier concentration and channel length are caused by quantum mechanical phenomena.
- Thermal Noise: It results from random electron migration owing to temperature, and reduces the precision of analog circuits.
- Random Telegraph Noise: Over time, random changes in transistor properties may be the result of discrete trapping and untrapping of charge carriers.

1.3.1.5 Aging and Wear

- Electromigration and Stress Migration: Circuit reliability and performance may be impacted over time by changes in the characteristics of metal conductors brought on by electromigration and stress-induced effects.

- Negative Bias Thermal Instability (NBTI) and Positive Bias Thermal Instability (PBTI): Due to continuous exposure to bias conditions, these effects gradually produce threshold voltage alterations in transistors.
- Hot Carrier Injection (HCI): It describes the process by which high-energy electrons (also known as "hot carriers") acquire sufficient energy to go past potential obstacles in a transistor's gate oxide or junction, eventually causing device degradation or failure. MOS transistors, which are frequently employed in ICs, are particularly pertinent to this variation.

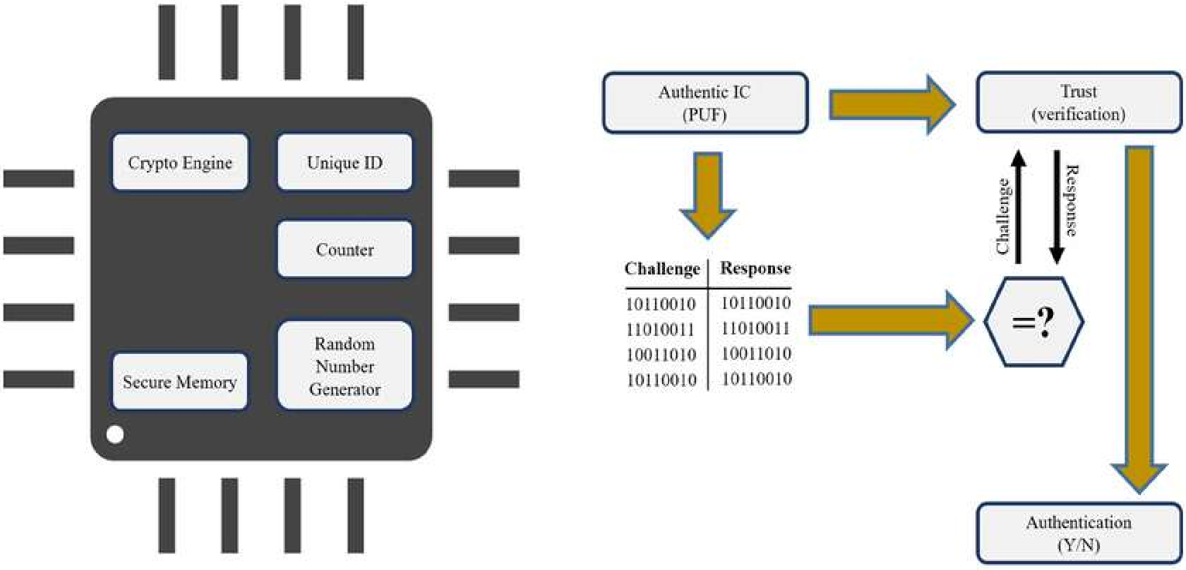
It is essential that the variances must be minimized to maximize the performance of the ICs. Process control, redundant circuit design, statistical analysis, and error-correcting mechanisms are only a few of the methods used to lessen the effects of variances. However, innovative manufacturing techniques like adaptive lithography and process compensation are used to overcome variances that may improve chip yield and quality.

1.4 Physical cryptographic primitives

Cryptographic operations that rely on the physical characteristics of objects or systems are known as physical cryptographic primitives. They take advantage of PUFs [11] or other hardware-based properties, as opposed to conventional cryptographic primitives, which are based on mathematical techniques. These are especially important for hardware security in situations when software-based techniques can be ineffective or inappropriate.

1.4.1 Physical Unclonable Functions (PUFs)

PUFs can extract a response from hidden timing or delay that occurred due to inherent manufacturing variations and could replace digital memories for storing keys. Moreover, these circuit delays produce a volatile response (key) that is perhaps difficult to expect or extract. Even though a PUF key is implemented on an IC, it is being cloned to access physically using different attacks. Modern cryptographic algorithms provide security to IoT devices but are unable to counterfeit since the security blocks are designed with cryptographic hash functions (implemented by mathematical and algorithmic mechanisms). So, when cyber-attacks happen, they fail to provide secure communication among IoT devices. In fact, it is a tedious task to build security functions for inexpensive IoT devices. Generally, PUF is not only to protect hardware components i.e. ICs sourced from manufacturers but also handles serious reliability implications. An on-chip PUF is a Challenge-Response (CR) based hardware function and exploits the inherent random physical variations in the manufacturing process. The physical variations of



Challenge	Response
10110010	10110010
11010011	11010011
10011010	10011010
10110010	10110010

Figure 1.8 Physical Unclonable Function [12]

PUF are determined by deep sub-micrometre level variations, which are produced due to uncontrollable deviations in the manufacturing process [12]. These variations are complex and random in nature making PUF very hard to be cloned. Hence, they are tamper-resistant against attacks. The extracted instance-specific keys from hardware components, which are hard to predict, are unique and unclonable to identify or authenticate each device [12, 13]. A PUF shown in Fig.1.8 can efficiently improve the device's resistance to various attacks when an on-demand generation of random keys from a CR-based scheme exists. Moreover, it ensures that there is no storing of keys in non-volatile memory during deployment.

1.4.2 Hardware Security Module (HSM)

A Hardware Security Module (HSM) is a specialized crypto processor created with the goal of safeguarding the crypto key lifecycle. It adds additional security for sensitive data by safely managing, processing, and storing cryptographic keys inside a hardened, tamper-resistant device. HSMs illustrated in Fig.1.9 are employed to provide cryptographic keys [14] for crucial operations like encryption, decryption, and authentication for the use of applications, identities, databases etc. However, HSMs serve as trust anchors that safeguard the cryptographic infrastructure of some of the most security-conscious operations in the world.

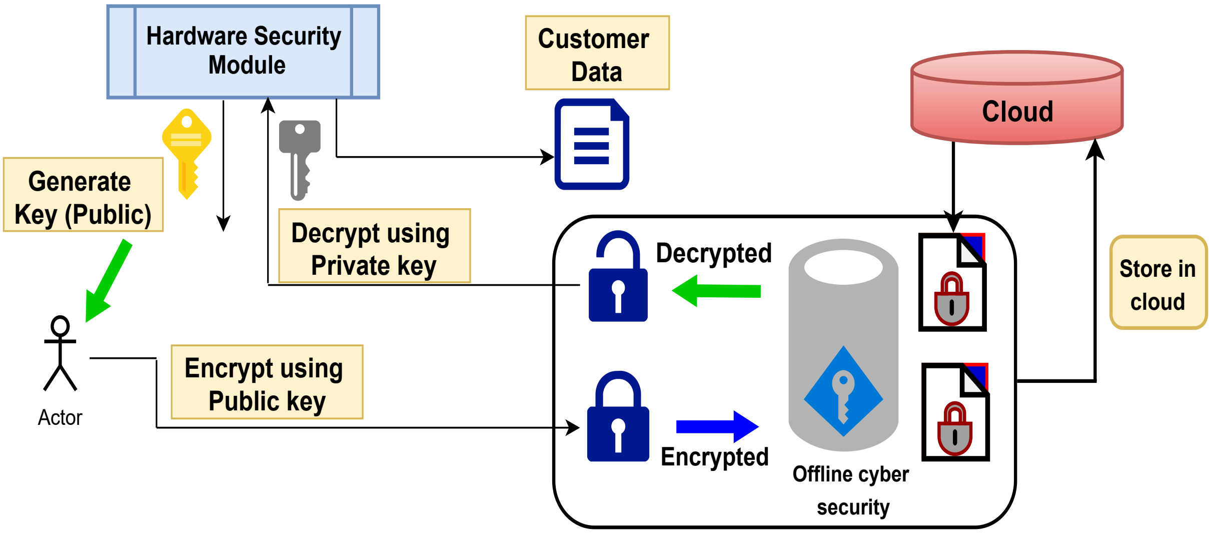


Figure 1.9 Hardware Security Module [14]

1.4.3 True Random Number Generators (TRNGs)

The generation of random numbers is crucial for high-speed processing at the core part of data encryption systems. These systems rely on fast RNGs for stochastic modeling, Monte Carlo simulations, etc [15]. The source of randomness is uncertain in a TRNG [16] that is typically accomplished by hardware. TRNG shown in Fig.1.10 is based on a physical source which makes it difficult to anticipate a random value, so the random number it generates is difficult to predict. In view of the complexity involved in creating an equal value, the random number generated by the TRNG is a secure method. The output of a TRNG may be biased in some way, such as having more ones than zeros or vice versa. There are several ways to alter a bit stream in order to lessen or eliminate bias. However, the bit stream can be generated through “de-skewing algorithms” which

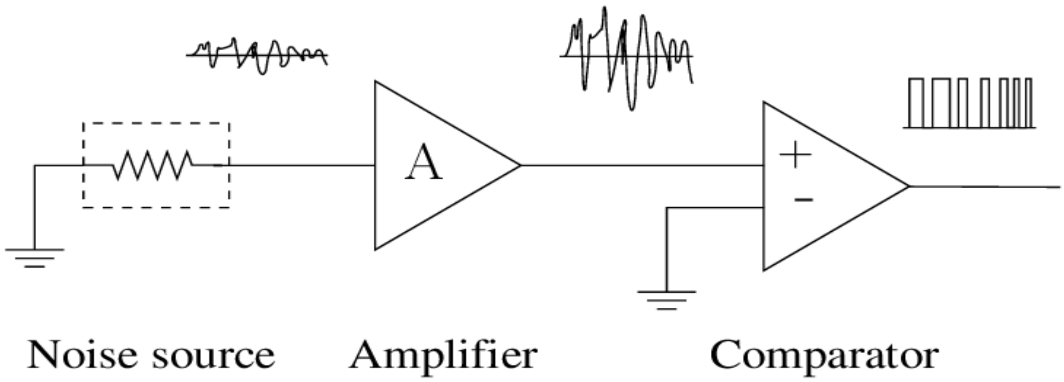


Figure 1.10 True Random Number Generator [16]

run through a hash function. The hash function converts an input of any length into an n-bit result. The hash function can acknowledge blocks of m input bits with m×n for de-skewing. TRNG is too repetitive, and there are several complex PRNGs [17] available. TRNGs can take advantage of both physical and intangible noise sources represented in Fig.1.10. Generally, the following physical phenomena are used to generate random numbers in logic devices.

- Clock Jitter: The clock edge is changed from its optimal position.
- Metastability: A circuit has the power to remain in an infinite state for an arbitrary amount of time.
- Chaos: It is the unpredictability of a system that is deterministic and highly responsive to its initial conditions.
- Analog signals: The noise present in thermal noise, and other types of noise are present in analog signals.

1.4.4 Side-channel analysis (SCA)

Side-channel analysis (SCA) [18] refers to a variety of techniques for taking advantage of inadvertent information leakage from a device's process (such as a computer program or application). Every device leaks some sort of side-channel information for each instruction, piece of processed data, or input to the device, whether it is a restricted IoT device, a smartphone, a laptop, or a supercomputer with hundreds of CPU cores. The side channels shown in Fig.1.11 have happened in distinct forms of physical characteristics like power usage or electromagnetic emissions and logical characteristics like processing speed or memory access patterns. An attacker may be able to observe the variation in side-channel emissions that relate to internal activities by deducing both the operations carried out and the data processed by the device. Moreover, it is possible to extract secret data, such as a cryptographic key, by observing and categorizing data-dependent side-channel emissions, or side-channel leaks when the hidden data's content directly influences it. Instead of taking advantage of software flaws or algorithmic weaknesses, side-channel attacks concentrate on gathering information from a system's physical implementation. It is possible to determine the actions taking place inside a device and, in some situations, recover encryption keys or other sensitive data by examining power consumption patterns. The general approach to extracting binary information from power traces is,

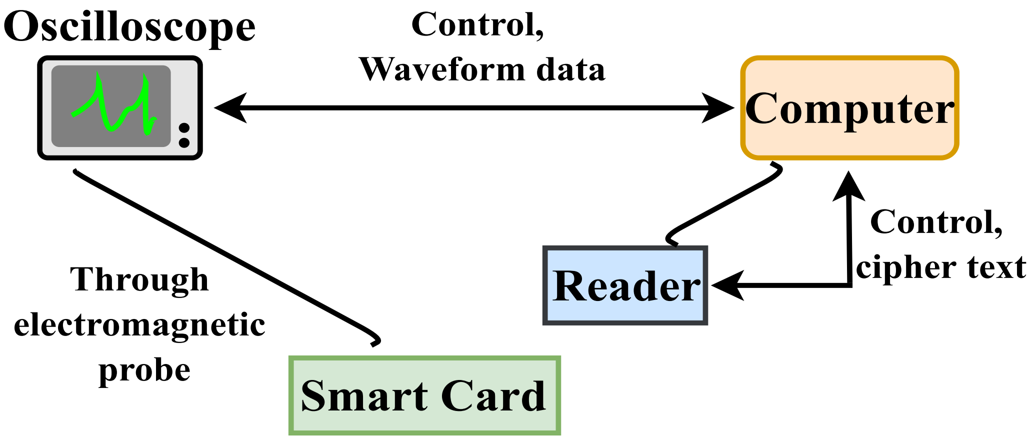


Figure 1.11 Side channel attack materials [18]

- Utilize statistical techniques to associate particular patterns of power usage with binary operations when there are enough traces and an understanding of the patterns.

- Extract specific pieces of information, such as encryption keys, advanced approaches can be used, such as Differential Power Analysis (DPA) or Correlation Power Analysis (CPA).

The first-ever hardware-assisted blockchain for simultaneously handling device and data security in smart healthcare. This article [113] presents the hardware security primitive PUF and blockchain technology together as PUFchain 2.0 with a two-level authentication mechanism. The proposed PUFchain 2.0 [113] security primitive presents a scalable approach by allowing Internet of Medical Things (IoMT) devices to connect and obtain

PUF keys from the edge server with an embedded PUF module instead of connecting a PUF module to each device. Blockchain is a decentralized, unchangeable transaction record that is kept on file at every network node. A system of consensus is a standard protocol that is used to validate and add transactions between any two nodes in the network to the chain. The implementation and outcomes have demonstrated that the combination of PUF and blockchain technology [113] can provide safe, intelligent healthcare. Every security protocol now in use for smart healthcare is centred around either blockchain-based data security or hardware-assisted security. To provide security for IoMT device authentication and data integrity guarantees through a two-level authentication protocol, this article [113] suggested and implemented the PUFchain 2.0 primitive, which combines Blockchain with PUF.

1.5 Motivation

The generation and protection of the secret keys, which are the main function of security applications, enable active logical controls to identify and authenticate users. However, malicious users can impersonate authorized users against various kinds of logical and physical tampering attacks when the secret key is exposed. Therefore, a common element is required to enable the aforementioned security operations, which an attacker cannot access or replicate. To authenticate a device and secure confidential information, the existing practice is to store a secret key using memory-based means fuses and Electrically Erasable Programmable Read- Only Memory (EEPROM) and using cryptographic mechanisms like digital signature and encryption.

The digital algorithms [6] manage the security attacks with cryptographic algorithms e.g. Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Message Digest (MD). However, digital platforms produce a key generation with hash functions (implemented by mathematical algorithms and cryptographic algorithms) that are able to make secure and counterfeit to some extent. So, PUFs are considered the more secure designs in IoT security because of their unpredictable nature. PUFs don't need any memory function to store the keys because they produce on-demand key generation for identification and authentication. The major issues observed in hardware security are,

- Persistent security threat in the digital domain
- Privacy inefficiency in IoT-constrained devices
- Lack of implementing AI development in the analog environment
- On-chip encryption has high memory overhead which is not practical for constrained IoT nodes
- Need to analyze a device for security purposes i.e. ensuring it's resistant to side-channel attacks
- Necessity of improvement in the resilience of PUF systems

1.6 Problem Statement

Generally, responses (secret keys) are always retained in digital form in memory-based systems. As a result, robustness decreases and cost increases as non-volatile memory systems are frequently subjected to invasive attacks. Also, it is due to the usage of battery-backed RAMs, where keys can be read afterwards and stored for a long period. A high level of security is achieved when the IC must be safeguarded with costly tamper-sensing circuitry that must be continuously powered by batteries. In the replacement of digital memories for storing keys, PUFs are used to extract a response from hidden timing or delay that may result due to inherent manufacturing variations [10]. Moreover, these circuit delays produce a volatile response (key) that is perhaps difficult to expect or extract [12, 13]. The provision of security to constrained IoT-enabled devices helps the user to protect themselves from exposing valuable information. The issues summed up regarding the provision of security to the ICs are,

- Avoid exploiting the secret information from authorized devices.
- Provision of security to the ICs against unauthorized attacks
- Provision of on-demand key generation with enhanced reliability
- Memory-less maintenance at endpoint devices.

1.7 Research Objectives

An arbiter-based scheme generates digital information from the PUF responses through the absolute delay values of two identical delay paths and evaluates the identification capability, authenticity, and security. The proposed architectures improve the reliability of arbiter-based PUFs against various malicious attacks by adding impulsive non-linearity. The issues related to the provision of security using PUFs are addressed by following the objectives mentioned below.

- Designing efficient PUF topologies to enhance the identification or authentication of ICs.
- Implementing arbitrary delays to produce uncertainty in the switching operations
- Design low-frequency PUFs suitable to IoT sensors
- Evaluate the reliability of PUFs from security analysis
- Introduce power management circuits to feed PUFs for the challenge generation
- Adding random noise or purposefully changing the power consumption to conceal sensitive activities
- Apply machine learning algorithms to evaluate the PUFs against sophisticated attacks.

1.8 Thesis Contributions

1. XoR Feed Arbiter Physical Unclonable Function (XFAPUF) for reliable key generation in IoT security: Introduced feed-forward mechanism to attain non-linearity in the arbitration process to reduce manual feeding of the challenges. Thereby, prominent randomness is achieved that can be measured in terms of unpredictability.

2. The Chaotic-based Challenge Feed Mechanism for Arbiter PUFs with enhanced reliability: Introduced chaotic function in the challenge generation to attain non-linearity in the arbitration process. Whereas the challenge generation is from the Chaotic Code Generator (CCG).

3. Recursive Challenge Feed Arbiter PUF (RC-FAPUF) for Key Generation: Introduced automated challenge generation mechanism through XoR gates between switch components, which are used for the arbitration process. Thereby, a high randomness is achieved to enhance the reliability.

4. ReOPUF: Design of Relaxation Oscillator Physical Unclonable Function for Identification Applications: Generated required frequency for IoT nodes with Relaxation Oscillator and attained more reliability. It is the replacement for RO PUF and is claimed that more reliable and power-efficient.

5. Schmitt Trigger Arbiter PUF (ST-APUF) with enhanced Uniqueness and Reliability in IoT security: Introduced arbitration between STs to attain the non-linearity using Hysteresis Width (HW) variation. Based on the HW differences it is claimed that the high uniqueness and randomness.

6. Low Dropout Regulator (LDO) based challenge generation mechanism: Designed to feed ReOPUFs and STPUFs to augment the randomness in challenges. Thereby, the reliability is achieved by the challenges generated through the power traces that occurred from LDO in terms of undershoot and overshoot.

1.9 Thesis Organization

Chapter 1: Contributes an introduction to the PUFs, Motivation, Objectives, and Thesis organization.

Chapter 2: Imparts literature survey corresponding to the related works and basic implementations of arbiter PUFs.

Chapter 3: Provides design and implementation of XFAPUF for key generation along with automated challenge generation through Chaos-PUF.

Chapter 4: Presents design and implementation of RC-FAPUF for a reliable key generation. without any external feed from the user

Chapter 5: Provides design and implementation of ReOPUF to power up IoT sensors.

Chapter 6: Ensues design and implementation of ST-APUF for enhancement in reliability.

Chapter 7: Augments the randomness by incorporating LDO as a key generation mechanism.

Chapter 8: Gives the conclusion for the proposed PUF designs and the Future scope will give the enhancements and possibilities to strengthen PUF designs.

The contributions of the aforementioned chapters will convey information about the design of various security mechanisms for key generation, supportive challenge feed mechanisms, and performance evaluation through PUF metrics. The following chapter will introduce the basic background of PUFs and their mechanism in the application of IoT. Subsequently, various PUFs will be discussed along with the inclusion of different types of attacks.

Chapter 2

Physical Unclonable Functions (PUFs)

PUFs are a family of security components that use the distinctive physical properties of semiconductor devices to provide random and unrepeatable digital identifiers or keys. PUFs are used in a variety of applications, such as device anti-counterfeiting, secure key generation, and authentication, to improve security. In recent years, different architectures in the Complementary Metal Oxide Semiconductor (CMOS) level for PUFs have been proposed by researchers for IC-level security. Among them, Arbiter PUF [11–15] is the conventional delay-based approach realized between two symmetrical engaged paths that provide efficient Challenge–Response Pair (CRP) space for device identification and authentication. PUFs have drawn interest because of their capacity to offer reliable, hardware-based cryptography solutions. They provide a mechanism to produce secrets that are firmly connected to the unique physical characteristics of particular chips, making it challenging for attackers to reverse-engineer or clone equipment.

2.1 Concept of PUF in IoT device

With the increasing demands of security, key generation and device authentication become the most challenging design concerns, particularly in developing security for IoT-enabled devices. Traditional security mechanisms suffer from power limits, and store keys in erasable programmable memories. To implement encryption and authentication, the tamper-resistant devices are equipped with countermeasures that are developed to defeat different kinds of physical attacks. However, resources like memory, Central Processing Unit (CPU) and limited battery power are not affordable to implement security using classic cryptographic solutions. Therefore, PUF has become a relatively simple and fast solution for security. PUFs are promising secure hardware primitives that produce device-dependent CRPs [19–21] based on unclonable properties and provide reliable key generation. The keys generated by PUFs are more resilient to malicious attacks from physical tampering attempted by the intruders. Fig.2.1 shows the security concept of IoT-enabled devices.

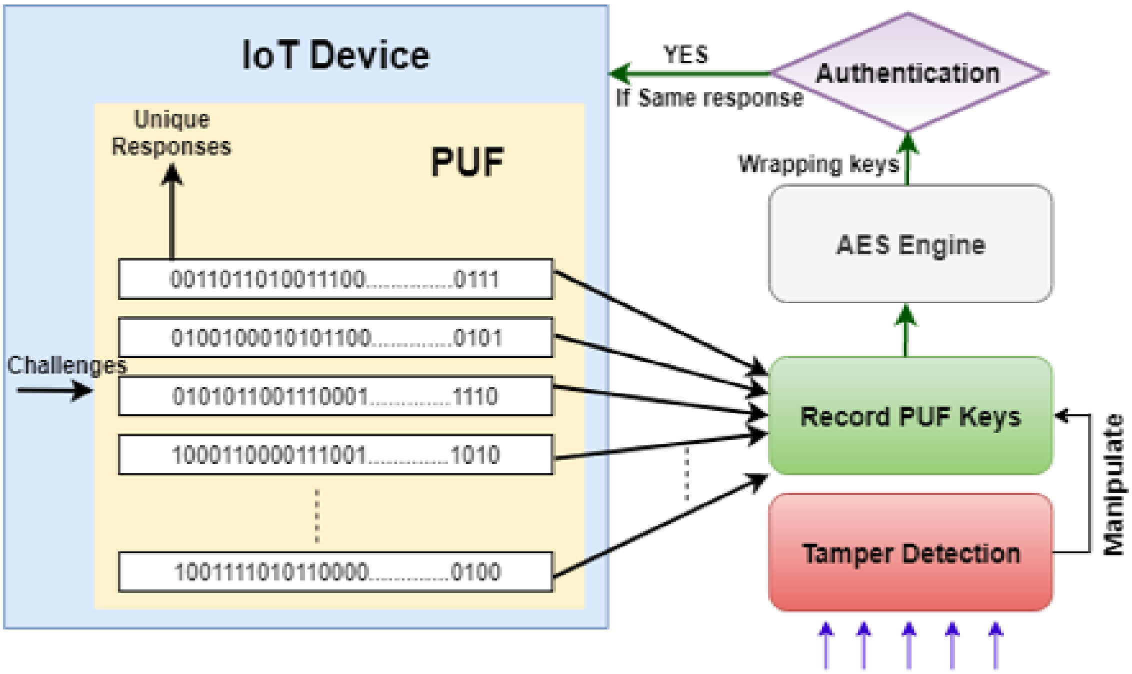


Figure 2.1 PUF in IoT device

An IoT device equipped with PUF generates unique IDs as PUF keys and is shared through a gateway with the cloud. PUF keys are acquired by the Advanced Encryption Standard (AES) engine which is situated in the cloud and can convert plain text to cipher text. Thus, the IoT device is to be identified and authorized with encryption. For example, an IoT-enabled sensor node is arranged in the field to sense the temperature or moisture data continuously from the atmosphere and upload the data to the cloud at every predefined interval of time. This stipulated data could be protected in the cloud by adding PUF keys generated from the designed PUF and correlated with the AES engine can produce encrypted data. While tampering is detected in the node or cloud, there is the chance that data manipulation is possible by intruders. So, an efficient security mechanism i.e.PUF with high uniqueness and reliability is to be deployed to identify or authenticate the sensor node.

Based on the fabrication, the PUFs fall into the categories of silicon and non-silicon

[108]. Silicon PUFs are made on the same die as the circuit and interface with other ICs. Different circuit features (timing and delay information) are produced as a unique response for a specific challenge, and PV during fabrication is captured as a challenge. Non-silicon PUFs are unique fabrication methods that are outside the scope of conventional CMOS fabrication technologies. Rather than using ICs, the response is derived from the challenge set acquired from the random physical variation in the physical system.

PUFs are designed to work in conjunction with or in substitute for other hardware authentication methods including smart cards, hardware one-time password (OTP) tokens, and biometric authentication (where the hardware is linked to a specific individual) [108]. PUFs, offer a dual layer of protection for biometric authentication and PUFs can only supplement biometric authentication; they cannot replace it. Biometric authentication identifies a specific individual while PUFs provide a specific piece of hardware. PUFs, on the other hand, are far more secure and cannot be stolen, unlike smart cards, therefore they can entirely replace them. Depending on whether two layers of protection are wanted (OTP token and PUF) or if a single layer of protection (OTP token of PUF) is adequate, PUFs can either complement or replace OTP tokens.

Generally, encryption and decryption techniques along with cryptographic primitives to safely store data. Every operation in the cryptography process requires keys [109]. Nonetheless, these keys must be kept in the memory for usage at any time. A key that is kept in memory can be taken by the enemy in several ways. Thus, in this day of security risks, keeping it in a non-volatile memory is not an option. The promising security primitives that generate keys rather than store them in memory are PUFs. For cryptography purposes, these modules generate the keys through the fabrication process using naturally occurring manufacturing variations.

2.2 Characteristics of PUFs

PUF is a concept used in information security and cryptography that makes use of the natural physical variances in electronic equipment to produce unpredictable and one-of-a-kind digital fingerprints that can be applied to a variety of security applications [21]. PUFs have the following salient features:

- **Randomness:** High levels of irrationality and irregularity should characterize the

PUF response. Without physically gaining access to the target device, this randomization makes it hard for an intruder to predict the response.

- **Uniqueness:** PUFs take advantage of the inherent differences that occur at the microscale in electronic components when they are being manufactured. As a result, every PUF instance generates a distinctive and chaotic response or fingerprint.
- **Unclonability:** It is highly challenging to duplicate or recreate the identical reaction of a PUF in another device because of the manufacturing process' inherent randomness and each device's own physical properties.
- **Challenge-Response Pair (CRP) mechanism:** The PUF is given a specific challenge, and in response, the device produces a response based on its physical features. The response is then utilized as a cryptographic key, token of identification, or authenticity.
- **Tamper Resistance:** PUFs are immune to physical tampering because changing a device's physical characteristics will modify its PUF response.
- **Non-volatile:** PUF replies are frequently extractable and storeable in a non-volatile way, enabling their usage as cryptographic keys or IDs even after power cycles.
- **Low Cost and Resource Consumption:** PUFs don't need additional hardware because they use the physical characteristics that already exist in devices. They have comparatively modest implementation costs in terms of space, power, and computational resources.

2.2.1 PUF quality metrics

The major intention of the PUF design is to produce keys but they need to be evaluated based on the quality metrics that are initiated by the National Institute of Standards and Technology (NIST) [22]. So, the validation of the key is assessed to make the PUF designs reliable. The following quality metrics are considered to evaluate the robustness of the key.

2.2.1.1 Uniformity (u)

It measures how different PUF instances can generate different responses when applying the same challenge. The average inter-chip Hamming Distance (HD) calculated between the obtained responses should be ideally 50%, thereby the performance of the

PUF is measured. Uniformity is the measure of distribution of ‘1s’ and ‘0s’ in the response vector R$_{i,j}$ and is defined as

$$\text{Uniformity [22]} = \frac{1}{n}\sum_{j=1}^{n} R_{i,j} \times 100\% \tag{2.1}$$

where R$_{i,j}$ is the ‘jth’ binary bit of a n-bit response for an ‘ith’ input. An ideal PUF should have equal probabilities for ‘1’ and ‘0’ in response, i.e., 50%.

2.2.1.2 Diffuseness (D)

Diffuseness is the degree of variations observed in the same PUF with different challenges applied nominally and can be measured by calculating the mean of HD from the response vectors. It is defined as

$$\text{Diffuseness [22]} = \frac{2}{l(l-1)} \times \sum_{i=1}^{l-1}\sum_{j=i+1}^{l} \frac{\text{HD}(R_i, R_j)}{\text{n}} \times 100\% \tag{2.2}$$

where ‘l’ represents randomly selected response vectors from CRP space. R$_i$ and R$_j$ are two different n-bit response vectors obtained from two different challenges. Ideally, 50% diffuseness ensures collision-free responses.

2.2.1.3 Uniqueness (U)

The randomness in different PUF responses reflects the performance in terms of uniqueness. Ideally, the probability of each response (i.e., ‘0’ or ‘1’) generated by identical PUFs with the same challenge is 50%. It can be calculated with inter-chip HD as shown below

$$\text{Uniqueness [22]} = \frac{2}{m(m-1)} \times \sum_{i=1}^{m-1}\sum_{j=i+1}^{m} \frac{\text{HD}(R_i, R_j)}{\text{n}} \times 100\% \tag{2.3}$$

where R$_i$ and R$_j$ are two different n-bit response vectors obtained from the same challenge and ‘m’ represents different PUF instances with the same challenge.

2.2.1.4 Reliability (R)

Reliability is measured by Intra-HD, which is performed between two n-bit response vectors generated from the same PUF instances with the same challenges. Ideally, it should be close to 0% for an environment-friendly PUF and its mathematical equation is given below.

$$\text{intra-HD} = \frac{1}{m} \times \sum_{t=1}^{m} \frac{\text{HD}(R_{i,ref}, R_{i,t})}{\text{n}} \times 100\% \tag{2.4}$$

$$\text{Reliability [22]} = 100 - (\text{intra-HD}) \tag{2.5}$$

where ‘m’ represents the number of measured trails applied on PUF instances with the same challenge. $R_{i,ref}$ is the reference response measured at normal operating conditions i.e., 25°C, 1.8V, $R_{i,t}$ is the t^{th} measured response at different operating conditions.

2.3 Types of PUFs

PUFs are available in a variety of forms, each of which is based on a unique set of physical characteristics. To produce distinct and irregular responses, several PUFs take advantage of numerous inherent variances in electronic devices. Some typical PUF kinds are described below:

2.3.1 Delay-based PUFs

Delay-based PUFs take advantage of manufacturing process variance inherited in analog or digital circuits. The foundation of these PUFs is the notion that, as a result of process variances, the delay routes in circuits can have internal differences, resulting in distinctive response patterns. The benefits of delay-based PUFs [23, 24] include their ease of implementation in design and the fact that they may be implemented using common digital logic components. However, they also have drawbacks, such as sensitivity to environmental factors and potential vulnerability to modeling attacks if an intruder has access to comprehensive knowledge about the circuit. The following PUFs categorized under delay-based mechanisms are discussed below.

2.3.1.1 Arbiter PUFs (APUFs)

A basic APUF is shown in Fig.2.2, consisting of Switch Components (SCs) and arbiter blocks to perform the arbitration process and earlier response detection respectively. Input and a random challenge are simultaneously fed to SC, it can produce the delay paths based on the arbitration mechanism forwarded to the arbiter for earlier rising edge detection as the response. The mechanism of delay-based PUF can introduce a race condition between two equally designed delay paths and is won by the faster path. The circuit consists of n-bit input ‘I’ and computes 1-bit response ‘R’ based on the contention between two symmetrical paths based on relative delay difference (Δd = d1−d2). The delay of the input bitstream is determined by the two-path processing of multiplexers (MUXs). Formally, the SCs are designed with 2×1 MUXs and properly tuned to get the

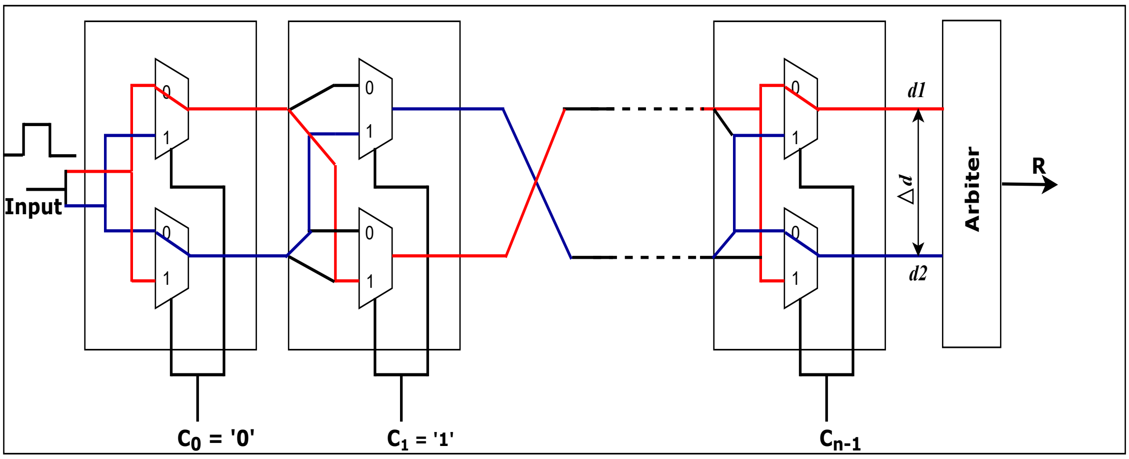


Figure 2.2 Basic APUF

precise delay (d) as a response. The delays are generally considered as PVs in APUFs, such as produced by the placement of a different combination of transistor arrangements in MUXs to produce certain delays at SCs. The MUXs will release the path straight if the selection (challenge) C_i is '0' else crossed when C_i '1'. Likewise, MUX stages act as SCs and can create a pair of delay paths for input 'I'. Output is evaluated for a particular input while a rising signal is a feed to both paths at the same time. The two signals race through the delay paths and the arbiter circuit (generally use D Flip-flop) catches the signal which comes earlier. The arbiter determines which rising edge arrives first and sets its output to '0' or '1' depending on the winner. For example, if a 16-bit input is given with a predefined challenge, an output is produced as '1' if path1 arrives early else produce '0' for path2.

APUF [12–21] is the conventional delay-based approach realized between two symmetrical engaged paths that provide efficient CRP space for device identification and authentication. In APUF-based device identification or authentication, setup time problems are raised between racing paths can be improved by the design of a new arbiter. A candidate hardware random number generator [14] using arbiter PUF as a replacement for pseudo-random number generators. To ensure the security and robustness of keys a new PUF methodology lightweight secure keys [24] was proposed with the integration of key principles. Toward an ideal APUF design, a bias-free Programmable Delay Line (PDL) [25, 26] is implemented on a Field Programmable Gate Array (FPGA) to achieve the structural regularity of APUF. The double APUFs (DAPUFs) [27, 28] provide comprehensive risk analysis and performance evaluation to make APUFs strong against machine learning attacks. Moreover, An XOR-based Reconfigurable Bistable Ring (XRBR) PUF [29,30] was proposed with a significant advantage in terms of hardware cost. A novel lightweight Flip-Flop Arbiter (FFA)PUF [31] is presented to overcome the degraded reliability bottleneck in the security implementation. The Bus keeper [32] also known as bus holder is a latch-based PUF that has no control signals and is probably an alternative for DFF PUFs. A compact architecture Flip-Flop (FF)-APUF, designed to achieve decent reliability properties, is presented in [31–33] to offer more resistance for security.

2.3.1.2 Ring Oscillator PUFs (ROPUFs)

Ring-Oscillator (RO) PUF [34], a delay-based architecture, produces responses from frequency differences acquired among a group of identical ring oscillators arranged in a designed pattern as shown in Fig.2.3. RO PUFs [35] are most popular due to their security, simplicity, ease of implementation, and evaluation. However, the main disadvantage of RO PUFs is poor response generation when temperature and supply voltage variations take place [36]. It cannot be stable to generate strong CRP concerning environmental condition variations [37]. Therefore, the reliability is enhanced by selecting a strong RO pair from '1' out of n-RO pairs, which has the maximum frequency distance from n-pairs. In multi-level supply voltage powered RO PUF was proposed to select the highest reliable voltage configuration [38]. The provision of feedback-based supply voltage control can improve the reliability better than the conventional RO PUFs [37].

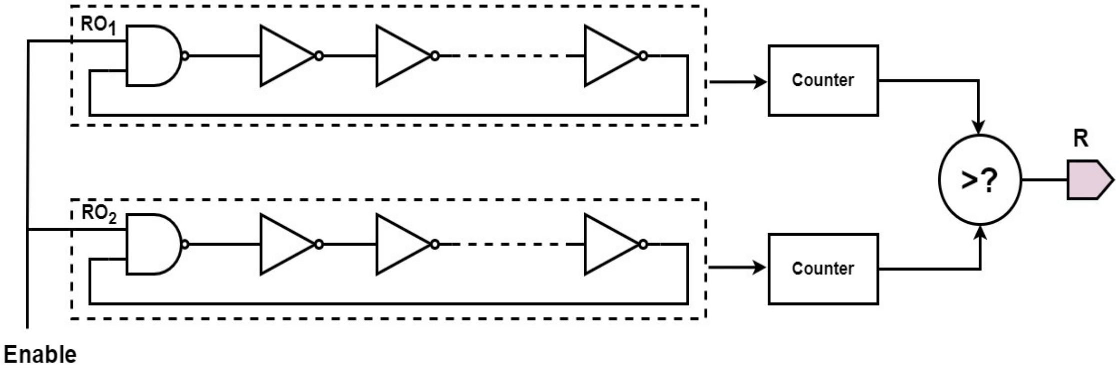


Figure 2.3 Ring Oscillator PUF [32]

A temperature-aware RO PUF with different RO pairs cooperation can generate reliable bits against temperature variations [39, 40]. The temperature sensitivity is the major drawback in RO PUFs and can be reduced by applying a negative temperature coefficient [41] of resistance to the inverters with two source feedback resistors. However, to achieve high reliability, a lightweight hybrid RO PUF was proposed with high thermal stability against supply voltage variation [42]. The devices are more authenticated when the system is designed with machine learning [43] based schemes for IoT edge node security. The inverters in the RO PUF are replaced with a configurable delay unit, composed of a tri-state matrix, and a Tri-state Configurable Ring Oscillator (TCRO) [44] that enhances the flexibility and entropy. Compared to RO PUF, APUF produces a stronger CRP set due to its complex arbitration mechanism. However, the responses can be predicted from machine learning (with training and testing) approaches as the path delay is linearly dependent on challenges. Even though RO PUF offers numerous CRPs, it requires more area, power and time.

2.3.1.3 Other delay-based PUFs

- **Butterfly or Clock PUFs:** Butterfly or Clock PUF [45] shown in Fig.2.4 is a special kind of PUF that makes use of the difference in propagation delays between two pathways in a digital circuit. A unique response depending on the relative time of signals is frequently produced using this delay difference, often taking the form of a butterfly or behaving like a clock.

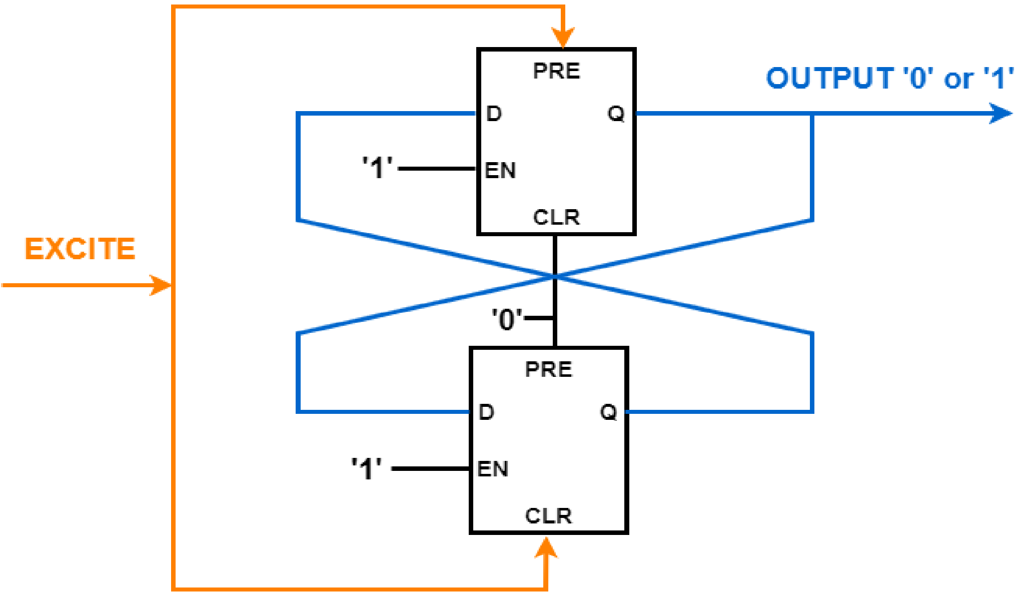


Figure 2.4 Butterfly or clock PUF [45]

- **Rotating Ring PUF (RRPUF):** It is a delay-based PUF that produces distinctive and chaotic replies by using the idea of ROs [46] provided in Fig.2.5. To produce unique challenge-response pairs, this sort of PUF takes advantage of the inherent process changes in delay paths. Although it is easy to implement in hardware, environmental fluctuations and calibration issues must be addressed to ensure its usefulness in security applications.

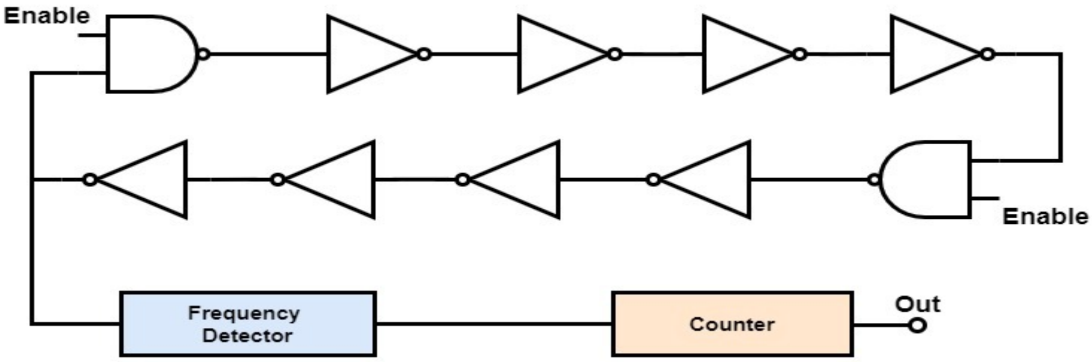


Figure 2.5 Rotating Ring PUF [46]

2.3.2 Memory-based PUFs

Along with delay-based mechanisms, researchers have also proposed memory-based PUFs [47–50] based on minute unbalances with cross-coupled structures. In these memory-based PUFs, SRAM PUFs [47], DRAM PUFs [49], FF-based PUFs [33] and Flash PUFs [50] provide a limited number of CRP pairs with low entropy and high density in many cases; consequently, they become weak. In [30], the design of a new memory-based combination PUF tightly integrates (two) heterogeneous memory technologies to address challenges/shortcomings. An SRAM-based countermeasure [48] against IC recycling was proposed to detect the ageing of SRAM cells. The SRAM cells are stable over time and are sensitive to ageing. Analog IC-level components are generally expensive, so circuits like tri-state flip-flop PUF [51] contribute less area and power to the system. However, they are reliable and tamper-resistant for many applications. Once the chip is manufactured, the signature key generated by the designed PUF is fixed and obtained CRP pairs can be deduced by knowing only one CRP combination.

2.3.2.1 Static Random-Access Memory (SRAM) PUF

It uses the intrinsic variability of SRAM [47] cells to produce unpredictable and distinctive identities for electrical devices shown in Fig.2.6. A dynamic highly reliable SRAM-based PUF [49] to obtain the mismatch of NMOSs is extracted during discharge process when biased in sub-threshold region can improve the stability and reliability of the responses. These identities can make ICs and other hardware parts more secure. Due to flaws in the manufacturing process, SRAM cells have minor electrical property changes. Due to these changes, individual SRAM cells behave differently, which can affect things like how quickly data is read and written. Even though these differences are often slight, each SRAM cell experiences them consistently and differently. So, SRAM cells use built-in variances to create arbitrary and unpredictable identities or cryptographic keys. They add a layer of defence against numerous attacks and efforts at fraud.

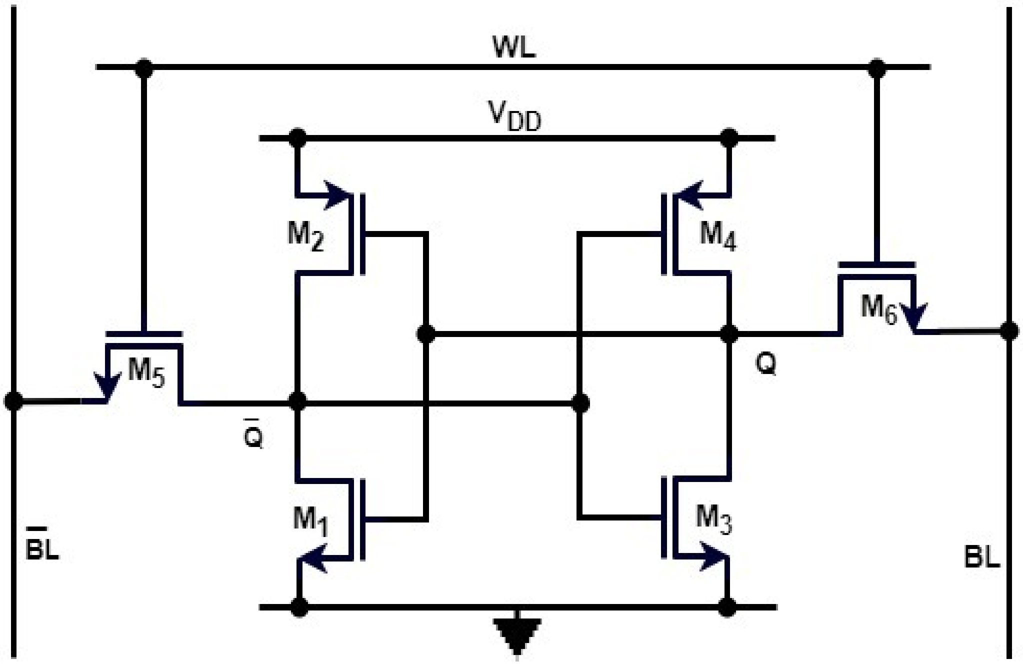


Figure 2.6 SRAM PUF [47]

2.3.2.2 Dynamic Random Access Memory (DRAM) PUF

DRAM PUF [49] makes use of the minute manufacturing variances in memory cells to produce unpredictable and unique IDs for devices as shown in Fig.2.7. The usage of these identifiers can improve cryptographic and hardware security. DRAM cells display minor manufacturing variances because of flaws in the manufacturing process, just like

SRAM cells. Among individual DRAM cells, these changes may result in disparities in electrical activity, such as retention duration and refresh behaviour.

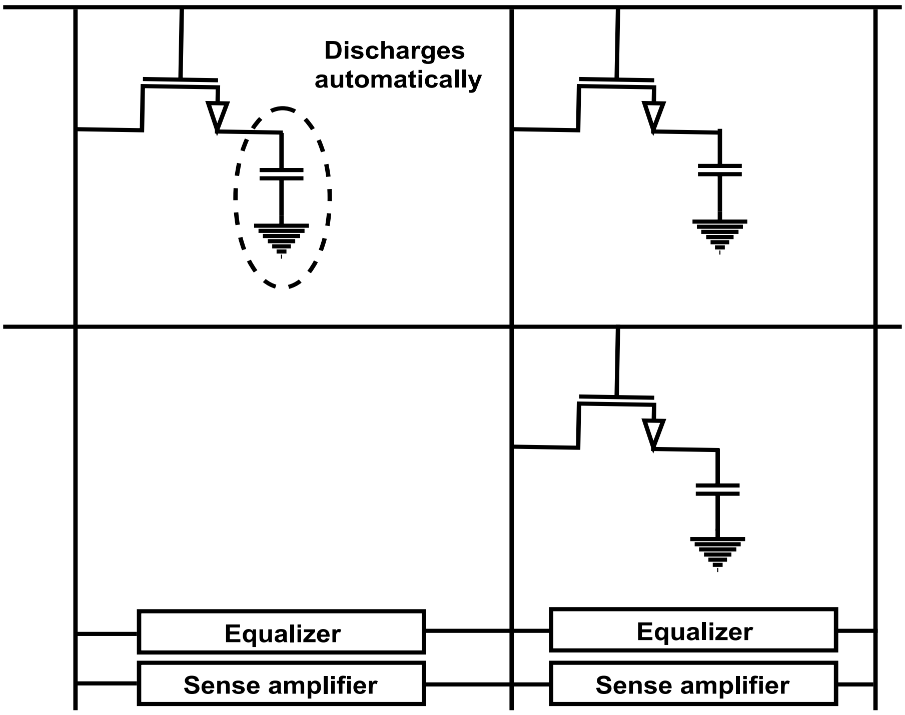


Figure 2.7 DRAM PUF [49]

2.3.2.3 Other Memory-based PUFs

- **Flash memory based PUF** Flash memories [50] shown in Fig.2.8 have the control gate and transistor channel electrically insulated from the floating gate by blocking oxide and tunnel oxide. The electrons deposited on a floating gate are trapped without a power source, and the floating gate can retain information in the form of charges (electrons) for a long time. Each flash cell has a varied oxide thickness, threshold voltage, oxide layer flaws, etc. due to process variance that are utilized to produce responses.

2.3.3 Mixed-signal PUFs

Mixed-signal PUFs create distinct challenge-response pairs by taking advantage of the inherent variances in a circuit's analog and digital components. These differences can include both digital and analog characteristics, such as gate delays and transistor threshold voltages. Analog IC level components are generally expensive, so circuits like tri-state flip-flop PUF [52] contributed less area and power to the system. However, they

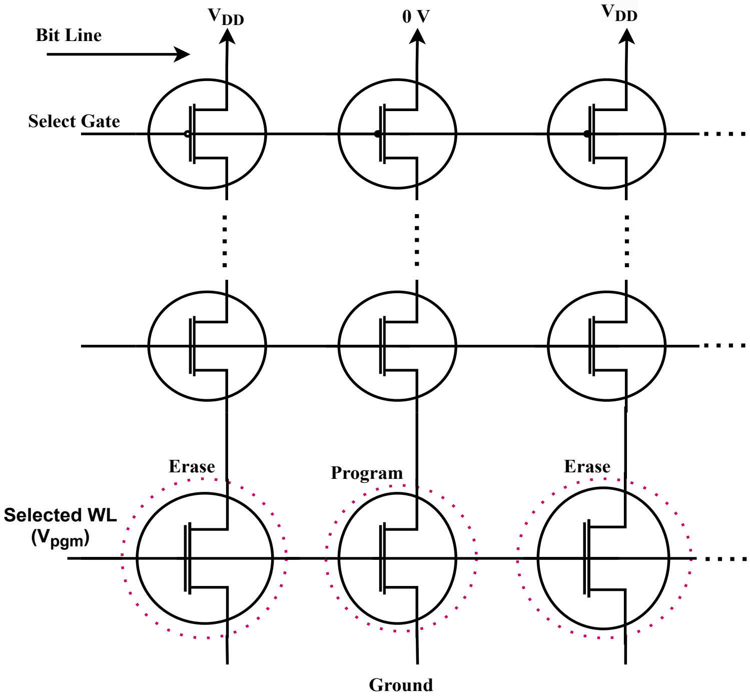


Figure 2.8 Flash PUF [50]

are reliable and tamper-resistant for many applications. Once the chip is manufactured, the signature key generated by the designed PUF is fixed and obtained CRPs can be deduced by knowing only one CRP combination.

In addition, Multiple-Valued Logic (MVL) [53] comparators are proposed based on device mismatches in either current mode or voltage mode to achieve energy efficiency. The Analog and Mixed Signal (AMS) circuits intentionally suffer from the effects of process variations, which impede the operation of the circuit due to trojan insertion. The ”logic locking” proposed in [53] can guarantee the security of the circuits. In the design of nano-scale PUF circuits Resistive Random Access Memory (RRAMs) [54] are proposed to achieve non-volatility, more resistive, and easy integration in CMOS.

2.3.3.1 Temperature stable PUF

The proposed PUF bit-cell circuit shown in Fig.2.9 only uses transient current, which increases in direct proportion to the clock rate. The transistors are biased in the sub-threshold region to maximize the local mismatch and, consequently, the PUF’s dependability. Such a PUF design can be thought of as naturally immune to modeling attacks because it doesn’t require any kind of challenge to get results. Hardly, low power consumption is feasibility explored in sub-threshold APUFs [55–57] to optimize the PUF supply voltage for the minimum power-delay product achieved small area occupancy and high reliability. Based on temperature stability, an ultra-low-power PUF [55] and current comparator PUF [58] are implemented in 65nm CMOS over the commercial temperature ranges resulting in the most energy-efficient and unpredictability verified by passing the NIST [22] randomness test.

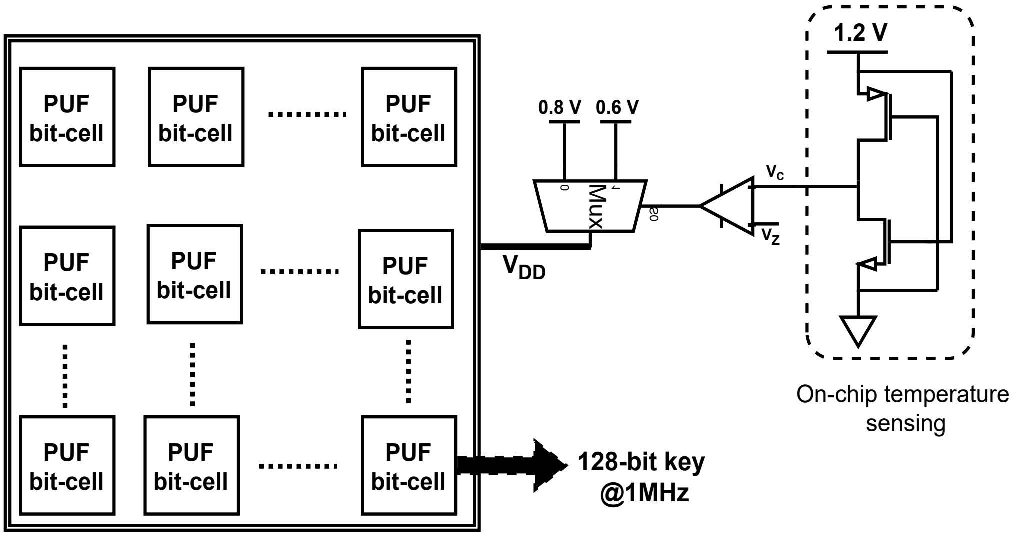


Figure 2.9 Temperature stable PUF [55]

2.3.3.2 Current Mirror Array (CMA) PUF

The fluctuation in mirrored currents brought on by transistors employed as current mirrors having different sizes. The CMA PUF [59] shown in Fig.2.10 makes use of a variety of current mirror circuits, which are simple analog circuits that reflect the current passing from one transistor to another transistor to produce unpredictable responses. This kind of PUF uses various challenge-response pairings by making use of the inherent process variability in electronic equipment.

2.3.3.3 Schmitt Trigger (ST) PUF

When ported to advanced technologies with lower supply voltage, existing PUF designs face a significant challenging circumstance. Furthermore, in various kinds of ultra-low-power IoT applications, the supply voltage provided by the battery or other energy sources can be heavily influenced by the battery's lifetime or environmental factors (e.g., solar radiation, vibration), which has stringent requirements for the PUF's reliability. Consequently, to improve the robustness of the circuits the STs [60, 61] shown in Fig.2.11

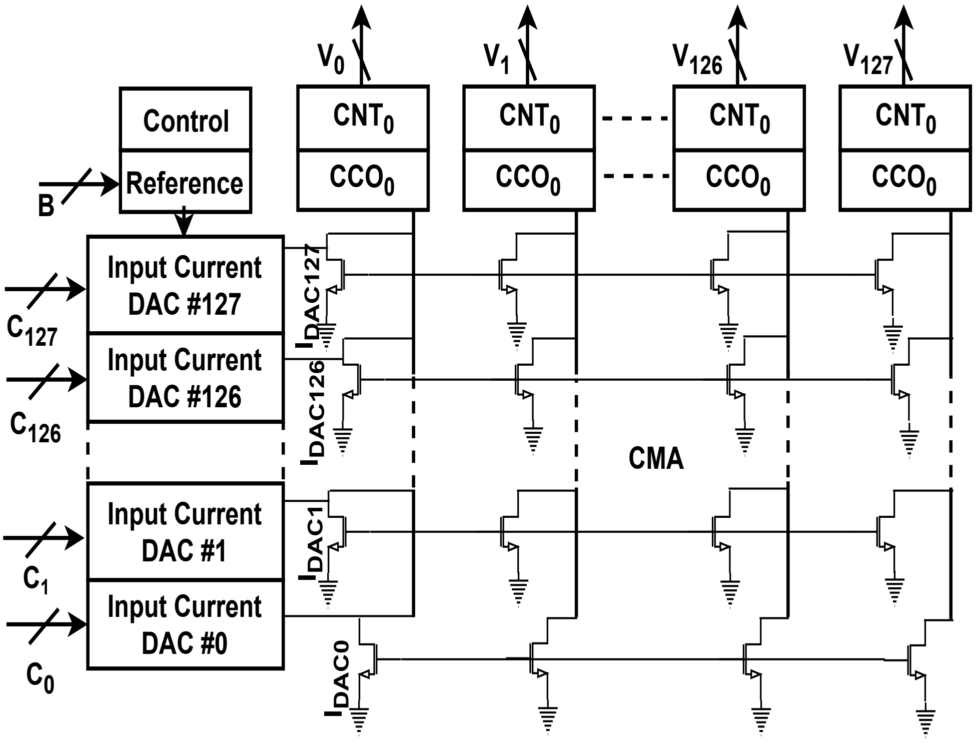


Figure 2.10 Current Mirror Array PUF [59]

are proposed to introduce variations in terms of noise immunity i.e., raise the static noise margin of the circuits but at the cost of increased power consumption and delay. The ST is a bi-stable circuit that acclaims popularity by its hysteresis characteristic to work in two different threshold levels (V$_L$ and V$_H$). Indeed, the ST [62, 63] is a restoring signal circuit that removes noise from the input signal and retrieves the original input signal information. Particularly, in identification or authentication applications, the hysteresis of an ST is presumed as PV and obtains the respective CRPs for key generation [64].

2.3.3.4 Power management circuit based PUFs

Power Management Unit (PMU) is the crucial building block for all electronic systems. It would not be possible to make modern electronics like smartphones, computers, and many other things without PMUs. Generally, a source of Direct Current (DC) or battery can be converted from one voltage level to another using an electronic circuit or device known as a DC-DC converter. It uses a switch (usually a MOSFET) that is rapidly turned on and off, transferring energy to an inductor and/or capacitor, which then smoothes out the voltage to the desired level. This can be in the form of step-down

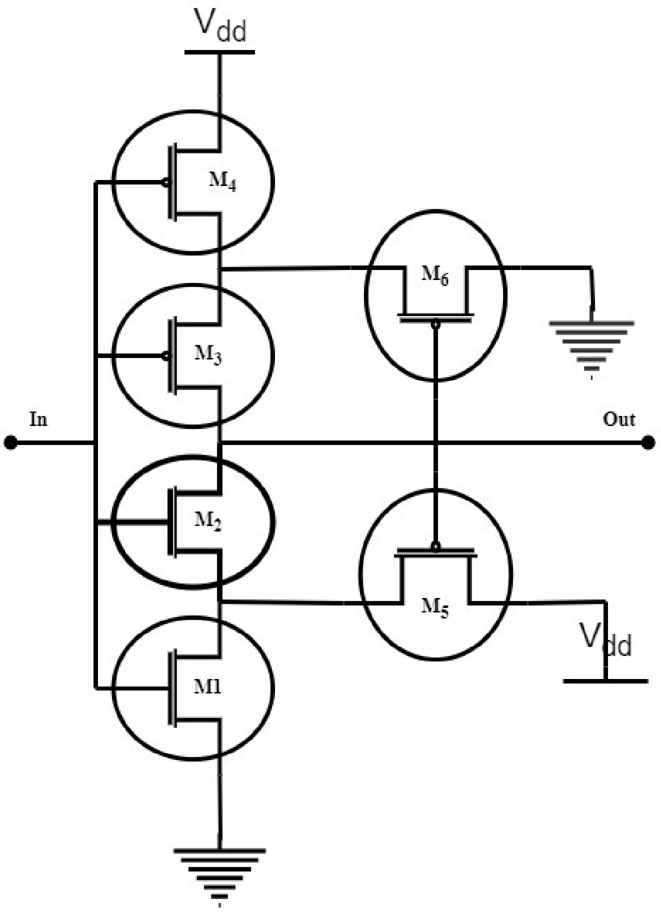


Figure 2.11 Schmitt Trigger PUF [60]

(buck), step-up (boost), or other topologies like buck-boost. The switching regulators used in DC-DC converters can generate noise and ripple on their output, which might be problematic for certain applications unless additional filtering is applied.

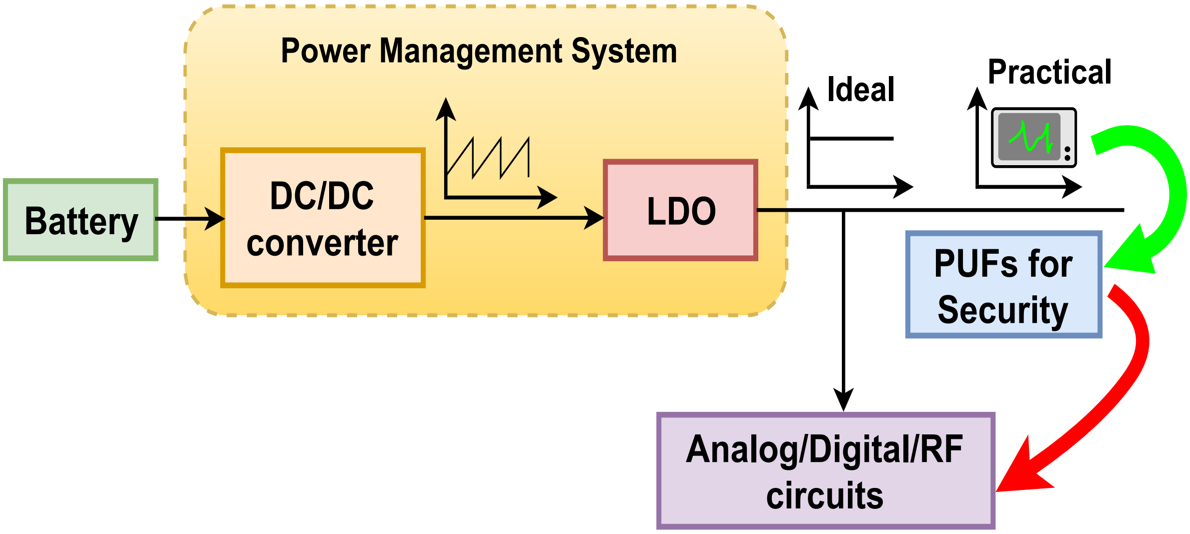


Figure 2.12 Power management system for PUFs

Low Dropout Regulator (LDO) is a linear voltage regulator that operates by using a pass transistor to drop the excess voltage from the input to achieve the desired output voltage. The difference between the input and output voltage is called the dropout voltage. LDOs tend to have lower output noise and ripple since it does not operate by switching like DC-DC converters. Both LDOs and DC-DC converters are used to provide stable output voltages from varying input voltages. The PMU shown in Fig.2.12 is not only suitable to drive analog, digital and RF circuits but also used for security applications. In addition, the LDO is used as a challenge generator to feed PUFs using power traces that are discussed in Chapter 7.

2.3.3.5 Other Mixed-signal PUFs

- **Current Starved Inverter (CSI) PUF:** Inverter pairs are used in the CSI PUF [65] as shown in Fig.2.13, with a reference transistor driving one inverter while a current-starved transistor drives the other. The PUF is based on the variances in propagation delays between these inverters caused by the processes.

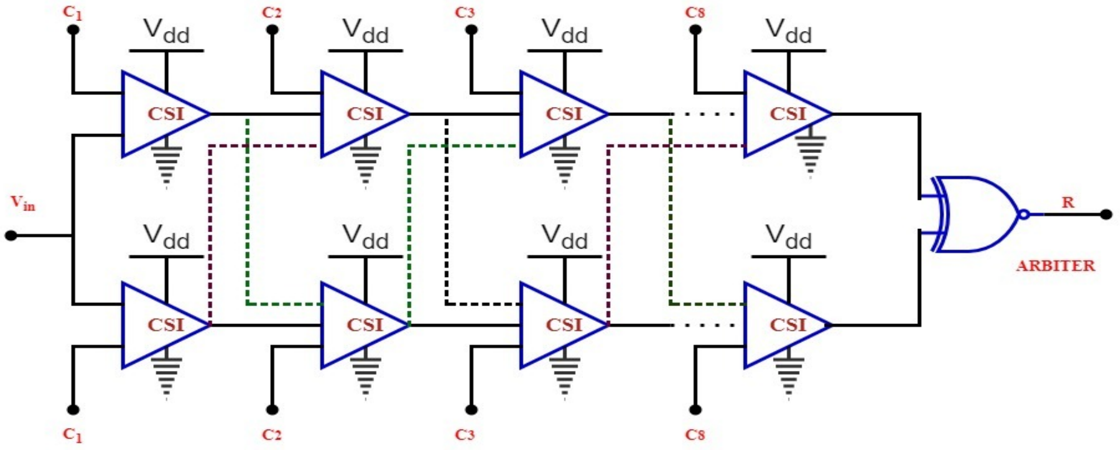


Figure 2.13 Current Starved Inverter PUF [65]

- **Comparator PUF:** A contemporary comparator [57] with the misalignment of the transistors produces the digital output is shown in Fig.2.14.

The switching behaviour of the transistors is impacted by these variations, which lead to differences in characteristics like threshold voltage. A cross-coupled structure with high gain is used to amplify the process variation and stabilize the comparator quickly, improving the structure's reliability significantly without adding any more power-hungry

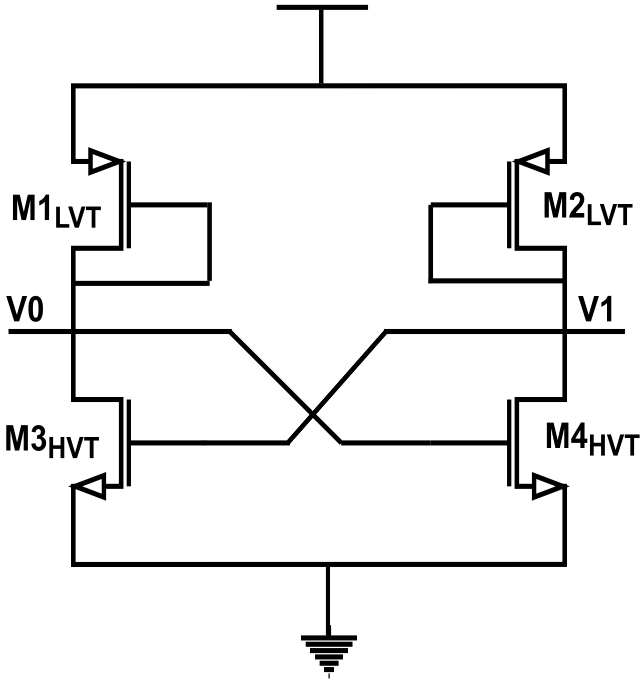


Figure 2.14 Comparator PUF [57]

digital modules. The Proportional To Absolute Temperature (PTAT) characteristic, when combined with positive feedback mechanisms, significantly reduces the temperature perturbations.

2.3.4 Strong and Weak PUFs

Transistors experience severe leakage when scaling beyond CMOS technology. The introduction of high−k dielectric materials was necessary since conventional dielectric materials were not adequate. The scaling issue was unsolvable at sizes larger than 32 nm, even with the high−k materials. The effective length of the channel of a FinFET is double the fin's height because the source and drain are projected into the third dimension which results in low-channel effects. However, FinFETs suffer from a substantial leakage leading to huge PVs impacting the circuit. Moreover, some of the drawbacks observed in junction-less FETs such as low on-state current, high parasitic capacitance (caused by increased doping), poor switch-off capability, and greater gate work function [110].

These issues are addressed by dopingless FETs that address higher band-to-band tunnelling and random dopant fluctuations (RDF) by forming the drain and source with a thin intrinsic silicon nano-wire rather than a strongly doped drain, channel, and source [110]. The device is more scalable and has lower leakage currents because of its DLFET construction. Two hybrid oscillator arbiter PUF designs, one using DLFETs for power optimization and the other for speed optimization are presented to demonstrate how these DLFETs can reduce power [110].

The strong PUFs are generally posed by an exponential number of challenges that create a large number of CRPs that are useful for key generation, storage, and authentication procedures. Whereas, weak PUFs have a finite challenge space and can only be used to generate and store keys for unique ID applications.

2.3.4.1 Strong PUFs

Strong PUFs [66–68] are a category of PUFs that offer a large selection of CRPs. Typically, there is a vast space of CRPs, making it impossible for an attacker to query and record every single one of them while the PUF is active. Strong PUFs present a wide range of possible challenges, and each task will have a different outcome depending on the intrinsic and arbitrary physical characteristics of the PUF [69]. Additionally, strong PUFs don't rely on persistent memory or secret storage. When a challenge is posed, the responses are created instantly depending on the physical properties of the device. Generally, the APUF shown in Fig.2.15 is recommended as a strong PUF due to the uncertainty attained in the arbitration mechanism performed between two identical delay paths [68]. A novel design of a strong PUF, resistive X-point array [66] PUF was proposed that enhances the entropy of the physical system; thereby increasing the space of CRP pairs. Furthermore, high robustness based on the intrinsic random micro or nanostructures of the electronic packages [67] is proposed thereby demonstrating a low-cost and label-free hardware security solution for IoT.

Utilization of intrinsic path delay [67] through Time-to Digital Converter (TDC) can increase the number of responses effectively and provide an extra level of unpredictability against model-based machine learning attacks [70, 71]. In the same way, A novel inter-connect PUF [71] utilizes the variability of interconnect lines for generating PUF signatures while exhibiting good reliability and robustness against various attacks. The classical ML attacks presented in [72] are vulnerable to exploiting the stability of single CRPs. These are managed through Interpose-PUF (iPUF) which is considered a standard primitive for the replacement of XoR PUF. Likewise, the effectiveness of APUFs is boosted in [73] against ML algorithms that are used to attack the PUF design. Moreover,

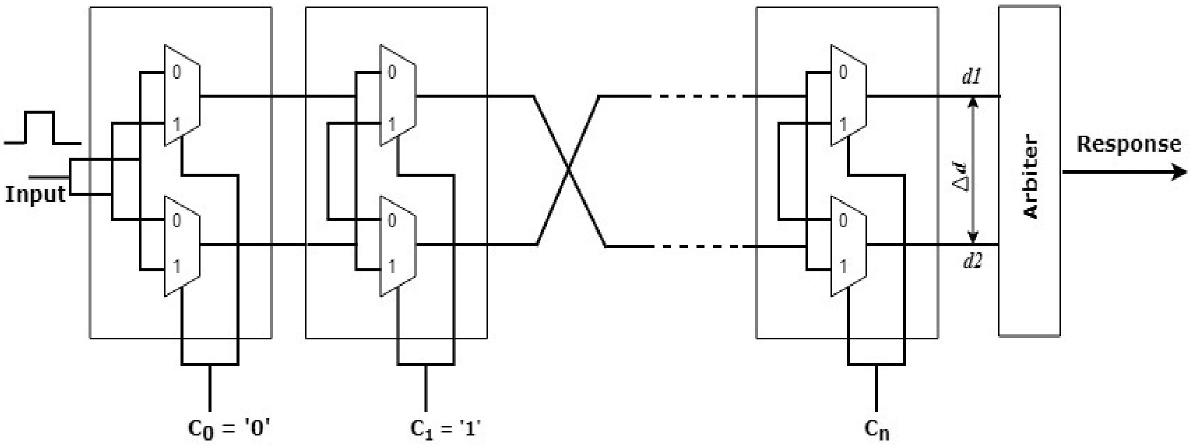


Figure 2.15 Strong PUF design

a lightweight resistant ML-based Controlled (MC-PUF) [74] generates CRPs on the fly to avoid storing limitations faced by the other PUFs. A memory-based architecture 3-XoR Mc-PUF [75] illustrated the resilience against ML attacks with the best randomness and uniqueness.

Strong PUFs are vulnerable to modeling attacks which is a major concern in the security of an IC. The attackers may gather a portion of CRPs to create a prediction model of the PUF (typically using ML methods), as they can be queried with a variety of challenges. When a reliable model is created, it may be applied to anticipate responses to given trials, essentially copying the PUF's action.

2.3.4.2 Weak PUFs

Generally, strong PUFs strive to provide a large CRP space that is difficult for attackers to thoroughly enumerate, whereas Weak PUFs only produce a smaller subset of replies. Weak PUFs as shown in Fig.2.16 continue to depend on the inherent diversity in physical qualities during the manufacturing process. However, it's possible that this variation isn't as well-tuned as Strong PUFs. Despite their drawbacks, weak PUFs can be helpful in device identification applications.

With the reach of smart electronics and their expanding global market, cybersecurity is becoming a significant concern. Building security and privacy-enabled primitives into an electronic system during its design phase is the goal of the Security-by-Design (SbD) philosophy, a developing field in cybersecurity. This work offers a novel Trusted Platform Module (TPM) for SbD primitive that is based on PUF. The encrypted and decryption

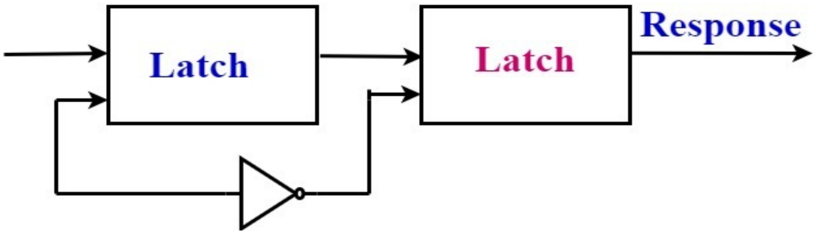


Figure 2.16 Weak PUF design

engine of TPM is used by the proposed SbD primitive to securely verify the PUF key [111]. All commercial PCs, laptops, and computer systems now come with TPM, a secure cryptoprocessor. Prominent features of TPM include cryptographic key storage, RSA and AES-based encryption, decryption, and verifying the integrity of a remote smart electronic system. Future research could include expanding the aforementioned security protocol to include other areas of smart electronics and enhancing the energy efficiency of the IoT by implementing low-overhead PUF-based solutions.

2.4 Attacks on PUFs

PUFs are special cryptographic primitives that get their purpose from the physical flaws and unpredictable nature of hardware architecture. PUFs are possible targets for numerous attacks due to the security applications they are used for, such as hardware authentication, key generation, and anti-counterfeiting. Depending on the type of attack, these can be divided into many groups and are discussed in the following sections.

2.4.1 Invasive attacks

The purpose of PUFs is to provide unique cryptographic keys for devices by making use of the physical changes that occur randomly in hardware [76]. It is impossible to replicate or clone a particular PUF instance since these variances are the product of uncontrollable and unpredictable manufacturing PVs. Micro-probing workstations are the key piece of equipment for invasive attacks.

2.4.1.1 Semi-invasive attacks

Semi-invasive attacks [76] necessitate chip depackaging to gain access to its surface, just like invasive attacks. Depassivation or making connections to the internal lines is not necessary for semi-invasive procedures, therefore the chip's passivation layer is left intact.

This is because this procedure does not involve microprobing, which eliminates the need for expensive tools like laser cutters and Focused Ion Beams (FIBs).

2.4.2 Non-invasive attacks

Physically altering or penetrating the hardware is not necessary for non-invasive attacks [77]. Instead, they exploit the PUF's visible behaviour or the environment around it to get important information or undermine the security that the PUF offers. When deploying PUFs, it's crucial to take a multi-layered security approach, taking into account both invasive and non-invasive potential attack methods. The supply voltage and clock signal manipulation are two of the most popular non-invasive attacks.

2.4.2.1 Modeling attacks

The aim of modeling attacks [78, 79] on PUFs is shown in Fig.2.17 to imitate a real PUF's behaviour without actually possessing or copying it. The attacker tries to use observations to create a model of prediction of the PUF that can be applied to challenges to get the identical responses as the original PUF. An attacker initially collects a set of CRPs from the real PUF in a modeling attack. Then, a predictive model is trained using this dataset. Once the model is sufficiently precise, it can forecast how the real PUF will react to fresh challenges. Effective Machine Learning (ML) techniques like Linear Regression (LR), Random Forest (RF), Support Vector Machine (SVM) and Neural Networks (NN) are especially well-suited to perform prediction. However, an attacker can create a model that behaves like the PUF by feeding the collected CRPs into ML techniques [80]. Modeling attacks like LR try to derive a mathematical model

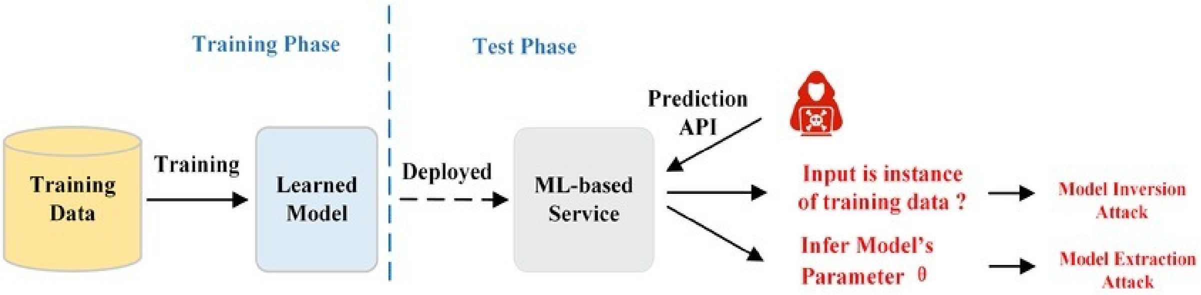


Figure 2.17 Modeling attacks [78]

from the generated PUF data, i.e., a computer algorithm that correctly predicts the PUF responses with high probability when feeding respective challenges. LR-based ML methods may be used to attack XoR PUFs, Feed-Forward PUFs, and Lightweight PUFs. However, their findings revealed that as the number of XoRs increases, the number of CRPs necessary to represent randomness exponentially. As a result, researchers observed that XoR PUFs may resist these ML threats if enough XoRs are used. ML attacks have received comparatively little attention in comparison to the number of studies that either suggest novel PUFs or assess their performance concerning reliability and uniqueness presented in [81].

Based on the FF-PUF and iPUF mechanisms [32] [72], a novel LP-PUF [80] was suggested to alleviate the ML attacks on XoR APUFs. LP-PUF employs a scheme where the attacker cannot compute the first or last operation in the cipher layer. Precisely, in the authentication process of the IoT devices, the enrollment PUF architectures [81] are preferred to overcome the reliability-based strategies against ML models that intentionally exploit the PUF behavior. However, the earlier studies mainly focused on simulated data, but they were affirmed and uncertain using data from an Application-Specific Integrated Circuit (ASIC).

2.4.2.2 Side-channel attacks

Side-channel attacks [82] make use of information that physical systems unintentionally leak while they are in use. For instance, ICs need energy and time to do the tasks that are given to them. Additionally, they produce some noise, release heat, and emit an electromagnetic field. In fact, there are a lot of information sources that are leaking from genuine computers that may be used by fraudulent adversaries. In the context of PUFs, side-channel attacks seek to infer the internal behavior or reactions of the PUF based on these observed leakages, without directly challenging the PUF. The process of side-channel attacks is represented in Fig.2.18. In order to defend against these attacks, a mixture of hardware and software techniques, tamper detection and response mechanisms, error correction, cryptographic post-processing, secure protocols, and constant monitoring and validation of the PUF's behaviour may enhance the resistance of the ICs.

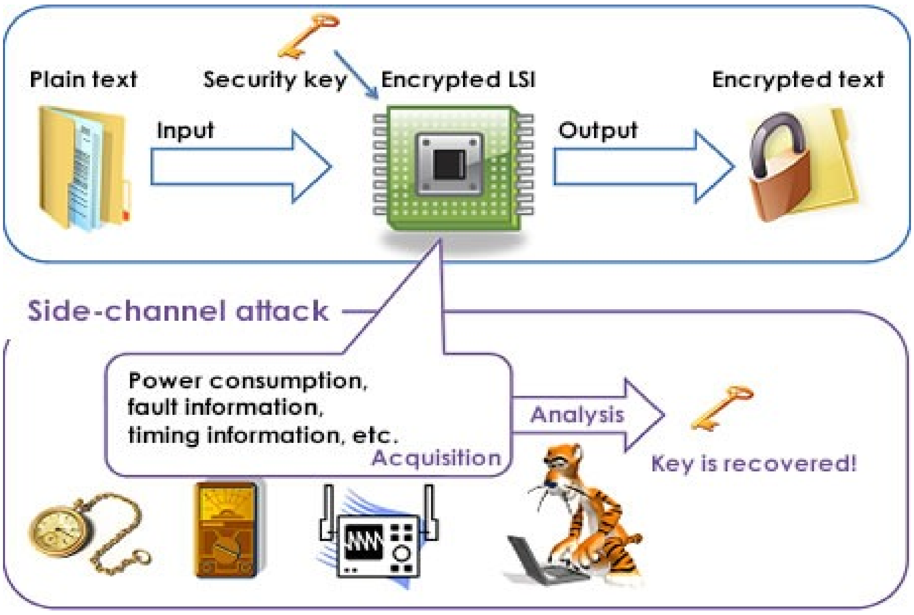


Figure 2.18 Side channel attack protection [82]

2.5 Summary

This chapter discussed how a typical PUF implementation creates its random bits by considering inherent PVs obtained among apparently identical circuits in the PUF core. Moreover, this chapter has described the most cutting-edge PUF approaches and architectures available in the literature to improve the quality matrices of the IoT PUF designs. We provided a simplified illustration to show the characteristics of PUF that impact the security metrics of a PUF. We then discussed different mixed-signal PUF designs and implementation through a feed-forward mechanism applied to APUFs that increases their resistance against ML attacks. Numerous studies that analyze the security and/or VLSI metrics of a single PUF core implementation may be found in the literature. Based on the findings of this research, a comparison of different PUF implementations initiates PVs with respect to the design and technology that are employed to challenge the ability and defend themselves from ML attacks.

In the next chapter, the design and implementation of XFAPUF based on the XoR feed-forward challenge mechanism is introduced and also compared with different PUF designs that are examined by PUF evaluation metrics.

Chapter 3

XoR Feed Arbiter PUF (XFAPUF)

The design of strong PUFs introduces intricacy in the circuit and also leads to security enhancement in a hostile environment. This chapter proposes a strong PUF design by exploiting the feed forwarder mechanism in arbiter PUF [12]. The main objective of this approach is to introduce non-linearity in the arbitration process. Nevertheless, a small number of feeding challenges and complexity are obtained through XoR feed for unique ID generation. So, it is very difficult for an intruder to get the key from the proposed PUF. In APUF, SCs have to be fed by an n-bit challenge whenever an attempt is made to generate a new response (key). Whereas the proposed method has the advantage of generating automated challenges, thereby generating strong CRPs. Hence, complexity becomes a bit more due to the positioning of the XoR gate in between the SCs.

In this chapter, we propose a feed-forward arbitration scheme for arbiter-based PUFs to improve the randomness of the PUFs with sophisticated feed structures. An arbiter-based scheme generates digital information from the PUF responses through the absolute delay values of two identical delay paths and evaluates the identification capability, authenticity, and security. The proposed architecture improves the reliability of arbiter-based PUFs against various malicious attacks by adding impulsive non-linearity. The major contributions of this chapter are,

- Basic APUF design is implemented and the PUF responses are examined with PUF evaluation metrics which help to analyze the performance of the APUF.
- An XFAPUF, which is less prone to attacks is proposed to achieve high reliability for key generation in security devices and is presented to attain non-linearity in the arbitration process with a feed-forward mechanism.
- Feed with a small number of challenges in the arbitration scheme using XoR feeding

at every Feed Forward Stage (FFS) stage of arbiter. Thus, the complexity, which is attained in the arbitration process, makes XFAPUF more resistant to attacks.

- Evaluated the simulation results with PUF metrics (e.g., Uniqueness, Uniformity, Reliability, and so on) and showed that the proposed one has less Bit-Error-Rate (BER) compared to the existing APUFs.
- The proposed design has a significant advantage in the arbitration process and produces reliable key generation against manufacturing PVs. Moreover, it offers better uniqueness and reliability than prior works as it achieves promising results, such as uniqueness of 50.03%, diffuseness of 49.52%, and worst-case reliability of 99.81% that ranges from 10°C to 80°C, with 10% fluctuations in supply voltage.

With the intention of a strong PUF design, an XFAPUF is implemented and evaluated by considering the basic APUF structure along with the complex switching mechanism described in the following sections.

3.1 Arbiter PUF

The basic idea of PUF [5–16] involves PVs in the circuits that can produce unpredictable responses, those that are unclonable. Basic arbiter PUF shown in Fig.3.1, consists of SCs and arbiter blocks to perform the arbitration process and earlier response detection respectively. Input and a random challenge are simultaneously fed to SC, it can produce the delay paths based on the arbitration mechanism forwarded to the arbiter for earlier rising edge detection as a response. Fig.3.2 illustrates the mechanism of delay-based PUF can introduce a race condition between two equally designed delay paths and decide the faster one. The circuit consists of n-bit input ‘I’ and computes 1-bit

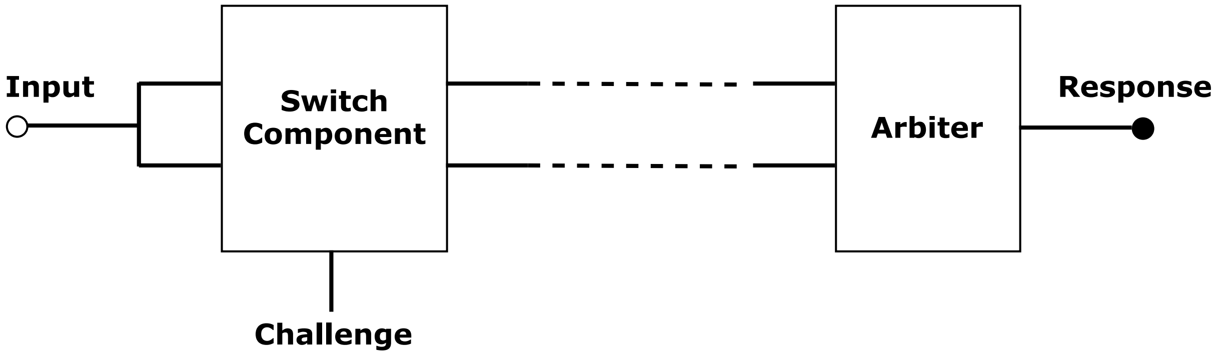


Figure 3.1 Basic Arbiter PUF

response ‘R’ based on the contention between two symmetrical paths based on relative delay difference (Δd = d1−d2). The delay of the input bit stream is determined by the two-path processing of multiplexers (MUXs). Formally, the SCs are designed with 2×1 MUXs and properly tuned to get the precise delay (d) as a response. The delays are generally considered as PVs in APUFs, such as produced by the placement of a different combination of transistor arrangements in MUXs to produce certain delays at SCs. The MUXs will release the path straight if the selection (challenge) C_i is ‘0’ else crossed when C_i ‘1’. Likewise, MUX stages act as SCs and can create a pair of delay paths for input ‘I’. Output is evaluated for a particular input while a rising signal is fed to both paths at the same time. The two signals race through the delay paths and the arbiter circuit (generally used as D Flip-flop) catches the signal which comes earlier. The arbiter determines which rising edge arrives first and sets its output to ‘0’ or ‘1’ depending on the winner. For example, if a 16-bit input is given with a pre-defined challenge, an output is produced as ‘1’ if path1 has arrived early else produces ‘0’ for path2.

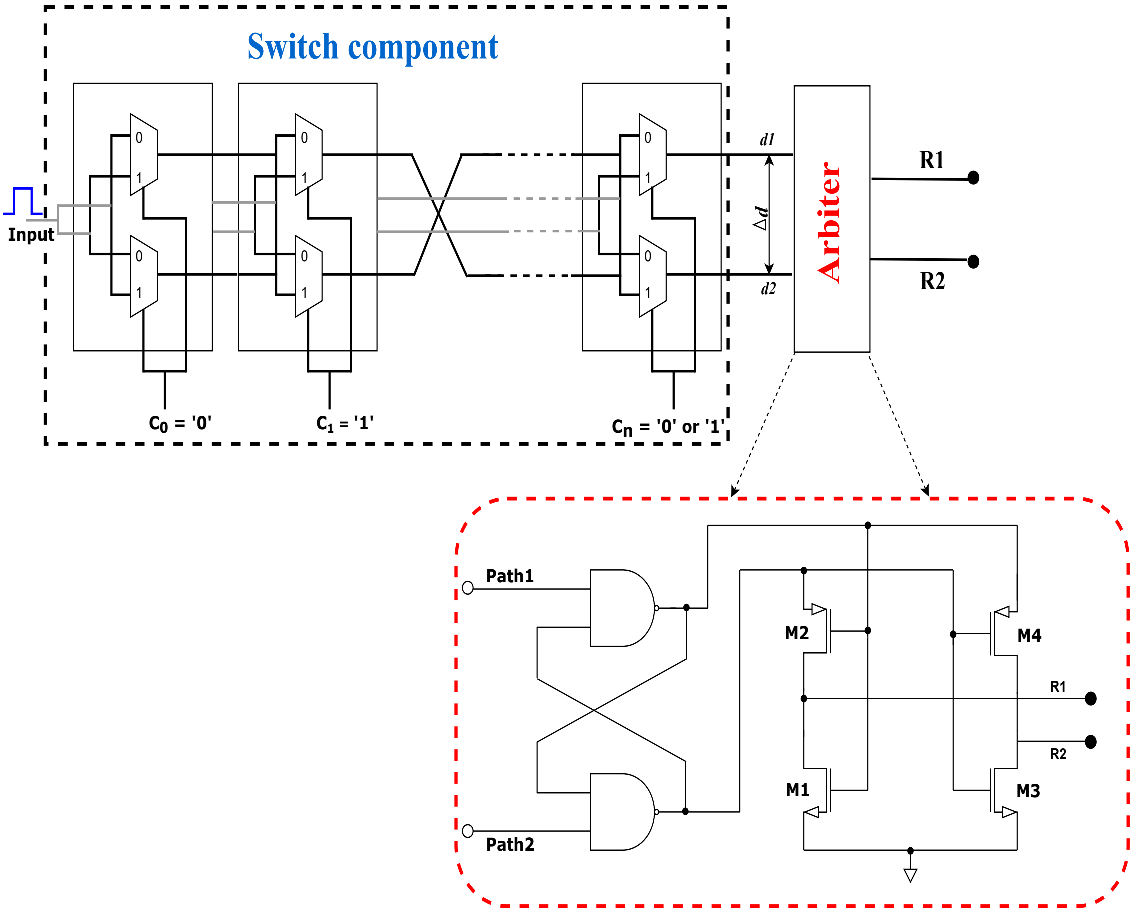


Figure 3.2 Arbiter PUF mechanism

3.2 Implementation of XFAPUF

Basic APUF produces the responses based on linear association with the random challenges, whereas the arbitration process is controlled by the additional circuit in the feed-forward mechanism; consequently, the challenge will be unpredicted. Usually, strong CRPs are availed by an intelligent switching mechanism performed by SCs in any APUFs. The unreliability of APUF is explored from the delay relationship between its input and output; thereby the propagation delay of an n-bit APUF for i^{th} is defined as D^i_{path1} and D^i_{path2} respectively. The timing difference between the two delay paths of n-bit APUF is summed up and deduced D^n_{path1} and D^n_{path2} by mapping the original challenge $C_i \epsilon \{0, 1\}$ into $C_i \epsilon \{-1, 1\}$ we get:

$$D^i_{path1} = \frac{1 + C_i}{2}(t^i_{path1} + D^{i-1}_{path1}) + \frac{1 - C_i}{2}(t^i_{path2to1\_cross} + D^{i-1}_{path2}) \tag{3.1}$$

$$D^i_{path2} = \frac{1 + C_i}{2}(t^i_{path2} + D^{i-1}_{path2}) + \frac{1 - C_i}{2}(t^i_{path1to2\_cross} + D^{i-1}_{path1}) \tag{3.2}$$

where $D^0_{path1} = D^0_{path2} = 0$, t^i_{path1}, t^i_{path2} are the straight forward delays, and $t^i_{path1to2\_cross}$, $t^i_{path2to1\_cross}$ are the crossed delays represented through i^{th} stage at challenges -1 and 1 respectively.

3.2.1 Design considerations for XFAPUF

Circuit design is a complex procedure that creates an electronic circuit in order to address the requirement. Although theoretical calculations are required to choose the components, there are some variables that are out of our control. The specification includes a complete description of the circuit, an electrical description, information on the input signals that the circuit accepts, its output properties, power consumption, etc. The designer continues to refine the specification as the design process goes along while taking the needs of the device into account. The design specifications for XFAPUF are shown in Tab.3.1.

3.2.2 Feed Forward Stage (FFS)

In XFAPUF, the switching between SCs is designed with the combination of Low Voltage Threshold (LVT) and High Voltage Threshold (HVT) transistors to produce delay variance; considered as one of the sources of PVs. So, unpredictability and randomness are achieved through XoR feed, as a proposed mechanism when compared to the existing

Table 3.1 Specifications for XFAPUF

Design Parameters		
Aspect ratio (μm) (Inverters)	PMOS	1.12/0.18
	NMOS	0.24/0.18
Aspect ratio (μm) (2x1 Muxes)	PMOS	0.24/0.18
	NMOS	0.24/0.18
Aspect ratio (μm) (Arbiter)	PMOS	0.24/0.18
	NMOS	0.24/0.18
Aspect ratio (μm) (XoRs)	PMOS	1.12/0.18
	NMOS	0.24/0.18
V_{DD} (V)	1.8	
Input (I)	16-bit	
Challenges (C)	"n-bit" (Depends on stages)	
Responses (R)	32-bit	

APUFs. The positioning of the XoR feed has to be taken care of, while the concurrent bit streams are generated to affect the randomness of the APUF. Fig.3.3 shows the proposed block of FFS designed by successive SCs with XoR feed. A single FFS of XFAPUF is fed with challenges C_1 to C_7 and has an XoR gate between 6th and 8th SCs of an 8-stage arbitration scheme. The propagation delay of XFAPUF is evaluated at every single FFS stage by splitting Eq.3.1 and Eq.3.2 into three individual SC delay stages, and all are summed up to get D^{FFS}_{path1} and D^{FFS}_{path2}. The delay upto 6th SC is deduced and represented

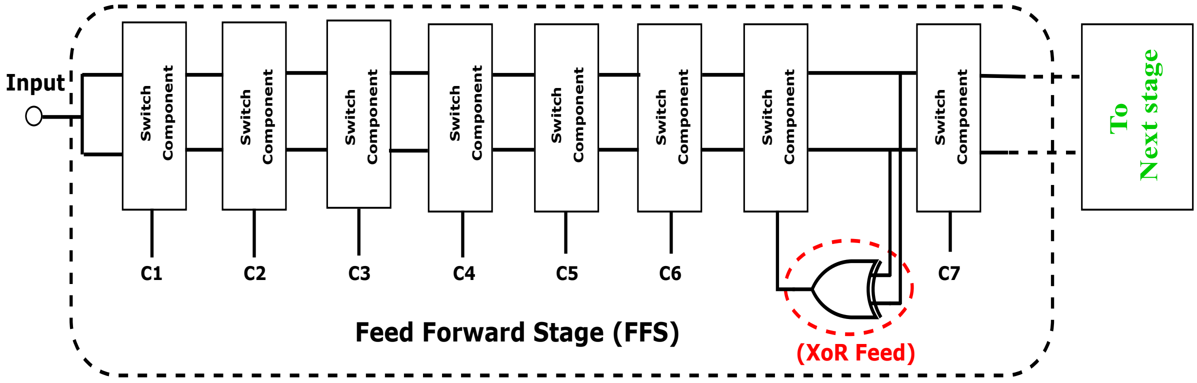


Figure 3.3 Single FFS arbitration

as D^6_{path1}, D^6_{path2} respectively.

$$D^6_{path1} = \frac{1+C_6}{2}(t^6_{path1} + D^5_{path1}) + \frac{1-C_6}{2}(t^6_{path2to1\_cross} + D^5_{path2}) \tag{3.3}$$

$$D^6_{path2} = \frac{1+C_6}{2}(t^6_{path2} + D^5_{path2}) + \frac{1-C_6}{2}(t^6_{path1to2\_cross} + D^5_{path1}) \tag{3.4}$$

At the end of the 7^{th} SC, the delays D^7_{path1} and D^7_{path2} are evaluated as

$$D^7_{path1} = \frac{1+C_{xor}}{2}(t^7_{path1} + D^6_{path1}) + \frac{1-C_{xor}}{2}(t^7_{path2to1\_cross} + D^6_{path2}) \tag{3.5}$$

$$D^7_{path2} = \frac{1+C_{xor}}{2}(t^7_{path2} + D^6_{path2}) + \frac{1-C_{xor}}{2}(t^7_{path1to2\_cross} + D^6_{path1}) \tag{3.6}$$

where C_{xor} is the challenge feed by XoR gate based on the 7^{th} SC output. Finally, at the end of the 8^{th} SC the total delays D^8_{path1} and D^8_{path2} are deduced as

$$D^8_{path1} = \frac{1+C_7}{2}(t^8_{path1} + D^7_{path1} + D_{xor}) + \frac{1-C_7}{2}(t^8_{path2to1\_cross} + D^7_{path2} + D_{xor}) \tag{3.7}$$

$$D^8_{path2} = \frac{1+C_7}{2}(t^8_{path2} + D^7_{path2} + D_{xor}) + \frac{1-C_7}{2}(t^8_{path1to2\_cross} + D^7_{path1} + D_{xor}) \tag{3.8}$$

where D_{xor} is a specific delay acquired in between 6^{th} and 8^{th} SC. Denoting the delay difference between top and bottom XFAPUF inputs as DD_{FFS}, following Eq. 3.1 to Eq.3.8, we get $DD_{FFS} = D^8_{path1}$ - D^8_{path2}. The response (R) of an XFAPUF of 8-bit length (single FFS) is therefore determined by the sign of DD_{FFS} is given below.

$$R = \begin{cases} 0, & \text{if sgn}(\mathrm{DD}_{FFS}) < 0 \\ 1, & \text{if sgn}(\mathrm{DD}_{FFS}) > 0 \end{cases} \tag{3.9}$$

A single (1-bit) response, corresponding CRP, is obtained at the end of FFS with Δd. A single FFS stage is successively connected to the next stages to bring complexity to the arbitration mechanism. An XoR feed is placed in the 7^{th} position (referred to as odd forwarding scheme) at each FFS stage to implement an n-stage arbitration shown in Fig. 3.4.

3.2.3 n-bit key generation

Each stage of FFS is active by 'm' challenges and corresponding n-bit responses are recorded as CRPs and its matrix representation is given below. For example, a 4-bit response is generated from 4-stage FFS XFAPUF (considered as one PUF cell), requiring 28 (28×4=112) challenges at each PUF cell. A small-stage arbitration scheme is not

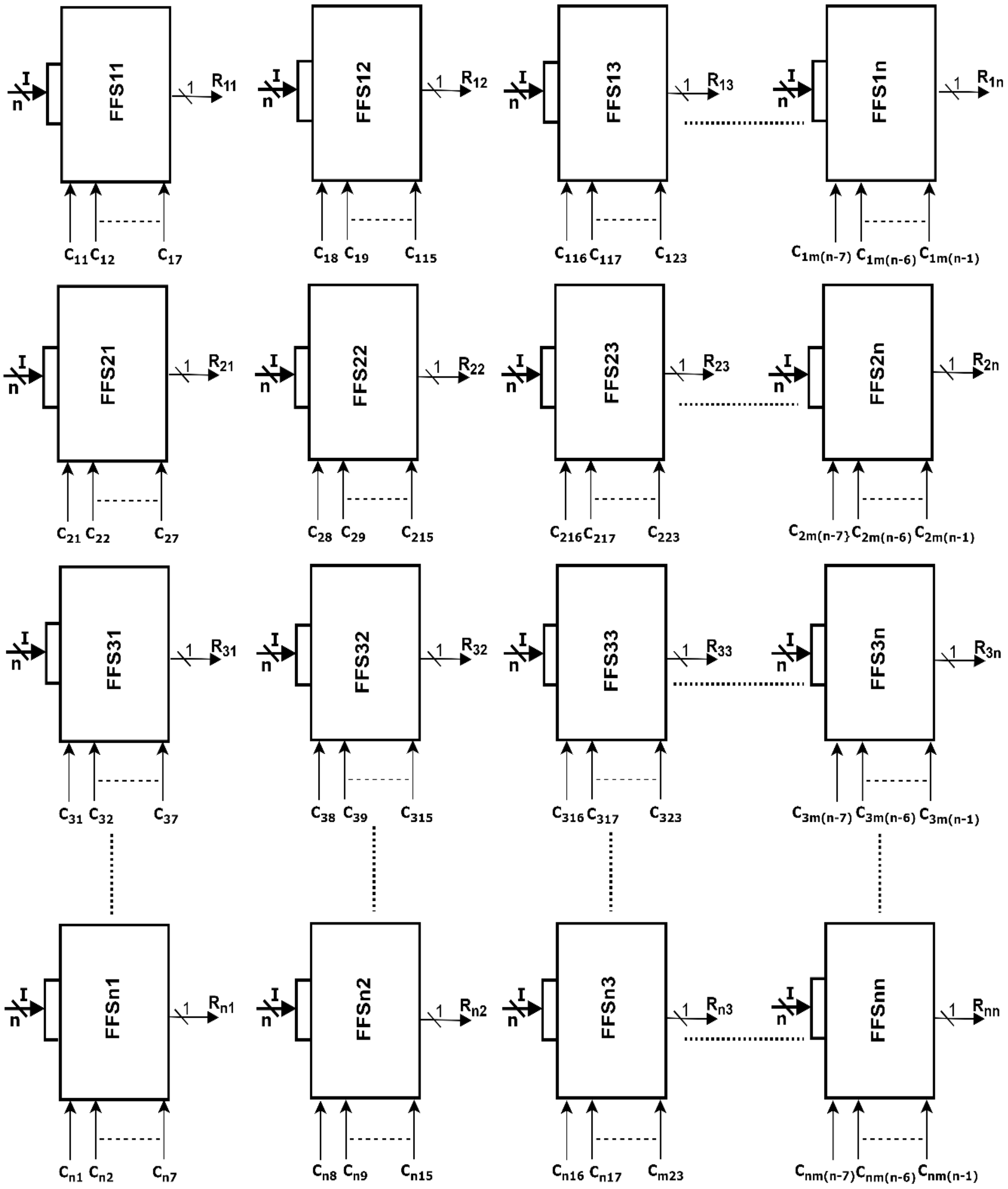


Figure 3.4 n-stage XFAPUF with 8-challenge FFS

appropriate in designs of delay-based PUFs; therefore, it has to be extended up to n-bit arbitration to produce larger delays. Due to large-stage arbitration, high randomness is achieved and it is very hard to predict the responses from unauthorized resources. The whole XFAPUF CRP generation is represented in matrix form is shown below.

$$\begin{bmatrix} I_1 & I_2 & I_3 & .... & I_n \end{bmatrix} \begin{bmatrix} C_{11} & C_{12} & C_{13} & ... & C_{1m(n-1)} \\ C_{21} & C_{22} & C_{23} & ... & C_{2m(n-1)} \\ C_{31} & C_{32} & C_{33} & ... & C_{3m(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ C_{n1} & C_{n2} & C_{n3} & ... & C_{nm(n-1)} \end{bmatrix} = \begin{bmatrix} R_1 & R_2 & R_3 & ... & R_n \end{bmatrix}$$

3.2.4 Earlier Response Detection (ERD) circuit

Elementary APUFs generate responses R1 and R2, which are not necessary as only a single response is required. To generate only a single response, an ERD circuit, shown in Fig.3.5, is proposed. ERD consists of OR and NOT gates (properly tuned) to take the responses from the arbiter and decide the earlier one. So, a unique response 'R' is generated from response bits R_1 or R_2 obtained at the arbiter end. The proposed ERD circuit generates a unique response 'R' either '1' if R1= '1' or '0' if R2= '1' instantly when there is a contention between R1 and R2. The first generated response should be identified by ERD, while the latter is suppressed. The main advantage of ERD is observed at prototyping or tape-out stages to achieve compactness in IC fabrication. Generally, pin availability is a major concern while fabricating an IC for customized applications. The arrangement of ERD after the arbiter stage also makes APUFs compact and compatible with the prototype.

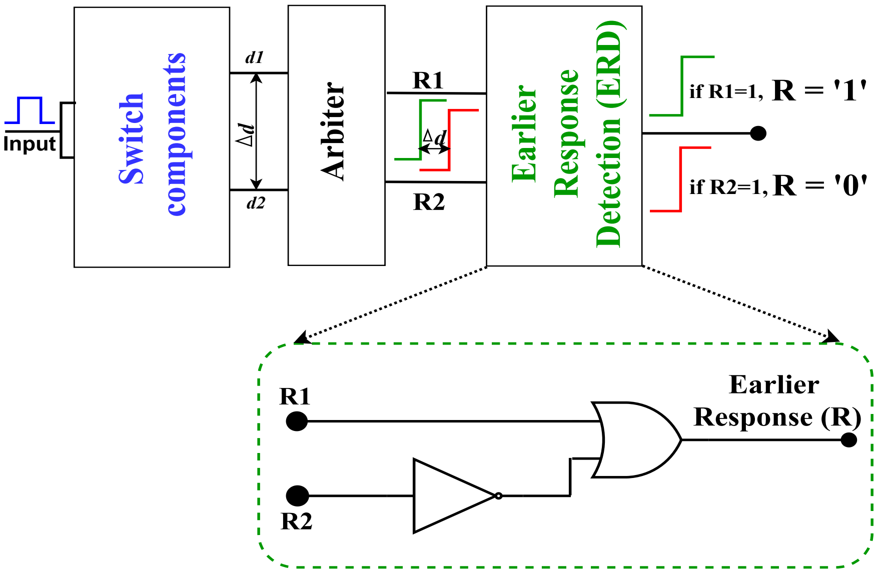


Figure 3.5 ERD circuit

3.3 Evaluation of XFAPUF

The proposed XFAPUF is implemented in UMC 180nm technology and simulated using Cadence Spectre. To perform the characterization of 100 different PUFs, 100 runs of Monte-Carlo simulation are performed. During simulation, intra-die and inter-die PVs are performed to evaluate the responses [29]. Each XFAPUF bit-cell designed with 8-stage becomes active with the 16-bit input 'I' and a 28-bit challenge (C_1 to C_{28}) through V_{bit} source and evaluates responses under the nominal operating condition at 25°C with a 1.8 V supply voltage.

3.3.1 Uniformity (u)

We evaluate the 32-bit responses from 50 XFAPUF instances with the PUF metric represented as Eq.2.1 in Chapter 2 at nominal operating conditions i.e., 25°C, 1.8V is shown in Fig.3.6. A white pixel can be interpreted as '1' and a black one as '0'. The probability of generating 1's is 45.5%, which indicates that XFAPUF output is not predictable and it is hard to attack.

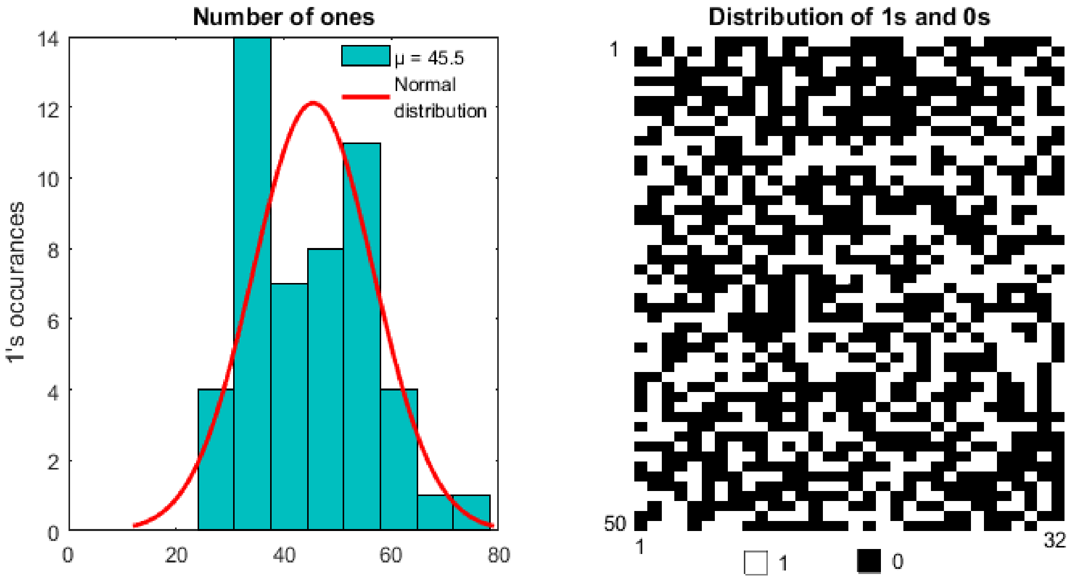


Figure 3.6 Uniformity of XFAPUF with a distribution of 1's and 0's

3.3.2 Diffuseness (D)

We performed diffuseness of 32-bit responses from 50 XFAPUF instances from the PUF metrics that represented as Eq.2.2 in Chapter 2 at 25°C and 1.8V is shown in Fig.3.7. The calculated mean (μ) from obtained HD values is 49.52%, which indicates that the variations of XFAPUF instances are close to the ideal value i.e., 50%.

3.3.3 Uniqueness (U)

Uniqueness measures inter-chip variation among different XFAPUF instances implemented with the same challenge as the PUF metric considered in Eq.2.3 of Chapter 2.

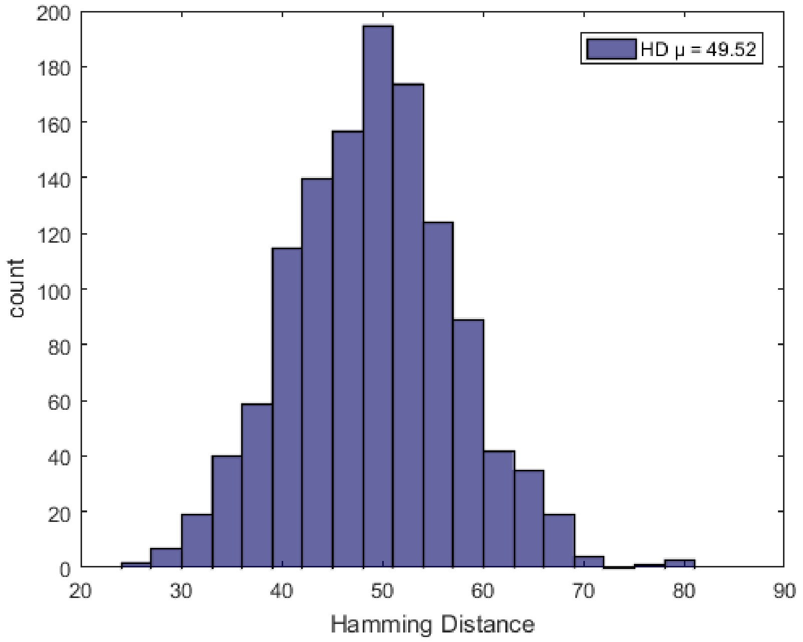


Figure 3.7 Diffuseness of XFAPUF

We evaluated the Inter-HD of 32-bit responses from 100 different XFAPUF instances at 25°C and 1.8V is shown in Fig.3.8. The calculated mean 50.03% indicates that the good randomness among different instances.

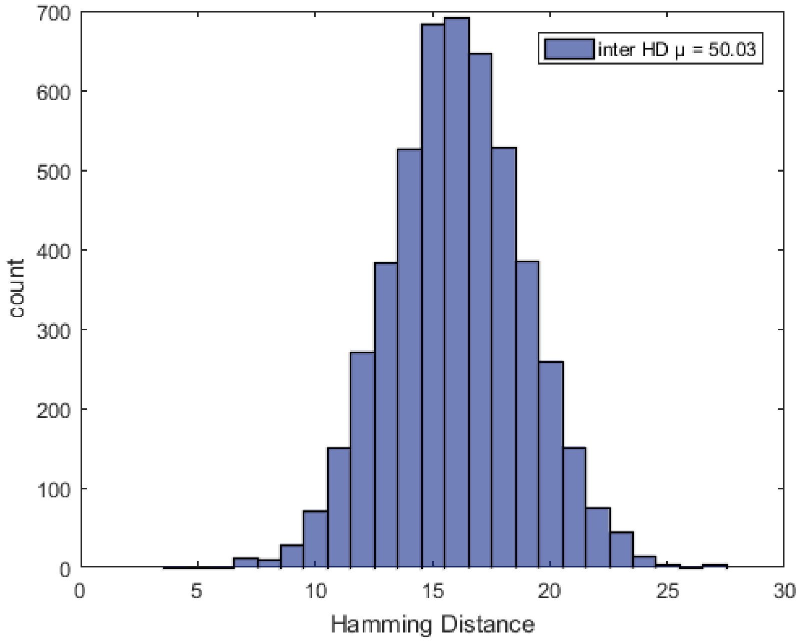
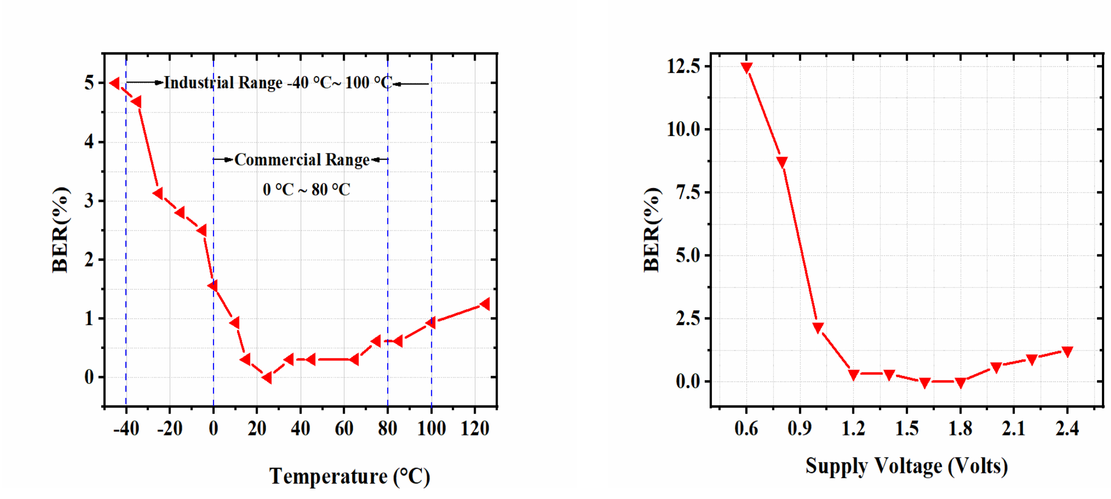


Figure 3.8 Uniqueness of XFAPUF (inter-HD)

3.3.4 Reliability (R)

A PUF should generate the same response at any state for the same challenge applied to identical ICs. Unfortunately, variations in the supply voltages or temperature can change the behaviour of the IC in the form of circuit delay and lead to unpredicted responses. So, the same response bits should be reproduced at different operating conditions. We measure the Bit Error Rate (BER) of the 32-bit responses from 100 XFAPUF instances that are evaluated through PUF metric represented as Eq.2.4 and Eq.2.5 in Chapter 2 at different operating conditions. The BER of the XFAPUF response versus temperature is shown in Fig.3.9a. The average reliability calculated from 100 XFAPUF responses over the commercial range (0°C to 80°C) is 99.81% at 25°C, and the worst-case reliability is 96.33% at 0°C with an error rate of 0.15% and 1.56% respectively. A supply voltage variation up to ±20% V_{DD} is applied to the XFAPUF as shown in Fig.3.9b. The corresponding reliability is 98.86% at 1.8V, and the worst-case reliability is 95.57% at 0.6V with an error rate of 0.31%, and 1.96% respectively. In addition, over the industrial range (-40°C to 100°C) BER is less than 4.8%.



(a) BER Vs Temperature

(b) BER Vs Supply Voltage

Figure 3.9 Reliability assessment through BER

3.3.5 Security evaluation

PUFs are specifically proposed for security applications and can maintain strong security against threat models performed by attackers. A PUF uses a CRP mechanism derived from inbuilt PVs performed by the ICs. If a PUF is used for authentication, the attacker can perform different trials to know the valid CRPs to crack the PUF function. Otherwise, if it is a secret key generation the attacker can concentrate on the PUF response pairs by exploiting the PUF weakness. To evaluate the security of the proposed XFAPUF, a common machine learning attack to PUF is employed, i.e., LR [78]. LR uses a maximum likelihood function and assumes the data follows a specific distribution. A prediction rate of 48% represents an unsuccessful attack to the proposed PUF which is shown in Fig.3.10. The XFAPUF of 32-bit is more resistant to attacks while the average prediction rate reaches 48% with a training sample of 400. The prediction accuracy of 32-bit XFAPUF reaches 51% with 1500 CRPs when compared with a smaller number of 500 CRPs. So, with a small number of samples trained, the prediction rates increase by increasing the training CRPs.

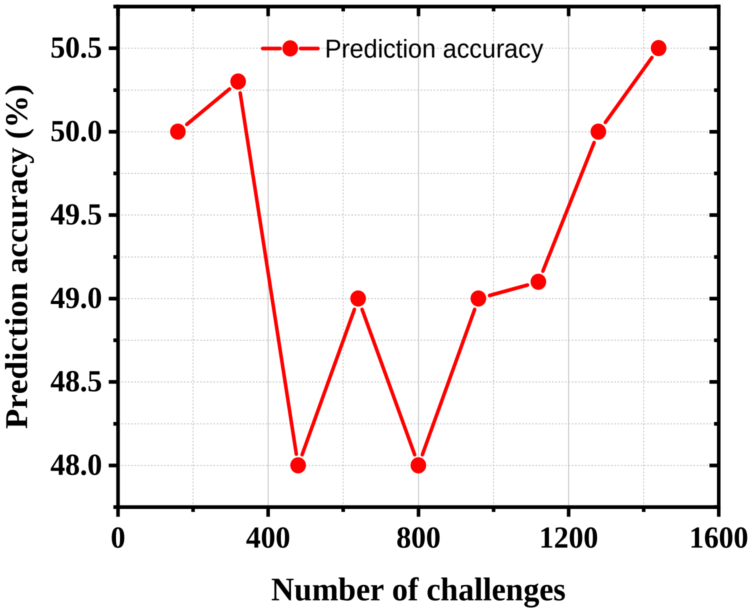


Figure 3.10 Prediction accuracy of LR to XFAPUF

3.3.6 Analysis and Comparison of XFAPUF

A comparison of major PUF metrics Uniqueness (U) and Reliability (R) of the presented XFAPUF scheme with the state-of-the-art is shown in Tab.3.2.

The most distinctive PUFs published in the recent fifteen years have been incorporated in this comparison. It is obvious from Table 1 that better 'U' is achieved when compared to the existing PUFs, except [55]. The 'R' of the proposed PUF in temperature and supply voltage variation is slightly improved by more than 1.5% and 1.3%, respectively, when compared to the PUF designed in [54]. In comparison with [48], the

Table 3.2 Comparison of metrics of different PUF designs

References	**Technology**	**Uniqueness (Ideal-50%)**	**Reliability (Ideal-100%)**	**BER (%)**	**Memory function**
Sankar et al., 2018 [54]	22nm	49.77%	-	-	No
Avvaru et al., 2020 [31]	28nm	41.53%	97.10%^{t}, 93.10%^{v}	-	No
Guo et al., 2017 [48]	45nm	50%	98.10%	-	No
Khan et al., 2020 [52]	65nm	50.07%	98.27%	-	No
Khan et al., 2020 [52]	65nm	49.92%	97.72%	-	No
Tao et al., 2016 [55]	65nm	50.04%	98.3%	-	No
Lee et al., 2004 [12]	180nm	23%	95.20%^{t}, 96.30%^{v}	-	No
Lim et al., 2005 [13]	180nm	38%	90.20%	-	No
Ruhr et al., 2010 [78]	40nm	49%	-	0.36^t, 0.98^v	Yes
Xu et al., 2020 [68]	Artix7	53.16%	95.54%	-	No
Ruhr et al., 2013 [79]	65nm	50.30%	98.60%^{t}, 98.52%^{v}	-	Yes
This work	**180nm**	**50.03%**	**99.81%^{t}, 98.86%^{v}**	**0.15^t, 0.31^v**	**No**

t = temperature variation, v=supply voltage variation

BER deteriorates by 50% when there are changes in temperature and supply voltage. The memory function is a limitation of the proposed PUF; however, higher reliability is achieved when compared to [48] and [50]. At the nominal operating condition (25°C), the proposed XFAPUF achieves a uniqueness of 50.03%, and a reliability of 99.81%, being the best as compared to the existing PUF implementations.

3.3.7 Performance evaluation

The input data with 20ns rising edge is excited across the 32-stage XFAPUF for a given 28-bit challenge, the response time at the arbiter is expected as 0.32µs. Suppose, we want to generate 1000 CRPs using a basic arbiter scheme to distinguish one billion chips it takes 20µs. This is fast as compared to other arbiter PUFs and evaluated infrequently to obtain a secret key for most applications such as chip authentication. To boost the performance of an arbiter we can introduce multiple delay paths at certain levels of the arbiter stage or evaluate the responses in parallel. The quality metrics to achieve high reliability of XFAPUF at different temperatures are shown in Tab.3.3. The performance of XFAPUF is evaluated by PUF metrics i.e., inter-HD and intra-HD expressed in Eq.3.12 and Eq.3.13 have significant advantages in voltage and temperature reliability. For per 10°C change, the average BER increases by 0.15%, and when the supply voltage changes per 0.2V, the BER worsen by 0.31%. Even though, an XFAPUF has the advantage of a compact challenge-feeding mechanism but is either dependent on the user or any external source. So, an advanced challenge generation mechanism is required to feed the SCs without any intervention from the user. Persistently, a chaos-based challenge generation mechanism is proposed in the following section to feed the SCs in an efficient manner.

Table 3.3 XFAPUF quality metrics at different temperatures

	-40°C	**0°C**	**25°C**	**80°C**	**100°C**
Intra-HD (%)	96.33	98.58	99.81	98.07	97.51
Hamming weight (%)	39.7	42.13	45.5	43.35	44.92
Inter-HD (%)	62.33	57.25	50.03	49.8	47.36
BER (%)	4.9	1.56	0.15	0.62	0.93

3.4 Random Number Generators (RNGs)/Random Bit Generators (RBGs)

Random numbers play a crucial role in cryptography applications due to their non-deterministic nature. Basically, RNGs or RBGs shown in Fig.3.11 are preferred to generate random numbers or random bits to manipulate the system by foreseeing processes. The random numbers are essentially required in the following applications for cashless payments, ATMs, online payments, e-banking, point of sale, prepaid cards, etc. In cryptography, the principle protocols use random numbers to generate a secret key between sender and receiver. Whereas, the presumption of the secret key will diminish the key rate when random numbers are generated by RBGs [7,14]. A PRNG produces periodic or

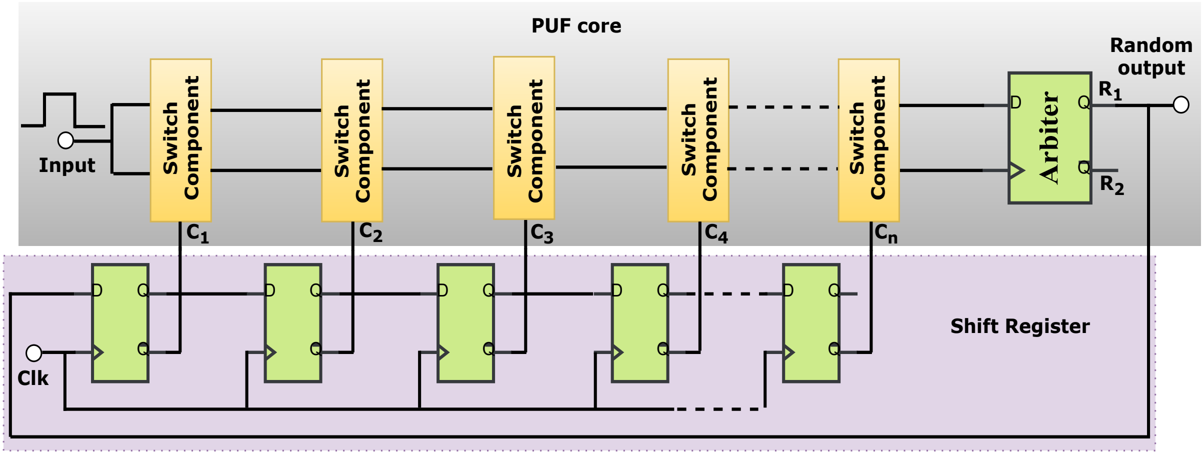


Figure 3.11 Random number generation

deterministic random numbers based on a mathematical formula, which are determined by the initial state called a seed. PRNGs [83, 84] form a strong correlation between 0's and 1's thereby increasing the cryptographic strength. In contrast to PRNGs, HRNG is proposed to generate random numbers through randomness extracted from physical processes that make them a better candidate for secret key generation.

3.4.1 Chaotic RNGs

Chaos means to generate indeterministic random numbers from repeated measurements. The chaotic-based RNGs [85–87] offer high-quality random numbers by the conceptual mixing of chaos and randomness to increase the robustness of the systems. Mostly, the state-of-the-art chaotic systems designed for the fast generation of random numbers are electrical, optoelectrical, optical and mechanical-based constructions. Hence, the chaotic-based systems are sensitively dependent on initial conditions that are purely hardware-based but they require discrete implementations of analog circuits. The digital chaotic circuits incorporating reprogrammable devices suffer from limited computational resources to produce pseudo-random output.

3.5 Chaotic-APUF

A chaotic-based APUF, which is less prone to attacks, is proposed to achieve high reliability in RNG-based PUFs, which are employed for key generation. Moreover, it presents the background knowledge of chaotic functions and the course of incorporating them into feeding SCs. The major contributions are as follows,

- A chaotic-based APUF for reliable key generation of security devices is presented to attain non-linearity in the arbitration process with chaos function.
- We introduced a chaotic APUF to feed the arbiter thereby the complexity is attained in the arbitration process, making APUF more resistant to attacks.
- We evaluate the simulation results with PUF metrics and show that the proposed one has high reliability compared to the existing RNG PUFs.

3.5.1 Design considerations for Chaotic-APUF

The design parameters considered to achieve the specific requirement for the design of chaotic APUF are presented in Tab.3.4. These are helpful to feed SCs with proper coordination between challenges and responses.

Table 3.4 Specifications for Chaotic-APUF

Design Parameters		
Aspect ratio (μm) (Inverters)	PMOS	1.12/0.18
	NMOS	0.24/0.18
Aspect ratio (μm) (2x1 Muxes)	PMOS	0.24/0.18
	NMOS	0.24/0.18
Aspect ratio (μm) (Arbiter)	PMOS	0.24/0.18
	NMOS	0.24/0.18
V_{DD} (V)	1.8	
Input (I)	16-bit	
Challenges (C)	Automated “n-bit” (Depends on stages)	
Responses (R)	16-bit	

3.5.2 Implementation of Chaotic-APUF

The chaotic feed mechanism is the sophisticated method to introduce dynamic behaviour in the random number generation which seems to be unpredictable. The chaotic

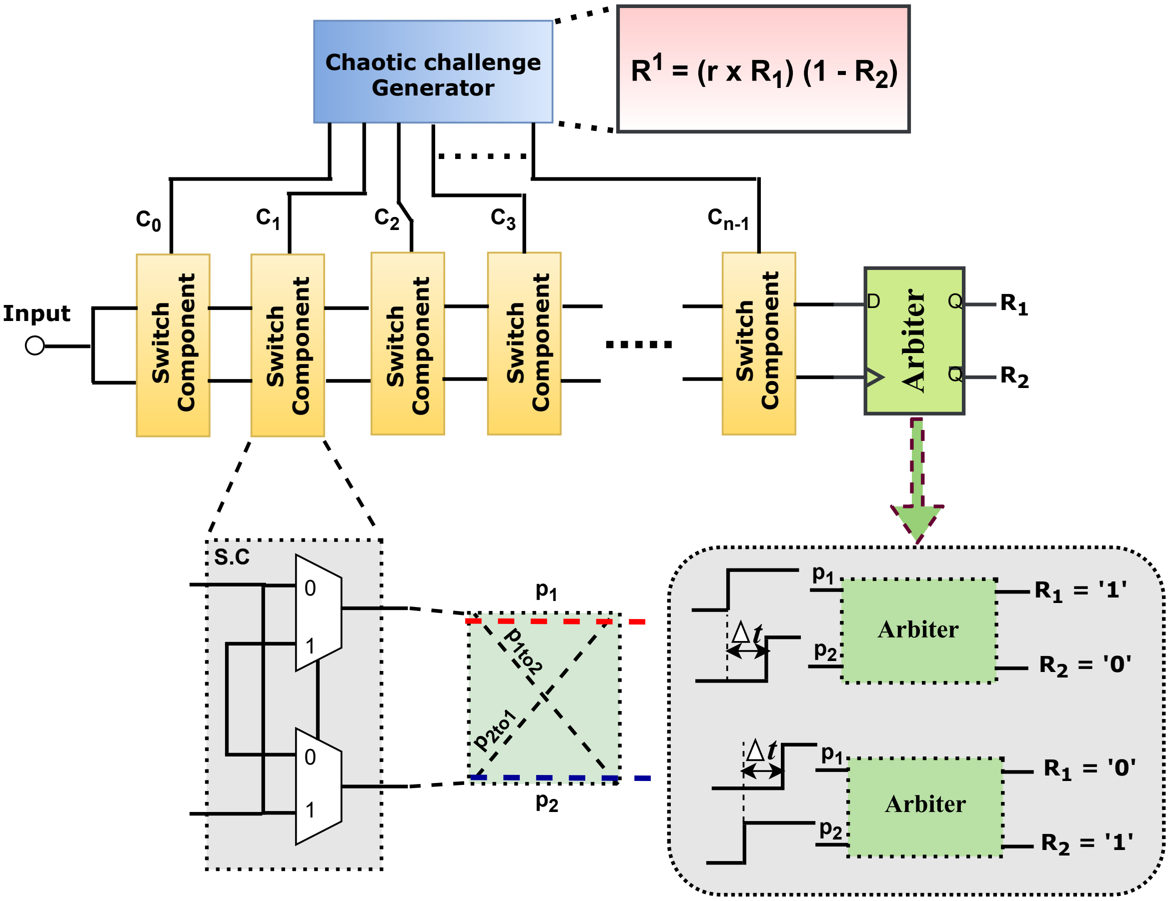


Figure 3.12 Chaotic APUF for key generation

systems build complex circuit behavior which affects the circuit's state to enhance the unpredictability. However, the hardware security mechanisms equipped with chaotic properties in PUFs came into existence to augment the uncertainty in the challenge generation. In this section, the chaotic-based challenge feed to the APUFs has been proposed thereby ambiguity in the arbitration mechanism is achieved.

An Arbiter PUF (APUF) [12–17] shown in Fig.3.12 is the basic PUF implementation that consists of Switch Components (SCs) for the switching mechanism and an arbiter for response selection. APUF is excited by delay paths of path1 (P_1) and path2 (P_2) concurrently and makes the contention against each other due to PVs. Generally, the SCs are invoked by the challenges (C_0 to C_{n-1}) for performing the arbitration process, and an arbiter for deciding the earlier path to generate a response (key). Even though, the challenges are given manually in APUF is considered to be a strong PUF because of its non-linear nature in the arbitration mechanism. In Fig.3.12, path delays P_1 (represented in red), P_2 (represented in blue), P_{1to2}, and P_{2to1} (represented in dashed lines) have existed as forward and crossed path delays due to PVs in the transistors, and the associated time delay Δt is evaluated at every end of the SC.

The proposed APUF generates reliable responses (keys) which are harvested from the chaotic feed. The Chaotic Challenge Generator (CCG) represented in Fig.3.12 generates the random challenges (C_0 to C_{n-1}) based on the chaotic function represented in Eq.3.15.

$$R^1 = (r \times R_1)(1 - R_2) \tag{3.15}$$

where R^1 is the subsequent bit estimation, 'r' is the initial parameter set as '1', R_1 is the response obtained from path1, and R_2 is the response obtained from path2. In order to improve the complexity and randomness in APUFs, the chaotic system generates confused and rearranged key spaces to reduce the possibility of comprehensive attacks. Moreover, the randomness is improved in the sequence by the value of the initial seed parameter which is arbitrary. We have designed an APUF circuit that addresses the identification or authentication issues for IoT-enabled devices using a suitable chaotic scheme. The respective chaotic sequence of the APUF when excited with the chaotic scheme with respect to the bit string is shown in Fig.3.13.

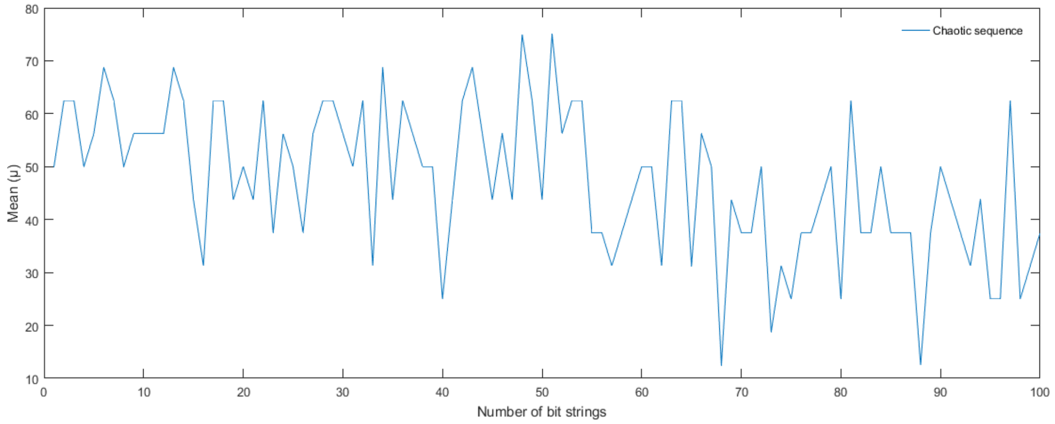


Figure 3.13 Chaotic sequence generation

3.5.3 Evaluation of Chaotic-APUF

The proposed chaotic APUF design is implemented in UMC 180nm technology and simulated using Cadence Spectre. The characterization is performed for 100 different

PUFs with 500 runs of Monte-Carlo simulation. Thereby, intra-die and inter-die PVs are performed with chaotic challenge generation to evaluate the responses. Each chaotic APUF bit-cell designed with 16-stage becomes active with the 16-bit input 'I' and a 16-bit challenge (C_0 to C_{15}) through CCG and evaluates PUF metrics for the responses under the nominal operating condition at 27°C with a 1.8 V supply voltage.

3.5.3.1 Uniformity (u)

The uniformity of a PUF design is used to calculate the proportion of "zero" (0's) and "one" (1's) in the response bit-stream, from which the likelihood of each value may be calculated. If a design generates replies that are ideally random, the pattern of response bits will be the same for 1s and 0s. Having this feature, from a security perspective, prevents an intruder from assuming that a device's answer is biased towards a particular value. The ideal value of uniformity 50% ensures the PUF's unpredictable nature. The

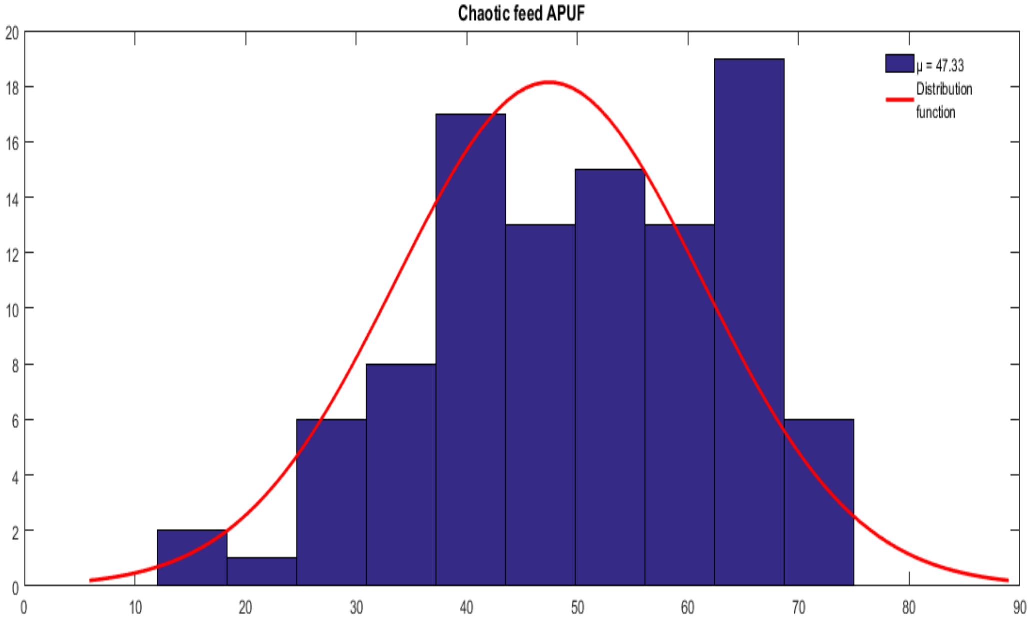


Figure 3.14 Uniformity of chaotic PUF

response vector $R_{i,j}$ and the distribution j's of "1s" and "0s" are described as Eq.2.1 in Chapter 2. We evaluate the 16-bit responses from 100 chaotic APUF instances at nominal condition i.e., 27°C, 1.8V is shown in Fig.3.14. The probability of generating 1's is 47.33%, which indicates that the chaotic behaviour of APUF is hard to predict.

3.5.3.2 Diffuseness (D)

Diffuseness can be assessed by calculating the mean of HD from the response vectors R_i and R_j in the same chaotic PUF with different challenges applied nominally represented as Eq.2.2 in Chapter 2. Two distinct n-bit answer vectors, R_i and R_j, were received from two distinct challenges. Ideal diffuseness guarantees collision-free responses at 50%. Fig.3.15 illustrates the diffuseness of 16-bit answers from 500 PUF instances done at 27°C and 1.8V. The acquired HD values of 50.02% for Chaotic APUF show that the variability of occurrences is close to the ideal value of 50%.

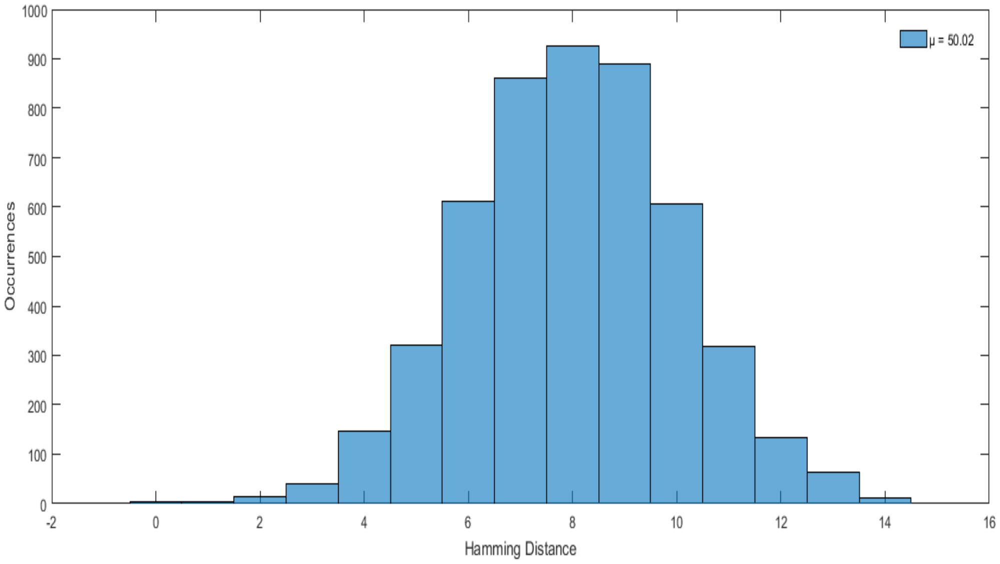


Figure 3.15 Diffuseness of Chaotic APUF

3.5.3.3 Reliability (R)

Reliability determines how robust a PUF is under diverse environmental conditions. A PUF should typically respond to a challenge in nominal conditions in the same way. While changes in supply voltage (V_{DD}) and temperature (°C) can significantly affect the responses. The number of uneven bits can be used to estimate the average intra-chip HD of n-bit replies, which can be used to assess a PUF's reliability. When presented with the same obstacles, PUF reactions should ideally remain constant throughout numerous observations. The definition of reliability evaluation is defined as Eq.2.4 and Eq.2.5 in Chapter 2. Where 'm' denotes the number of observed trials performed on the same Chaotic APUF instance with the same challenge. The reference response $R_{i,ref}$ is measured at normal operating conditions i.e., 27°C, 1.8V, and $R_{i,t}$ is the t^{th} measured response at a different temperature or supply voltage conditions. The variation in

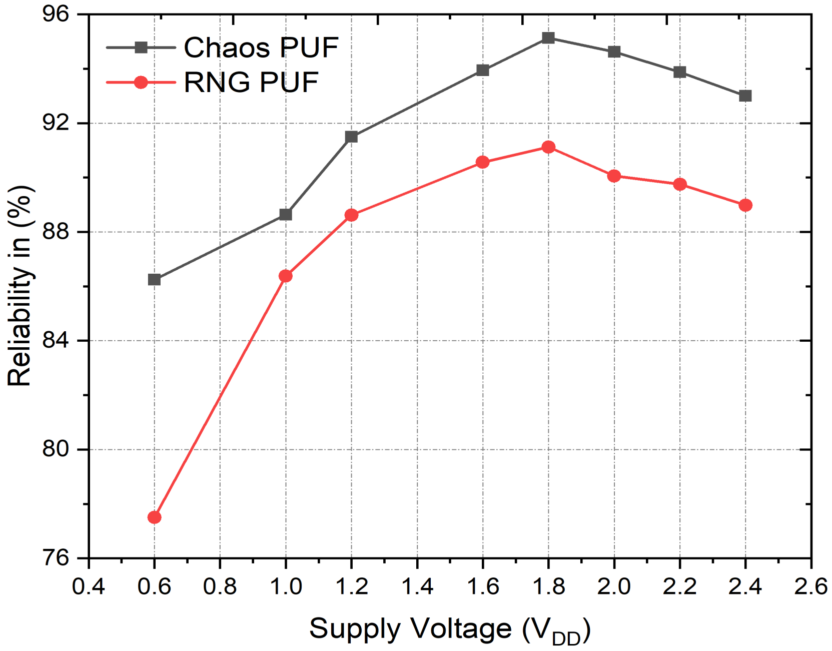


Figure 3.16 Reliability analysis through supply voltage variation

output responses when operating at a changing supply voltage or temperature indicates the reliability of the device. The simulations are run at a range of temperatures between -40°C to 125°C. The 16-bit chaotic APUF has attained an improved average dependability rating of 93.52% against RNG APUF of 89.28%. In nominal settings and worst-case scenarios, the reliability of Chaotic PUF and RNG PUF come down at 89.66% and 82.13%, respectively. The impact of a change in supply voltage at a range of 0.6 V to 2.4 V, the average values of Chaotic PUF and RNG PUF are 92.11% and 87.87%, respectively. The worst-case reliability of Chaotic PUF and RNG PUF are observed as coming down at 86.25% and 77.5% at nominal operating conditions.

3.5.3.4 Analysis and Comparison

The reliability measurement of the Chaotic APUF is shown in Fig.3.16 and Fig.3.17 as a function of supply voltage and temperature. As compared to the state-of-the-art designs represented in Tab.3.5, the Chaotic PUF attained prominent reliability of 96.54% at 27°C temperature and 95.13% 1.8V supply voltage. Tab.3.5 shows a comparison of the presented Chaotic APUF scheme with the state-of-the-art in terms of significant PUF metrics Uniformity (u), Diffuseness (D), and Reliability (R) are evaluated through the

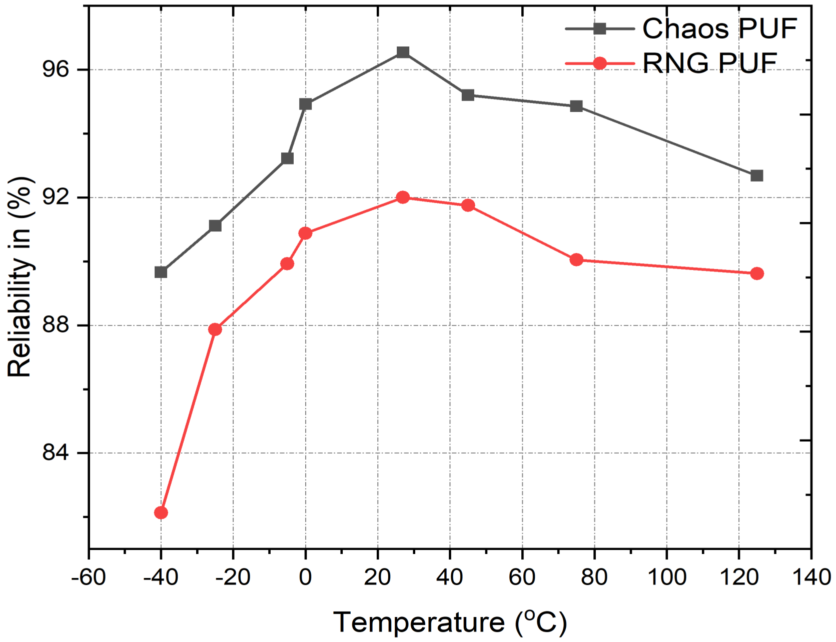


Figure 3.17 Reliability analysis through temperature variation

Table 3.5 Comparison of metrics of different PUF designs

References	**PUF Design**	**Technology (nm)**	**Uniformity (Ideal-50%)**	**Diffuseness (Ideal-50%)**	**Reliability (Ideal-100%)**
Idriss et al., 2021 [4]	APUF	65	47.22%	46.81%	NA
Lee et al., 2004 [12]	APUF	180	23%	NA	95.20%^{t}, 96.30%^{v}
Lim et al., 2005 [13]	FF-APUF	180	38%	NA	90.20%
Liu et al., 2019 [29]	FF-APUF	28	40%	NA	97.10%^{t}, 93.90%^{v}
Majo et al., 2008 [24]	DAPUF	-	55.01%	49%	NA
Khan et al., 2020 [52]	CMQC	65	50.25%	64.03%	98.27%
Khan et al., 2020 [52]	VMQC	65	50.02%	63.92%	97.72%
Jaya et al., 2018 [54]	CMOS	65	50.04%	64.09%	98.3%
Maiti et al., 2009 [17]	RO-PUF	180	42.8%	NA	80.6%
Bonil et al., 2016 [87]	Chaos-PUF	180	36.5%	NA	91.33%
This work	***Chaotic APUF***	***180***	***47.33%***	***50.02%***	***96.14%^{t}, 95.13%^{v}***

t = temperature variation, v=supply voltage variation, NA = Not Applied number of CRPs used to attain the results are 500.

3.5.3.5 Performance evaluation

The chaotic APUF has better uniformity compared with the conventional APUF's [4, 12], FF-APUF's [13, 29], DAPUF [24], RO-PUF [17], and Chaos PUF [87]. However, it is better as compared with CMQC [52], VMQC [52], and CMOS [54] PUF designs. The Diffuseness for proposed Chaotic APUF results of 50.02% when compared with the conventional APUF is 46.81% by [4], 64.03% by [52], and 64.09% by [54] respectively. When compared to the PUF designed in [4, 12], the Chaotic APUF's reliability over the temperature and supply voltage variation is enhanced by more than 1.6% and 0.2%, respectively. The chaotic APUF design exhibits good reliability results of 96.14% as the conventional APUF design [12] on an ASIC. The proposed Chaotic APUF has a memory function limitation; however, it achieves higher reliability than other state-art RO and chaos-based PUF designs [17, 87].

3.6 Summary

In this chapter, we have introduced the delay-based feed-forward arbiter PUF mechanism, XFAPUF has the advantage that compact challenges fed through complex arbitration can achieve higher reliability than any other APUFs. The experimental evaluation of XFAPUF shows the uniqueness and reliability of 50.03% and 99.81% respectively, higher than that of the previous works. Moreover, XFAPUF is also highly resistant to attacks since a prediction accuracy of 48% is achieved when LR is applied. The compactness by ERD to develop PUF for prototyping ensures that the design incurs better compatibility than reported in the literature to date. XFAPUF significantly improves upon the previous APUF designs and has the potential to be the basis for CRP-based identification and authentication applications in the IoT. Moreover, the proposed XFAPUF mitigates the common machine learning attack like LR. Despite XFAPUF is strong, it doesn't have memory retention, which is a major function in memory PUFs to store the secret keys for authentication.

Subsequently, we have introduced the chaotic behaviour in the arbitration mechanism of APUF that has the advantage of higher uniformity and reliability than any other RNG PUFs. Since chaotic activity lacks statistical properties, it is challenging to make assumptions about creating pseudo-random numbers from it. The experimental evaluation of Chaotic APUF shows the uniqueness and reliability of 47.33% and 96.14% respectively, higher than that of the previous works. The chaotic values produced by the former chaotic systems are related to their system characteristics. The output sequence is confused and rearranged so that the system parameters from the previous run cannot be obtained from the following run, ensuring security. However, the proposed XFAPUF and Chaotic APUF achieved promising reliability in a key generation but are unable to feed challenges automatically.

Perhaps, the following chapter will address automatic challenge generation through the recursive feeding mechanism employed between SCs. The next chapter will describe the design and implementation of RC-FAPUF and introduce an automated challenge-feeding mechanism to enhance the process of non-linearity in arbitration. Thereby, the key generation mechanism made complex and improved reliability as compared to the state-of-the-art PUF designs.

Chapter 4

Recursive Challenge Feed Arbiter PUF (RC-FAPUF)

A feed-forward arbitration scheme is employed in arbiter-based PUFs to improve the randomness of the PUFs with sophisticated feed structures. An arbiter-based scheme generates digital information from the PUF responses through the absolute delay values of two identical delay paths and evaluates the identification capability, authenticity, and security. This chapter presents the recursive-based challenge feeding mechanism which improves the reliability of arbiter-based PUFs against various malicious attacks by adding impulsive non-linearity. The contributions of this chapter are,

- The feed-forward mechanism is used to achieve non-linearity in the arbitration process using a novel RC-FAPUF with recursive challenges-based key generation.
- We propose an RC-FAPUF with randomized challenges in the arbitration scheme using XoR feeding at each SC level. Thus, the feeding of the external challenges from the user is eliminated and makes RC-FAPUF more resilient to possible attacks.
- We provide the simulation results to infer the identification capability, reliability, and security of the arbiter-based PUF schemes in IoT-enabled applications.

4.1 Design considerations for RC-FAPUF

The RC-FAPUF utilizes specific requirements that create the design specification to achieve recursive feeding between SCs as presented in Tab.4.1. Specifically, the special care must be taken to meet the timing constraints between SCs and XoR gates.

Table 4.1 Specifications for RC-FAPUF

Design Parameters		
Aspect ratio (μm) (Inverters)	PMOS	1.12/0.18
	NMOS	0.24/0.18
Aspect ratio (μm) (2x1 Muxes)	PMOS	0.24/0.18
	NMOS	0.24/0.18
Aspect ratio (μm) (Arbiter)	PMOS	0.24/0.18
	NMOS	0.24/0.18
Aspect ratio (μm) (XoRs)	PMOS	1.12/0.18
	NMOS	0.24/0.18
V_{DD} (V)	1.8	
Input (I)	16-bit	
Challenges (C)	"n-bit" (Depends on stages)	
Responses (R)	16-bit	

4.2 Implementation of RC-FAPUF

In this section, a novel approach to the feeding of SCs in APUF through automated challenges is introduced without any intervention from the user. It has a great advantage in the arbitration mechanism and generates strong CRP pairs to build secure and robust PUF. In general, the challenges are invoked by the user concerning the specified sequence. Whereas, in the proposed PUF concept the SCs are fed by the XoR gate that feeds challenge frequently. Thereby, complex arbitration and non-linearity are achieved in unique ID generation.

The conventional APUF shown in Fig.4.1 is the fundamental candidate implementation, which is aroused by delay paths path1 (P_1) and path2 (P_2) at the same time and creates contention between them as a result of PVs. The APUF is composed of SCs that are called upon by the challenges (C_0 to C_{n-1}) to carry out the arbitration procedure, and an arbiter chooses the earlier path to generate a response (key). Even though the challenges are supplied manually APUF is regarded as a robust PUF because of its non-linear nature in the arbitration mechanism. In Fig.4.1, path delays P_1 (denoted in red), P_2 (denoted in blue), P_{1to2}, and P_{2to1} (denoted in dotted lines) have been present as forward and crossed path delays due to PVs in the transistors and the related time delay Δt is evaluated at either end of the SC. Generally, strong CRP pairs are generated at the arbiter, and the delay relationship is explored for n-bit APUF for the "ith" instance is defined as D^{i}_{path1} and D^{i}_{path2} respectively. The timing difference Δt = t$_2$–t$_1$ between D^{i}_{path1} and D^{i}_{path2} of n-bit APUF are totalled and assume D^{n}_{path1} and D^{n}_{path2} by mapping the original challenge $C_i\epsilon\{0,1\}$ into $C_i\epsilon\{-1,1\}$ are represented in Chapter 3 as Eq.3.1 and Eq.3.2. Where $D^{0}_{path1} = D^{0}_{path2} = 0$, t^{i}_{path1}, t^{i}_{path2} are the straight forward delays, and $t^{i}_{path1to2\_cross}$, $t^{i}_{path2to1\_cross}$ are the crossed delays represented through i^{th} stage at challenges -1 and 1 respectively.

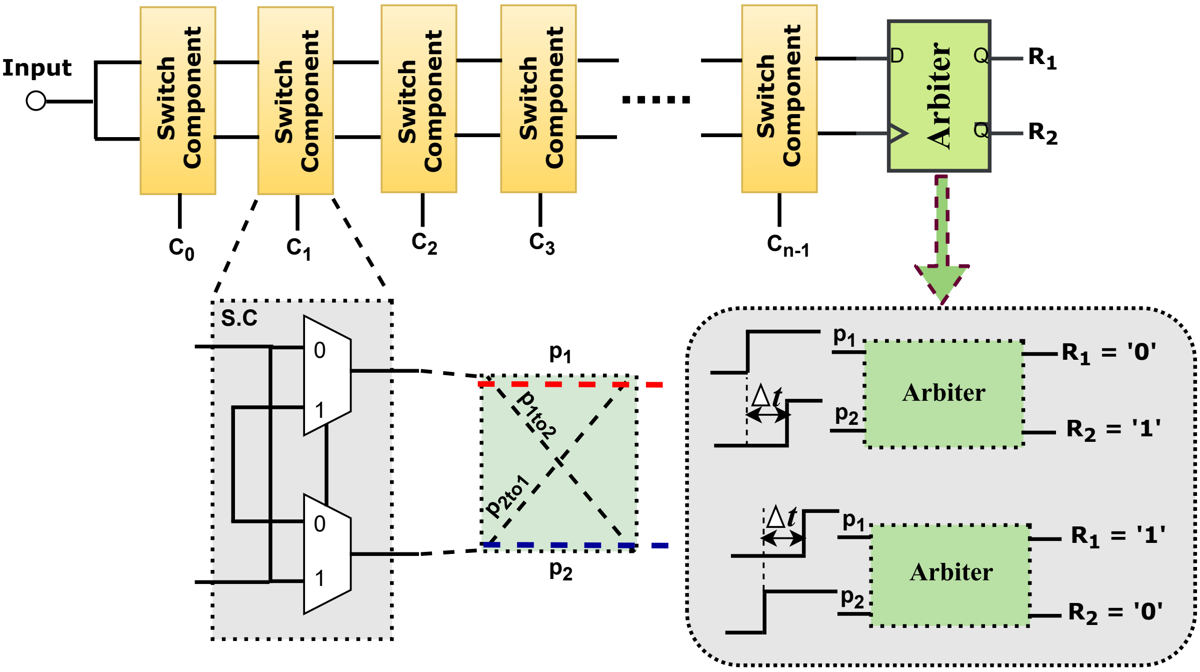


Figure 4.1 APUF design and operation of Arbiter

The proposed RC-FAPUF, shown in Fig.4.2, consists of SC, XoR gates, and an arbiter. The SCs are equipped with 2×1 Muxes that are involved in the arbitration process excited with challenge "C". Depending on the challenges the switching path is decided and corresponding path delays are evaluated. In RC-FAPUF, the design of SCs is intended with the combination of High Voltage Threshold (HVT) and Low Voltage Threshold (LVT) transistors to acquire PVs in delay variances. So, randomness is achieved by the arbitration mechanism when the XoR gate is placed in between the SCs. PUFs rely on minuscule manufacturing variations that result in device mismatch. The idea is that two (or more) transistors are identical by design and will have diverse electrical or physical characteristics. The crucial parameters that show a major impact on the PVs are Threshold Voltage (V$_T$), Drain–Source Current (I$_{DS}$), or Drain–Source Resistance(R$_{DSON}$), etc. Specifically, the reason for the improvement in reliability is achieved through the combination of LVT and HVT arrangement in the SCs produces uncertainty in the delay generation. Moreover, the uncertainty in the responses helps to make the proposed RC-FAPUF strong and reliable. The assessment of reliability is performed through the error rate calculated by the responses obtained from various challenges under different temperature and supply voltage circumstances. The major advantage of the proposed approach is the CRPs are very hard to predict by the intruder when performing unauthorized attempts in the cloning process. The positioning of the XoR gate at every end of SC can provide challenges either “0” or “1” based on the previous path delays that occurred from the prior SCs. The proposed structure is based on the Feed Forward (FF) mechanism that is introduced between SCs and the Feed-Back (FB) concept applied at the last SC to feed C$_0$.

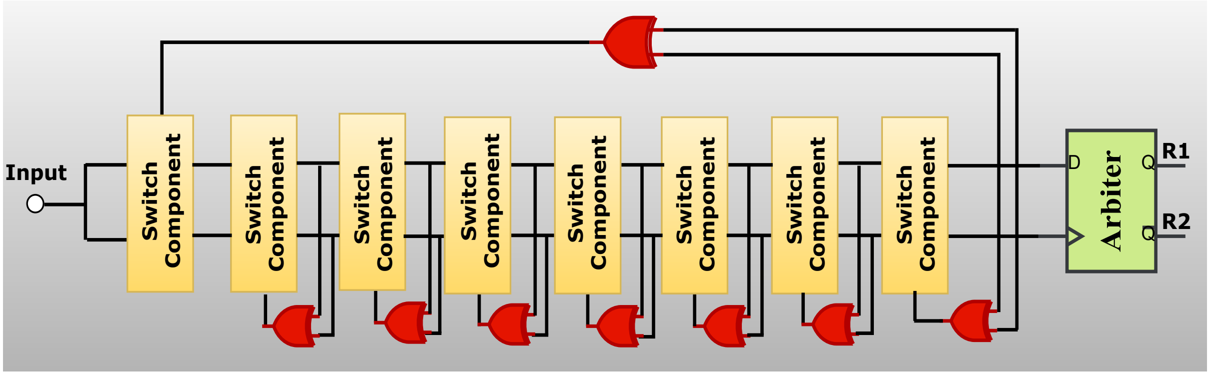


Figure 4.2 Proposed design of RC-FAPUF

In the operation of RC-FAPUF shown in Fig.4.3, the corresponding SCs are excited with recursive challenges C$_0$, C$_1$, . . . C$_{n-1}$ as “0”, “1”, . . . “0” are fed by XoR gates. Whereas the corresponding path delays P$_1$, P$_2$, P$_{1to2}$, and P$_{2to1}$ are determined regarding the PVs inherited in the transistors. The cumulative delay relationship for D^i_{path1} and D^i_{path2} is explored as

$$D^i_{path1} = \frac{1+C_i}{2}(t^i_{path1} + D^{i-1}_{path1} + D^{i-1}_{xor}) + \frac{1-C_i}{2}(t^i_{path2to1\_cross} + D^{i-1}_{path2} + D^{i-1}_{xor}) \quad (4.1)$$

$$D^i_{path2} = \frac{1+C_i}{2}(t^i_{path2} + D^{i-1}_{path2} + D^{i-1}_{xor}) + \frac{1-C_i}{2}(t^i_{path1to2\_cross} + D^{i-1}_{path1} + D^{i-1}_{xor}) \quad (4.2)$$

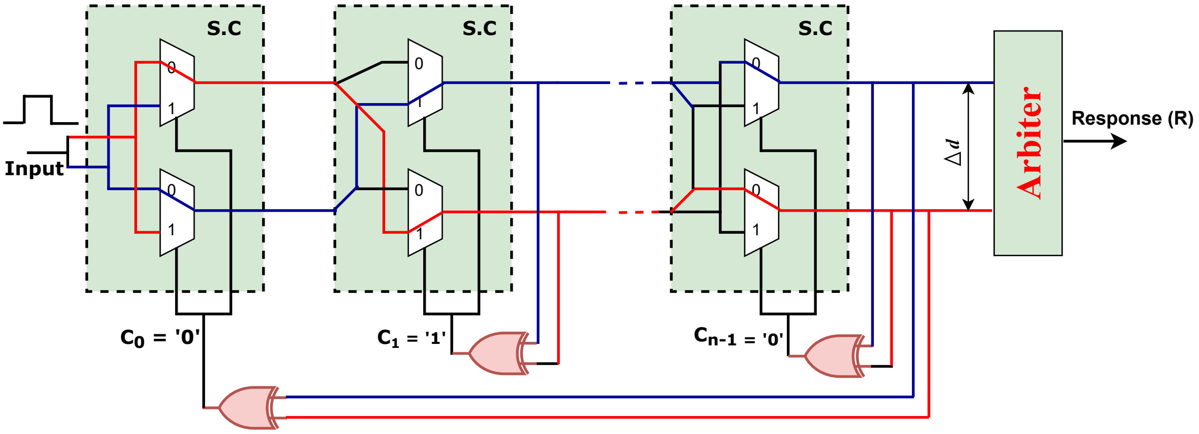


Figure 4.3 Operation of RC-FAPUF

where the delay D^{i-1}_{xor} represents the delay of the XoR gate contributed at every end of the SC and is additionally added to the previous path delays D^{i}_{path1} and D^{i}_{path2} to increase the randomness represented as Eq.4.1 and Eq.4.2. An arbiter compares the arrival time of P_1 and P_2 followed by Delay Difference (DD) ($\Delta d = d_2 - d_1$) that evaluates the response "R" based on the earlier path arrival, which should vary between instances or devices due to PV is expressed as,

$$R = \begin{cases} 0, & \text{if sgn(DD)} < 0 \\ 1, & \text{if sgn(DD)} > 0 \end{cases} \tag{4.3}$$

The recursion is achieved by the successful feed of the last SC response fed as challenge C_0. Special care must be taken in designing of SC and XoR gate to get rid of the delay mismatch and also noting down the challenges C_0, C_1, . . . C_{n-1} at every SC to evaluate the PUF metrics. The n-bit response "R_n" is generated by the recursive challenges C_0, C_1, . . . C_{n-1} using the following matrix:

$$\begin{bmatrix} I_n \end{bmatrix} \begin{bmatrix} C_0 & C_1 & C_2 & ... & C_{n-1} \end{bmatrix} = \begin{bmatrix} R_1 & R_2 & R_3 & ... & R_n \end{bmatrix}$$

In the proposed RC-FAPUF, the 16-bit responses are automatically fed as challenges to the SCs for which suitable CRPs are recorded. By following the specific time intervals, the 16-bit CRPs are measured and tabulated. In the process of secret key generation, these CRPs are subjected to PUF metric evaluation of diffuseness and reliability to employ them for identification or authentication applications. The former APUFs used manual or forced challenge feed mechanisms to feed the arbiters and were called dependent. Whereas in RC-FAPUF the challenges are produced from SCs outputs i.e. from P_1 and P_2 are fed as inputs to the XoR gates. So, the challenges are independent and uncertain because of the functioning of XoR gates. Thus, the dependency on manual feeding is avoided in the proposed RC-FAPUF mechanism. The automated challenge generation is implemented by taking care of delay matching between SCs and XoR gates. One or multiple SC components are considered as a single stage to increase the unpredictability in response generation.

The RC-FAPUF is not only suitable for IoT implementations but it can serve as a random number generator, create keys that are introduced during a manufacturing process within embedded security ICs, and utilized as a unique key/secret to support cryptographic algorithms (i.e. Message Digest (MD4), Secure Hash Algorithm (SHA)). For example, to generate a 16-bit key, if an 8-individual SCs are considered as a single stage then the design needs 16 2-stage SCs, and 2^8 XoR gates are required. In a secret key generation, the PUFs need to produce either different responses for different challenges (Diffuseness) or the same responses for the same challenges (Reliability) correspondingly for identification, and authentication applications. For example, in the mass production of ICs in an industry there is a need for unique ID generation to identify them. So, the categorization of ICs is done by a unique response (ID) generation concerning a random challenge. Whereas in device-to-user or user-to-device authentication, the PUFs need to generate specific CRPs that are recorded at different temperatures and supply voltage conditions. So, to recognize the device/user the PUFs could produce the same responses for the same challenges from permitted CRPs without fail. Otherwise, the authentication would fail and it seems to be faulty or expected to be hacked.

4.3 Evaluation of RC-FAPUF

The effectiveness of the PUF designs is assessed by the key metrics that are evaluated in this chapter, i.e. uniformity (u), diffuseness (D), and reliability (R). The proposed RC-FAPUF is implemented in UMC 180nm technology and simulations are performed using Cadence spectre. The characterization of 500 PUFs is performed through Monte Carlo simulations and evaluated the responses. Each RC-FAPUF cell is designed as 16-stage and active with 16-bit input “I” and excited with recursive challenges C_0 to C_{15}. Initially, challenge C_0 is set as "0" or "1" to start the arbitration process and the other challenges C_1 to C_{15} are followed by the feed-forward mechanism offered by XoR gates. The responses are evaluated under the nominal operating condition at 27°C with a 1.8V supply voltage.

4.3.1 Uniformity (u)

The percentage of "zero" (0's) and "one" (1's) in the response bit stream is measured by the uniformity of a PUF design, from which the probability of each value can be determined. The distribution of response bits will be identical between 1's and 0's if a design returns ideally random responses. From a security standpoint, having this feature prevents an attacker from presuming that a device's response is biased toward a certain value. To assess the uniformity, the Hamming Weight (HW) of response concerning the ratio of 1's and 0's and any biases in the PUF cell's design. The PUF's unpredictability is ensured by the uniformity of 50%. The distribution of "1s" and "0s" in the response vector $R_{i,j}$ are represented in Chapter 2 as Eq.2.1. Where $R_{i,j}$ is the "j^{th}" binary bit of an n-bit response for an "i^{th}" input. We evaluated the 16-bit responses from 500 RC-FAPUF instances at nominal operating conditions i.e. 27°C, 1.8V as shown in Fig. 4.5. The possibility of generating 1's for APUF [12], XFAPUF (chapter 3), and RC-FAPUF is 44.75%, 45.5%, and 47.32% respectively, which indicates that RC-FAPUF has high uniformity than other APUF designs and it is hard to attack.

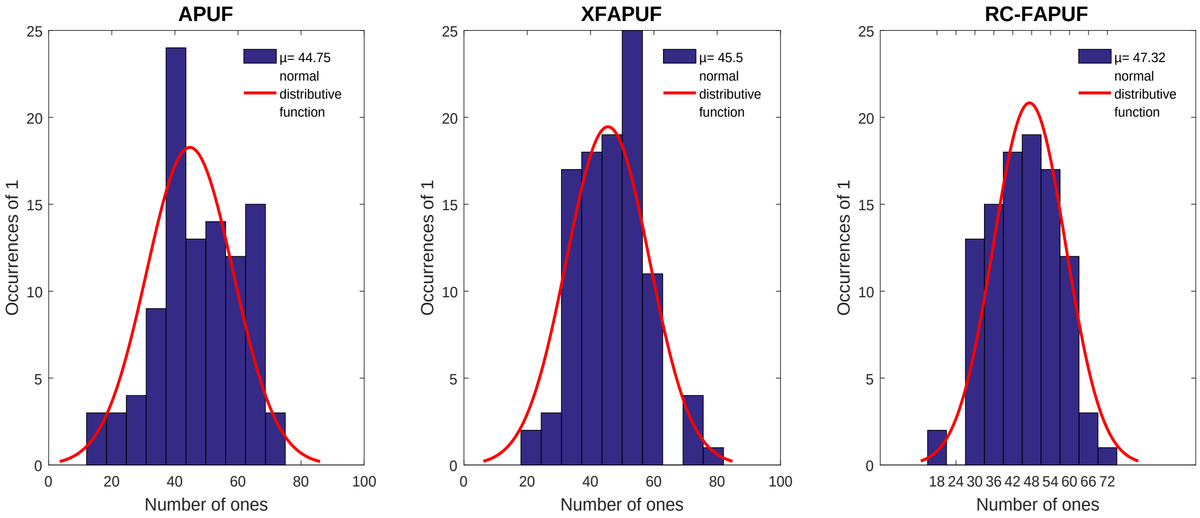


Figure 4.4 Uniformity of RC-FAPUF

4.3.2 Diffuseness (D)

Diffuseness can be evaluated by computing the mean of HD from the response vectors R_i and R_j in the same RC-FAPUF with various challenges applied nominally. It is represented in Chapter 2 as Eq.2.2. Where "l" stands for randomly selected response vectors picked from CRP space. R_i and R_j are two distinct n-bit response vectors obtained from two different challenges. Ideally, 50% diffuseness offers collision-free responses. We performed diffuseness of 16-bit responses from 500 RC-FAPUF instances at 27°C and 1.8V as depicted in Fig.4.6. The estimated mean (μ) for APUF [12], XFAPUF (chapter 3), and RC-FAPUF from obtained HD values 49.63%, 49.79%, and 49.89% are proving that the variations of instances are close to the ideal value i.e. 50%.

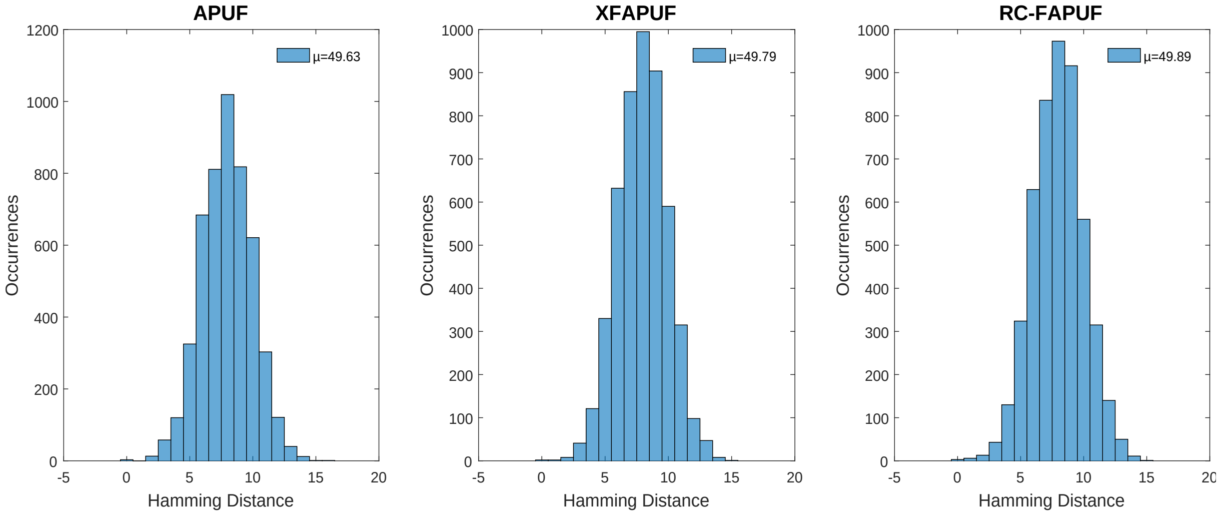


Figure 4.5 Diffuseness of RC-FAPUF

4.3.3 Reliability (R)

The robustness of a PUF under various environmental circumstances is determined by reliability. In general, a PUF should produce the same response to the same challenge in nominal conditions. Whereas the variations in temperature (°C) and supply voltage (V_{DD}) can have a major impact on the responses. To determine a PUF's reliability, the percentage of the number of irregular bits can be calculated to measure the average intra-chip HD of n-bit responses. Ideally, PUF responses stay consistent across many observations when faced with the same challenges. The evaluation of reliability is represented in Chapter 2 as Eq.2.4 and Eq.2.5. Where "m" stands for the number of trials that were observed and carried out on the same RC-FAPUF instance with the same challenge. The reference response $R_{i,ref}$ is measured at operating conditions i.e. 27°C, 1.8V, and R_i,t is the t^{th} measured response under a different temperature or supply voltage circumstances.

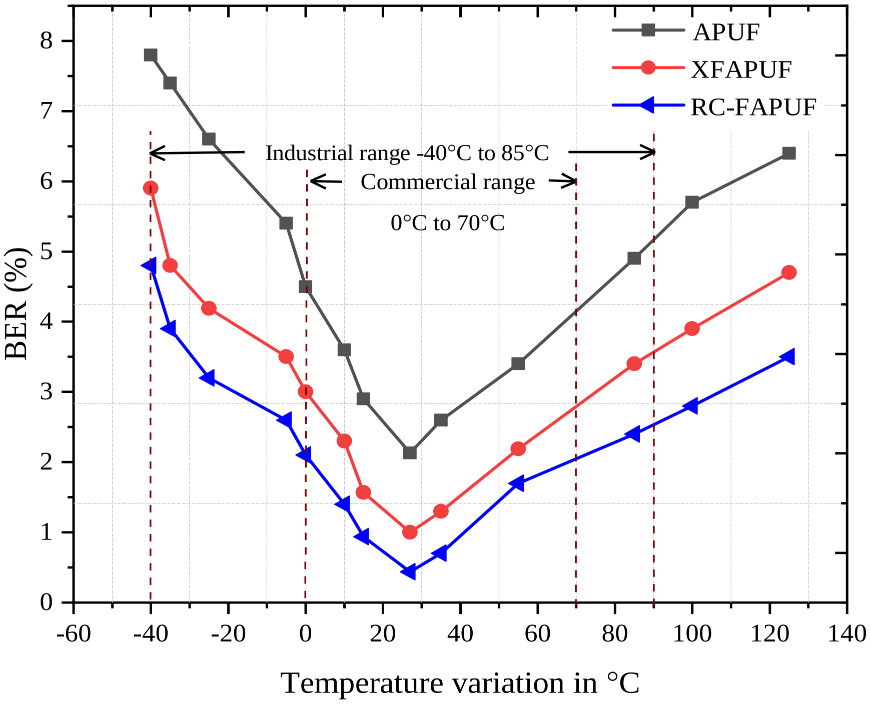


Figure 4.6 BER Vs Temperature in °C

The device's reliability is determined by the change in output responses when running at a different supply voltage or temperature. A PUF is reliable when its responses are consistent over time, with minute variations, and operated under intended circumstances. The reliability depends on the probabilistic behaviour of the PUF itself. The proposed RC-FAPUF enhances reliability through the arbitration mechanism employed between the SCs. If the PUF produces a very high value of reliability consistently, it is the fact that the proportion of the noisy bits presented in the responses is low. In any case, if the PUF produces more noisy bits it leads to misidentification. This reliability makes RC-FAPUF suitable for extensive custom cases that have very strict requirements.

The simulations are performed at various temperatures ranging from -40°C to 125°C. With temperature, the RC-FAPUF has an average dependability rating of 99.91%. The error rate was measured as 0.44% and 4.8% in nominal conditions and worst-case conditions respectively. Supply voltage change has a greater impact with 97.60% at 0.8V and

99.23% at 1.8V, respectively. So, whenever the temperature and supply voltage changes have occurred the proposed RC-FAPUF can withstand them. The error rate slightly increased because the minimum threshold voltage required to operate the transistor is measured as 12% at 0.8V and 3.81% at 1.8V. In the worst-case scenario, the temperature reliability of the 16-bit arbiter PUF is 99.89% on average, while the supply voltage reliability is 96.91% on average. We assess the Bit Error Rate (BER) of the 16-bit responses from 500 RC-FAPUF instances. Fig.4.6 and Fig.4.7 give the BER of the RC-FAPUF response as a function of temperature and supply voltage. If the PUF produces a very high value of reliability consistently, it is the fact that the proportion of the noisy bits presented in the responses is low. In any case, if the PUF produces more noisy bits it leads to misidentification.

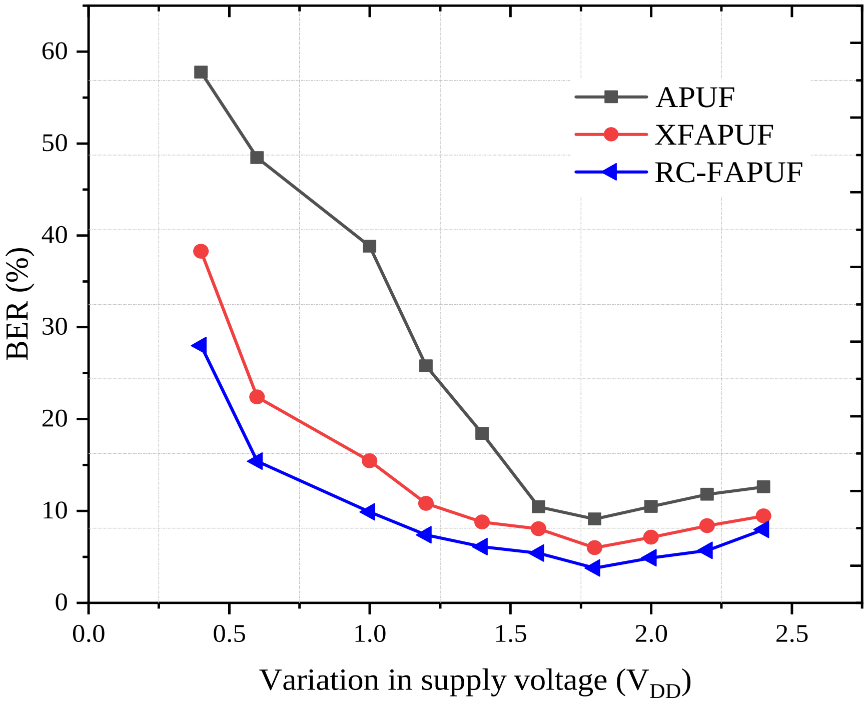


Figure 4.7 BER Vs Supply voltage V$_{DD}$

4.3.4 Security evaluation of RC-FAPUF

The proposed RC-FAPUF yields CRPs that are independent in an information-theoretic sense. It may lead to security problems such as a prediction attack, in which an attacker uses a previously known response bit to infer the value of an unknown response bit. In this section, the security analysis of RC-FAPUF is performed through LR and evaluates the prediction accuracy of the responses given in Fig.4.8. It also examines the security weaknesses of the PUF when it is employed in a hostile environment. When an adversary is supposed to be able to see the PUF's challenges, responses, and auxiliary data can attentively apply and observe suitable reactions. Whereas the proposed RC-FAPUF achieves 48% prediction accuracy when contrasted with the former PUF designs in [12] concerning the prediction analysis in security improvement to the ICs.

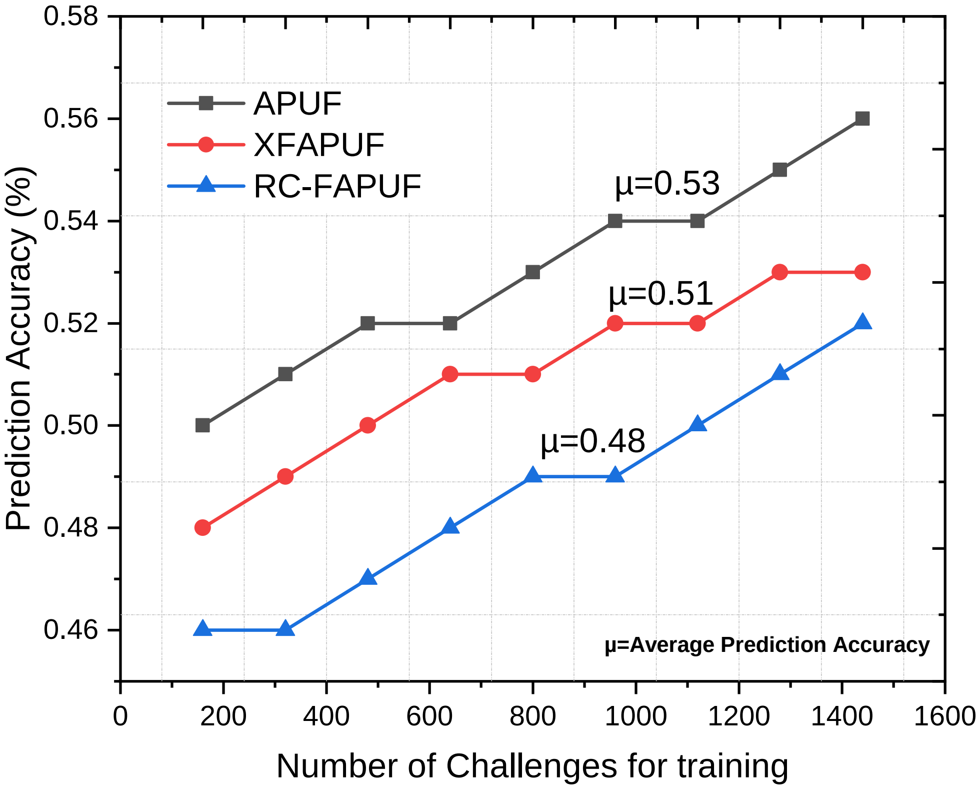


Figure 4.8 Prediction analysis of RC-FAPUF with LR

Moreover, the performance of the PUF topologies like APUF [12], XFAPUF (Chapter 3), and proposed RC-FAPUF are evaluated with some of the ML classifiers in Fig.4.9 to estimate the prediction accuracy. The classifiers such as Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), K-Nearest Neighbor (KNN), Two-class Bayes, and Neural Networks (NN) are applied to the selected CRPs to enhance the resistivity against ML attacks. The prediction accuracy of different classifiers applied on the RC-FAPUF is given in Tab.4.2. Among them, RF shows a prediction accuracy of 54.22%, which is better than other classifiers. Interestingly, the prediction rate obtained from 1600 CRPs of RC-FAPUF is reduced to 3.37%, and 1.01% when compared with APUF, and

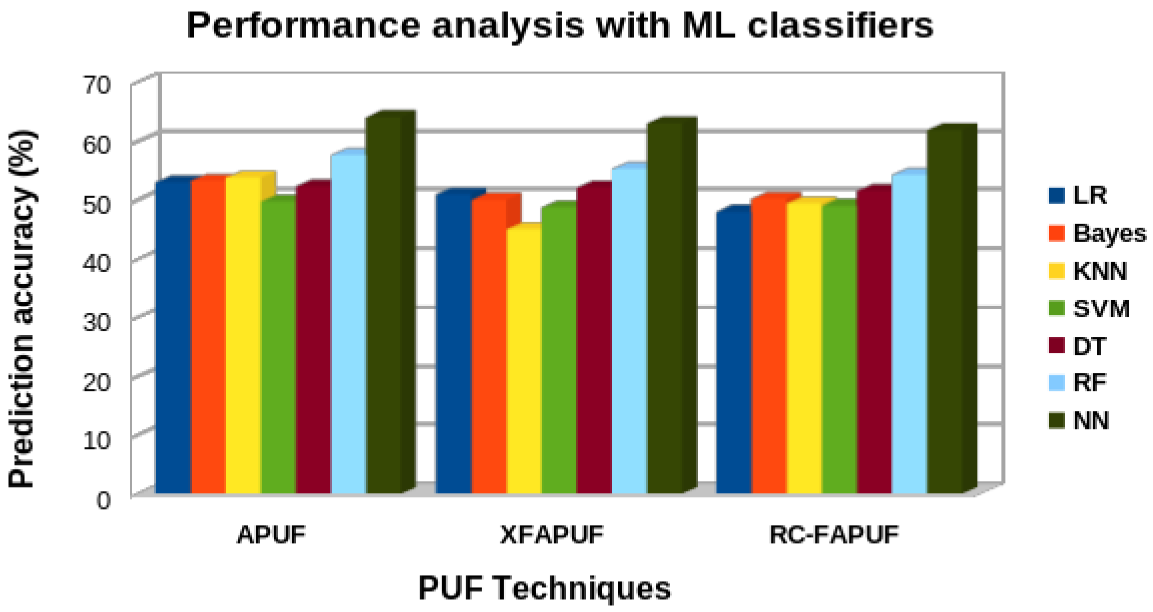


Figure 4.9 Performance analysis of PUFs with various classifiers

XFAPUF respectively. Indeed, when RC-FAPUF is evaluated with NN the prediction accuracy is increased up to 61.87%. Correspondingly, the prediction rate of APUF and XFAPUF is reduced to 2.19%, and 1.1%, respectively. So, the proposed RC-FAPUF is resilient to machine learning attacks with its uncertain behavior ensuing in the circuit.

Table 4.2 RC-FAPUF evaluation with ML classifiers

	SVM	DT	RF	KNN	Bayes	NN
No. of CRPs (%)	1600	1600	1600	1600	1600	1600
Prediction Accuracy (%)	49	51.56	54.22	49.38	50.19	61.87

4.3.5 Analysis and Comparison

The quality metrics of PUF dependability at various temperatures and supply voltages are presented in Tab.4.3 and Tab.4.4. The comparison of the proposed RC-FAPUF in terms of major PUF metrics is shown in Tab.4.5. The results are obtained using 500 CRPs to test uniformity (u), diffuseness (D), and reliability (R). This comparison includes the most distinctive PUFs published in the last fifteen years. The RC-FAPUF has better uniformity compared with the conventional APUFs [4,12,70], FF-APUFs [13], DAPUF [24], and BRPUF [45]. However, it is generally better compared with the XFA-

Table 4.3 RC-FAPUF quality metrics at different temperatures

	-40°C	**0°C**	**27°C**	**85°C**	**125°C**
Intra-HD (%)	99.03	99.56	99.91	99.52	99.30
BER (%)	4.8	2.1	0.44	2.4	3.5

Table 4.4 RC-FAPUF quality metrics at various V_{DD}

	0.8 V	**1.2 V**	**1.6 V**	**1.8 V**	**2 V**
Intra-HD (%)	97.60	98.51	98.92	99.23	98.58
BER (%)	12	7.4	5.4	3.81	4.9

PUF (Chapter 3), CMOS PUF [54], Sub-threshold PUF [55], and X-point PUF [66]. The diffuseness of the proposed RC-FAPUF results is 49.89% when compared with the conventional APUF is 46.81% by [3], 49% by [14], and 49.79% by [16] respectively. The X-point [66] and iPUF [72] concepts achieve higher diffuseness but have to sacrifice reliability and BER. When compared to the PUF designed in [12], the RC-FAPUF's reliability over the temperature and supply voltage variation is increased by more than 1.5% and 1.3%, respectively. When temperature and supply voltage fluctuate, the BER degrades by 37% compared to [72]. The RC-FAPUF design exhibits good reliability results of 99.91% as the traditional PUF design [12,70] on an ASIC. The proposed RC-FAPUF has a memory function restriction, yet it excels in higher reliability than other state-of-the-art PUF designs [32,54,72].

4.3.6 Performance analysis

For a 16-bit challenge feed to distinguish RC-FAPUF instances based on the feed-forward arbiter scheme, it takes 0.2s for a single response. To generate 1600 CRPs across 16-stage RC-FAPUF positioned by delay circuit is sufficient to produce PVs required to propagate responses between SCs and evaluate fast-rising edge response at an arbiter. It takes about 3.2s to extract 16-bit keys from 1600 randomly generated CRPs across 16-stage RC-FAPUF instances. Even though the PUFs are fast in the key generation they are suffering from power and computing limitations. Perhaps PUFs utilize adequate computing power, and a small footprint to work effectively in stressful or vulnerable

Table 4.5 Comparison of metrics of different PUF designs

References	**PUF Design**	**Technology**	**Uniformity (Ideal-50%)**	**Diffuseness (Ideal-50%)**	**Reliability (Ideal-100%)**	**BER(%)**
Idriss et al., 2021 [4]	APUF	65nm	47.22%	46.81%	NA	4.79
Lee et al., 2004 [12]	APUF	180nm	23%	NA	$95.20\%^t$, $96.30\%^v$	NA
Lim et al., 2005 [13]	FF-APUF	180nm	38%	NA	90.20%	NA
Majzoobi et al., 2008 [24]	DAPUF	–	55.01%	49%	NA	
Laguduva et al., 2019 [43]	TCRO	65nm	52.45%	NA	NA	NA
Li et al., 2021 [51]	DFFPUF	65nm	NA	NA	98.82%	$2.6\%^t$, $1.5\%^v$
Jaya et al., 2018 [54]	CMOS	65nm	50.04%	64.09%	98.3%	1.7
Tao et al., 2016 [55]	Sub-T	45nm	50%	NA	98.10%	NA
Khan et al., 2020 [52]	CMQC	65nm	50.25%	64.03%	98.27%	2.07
Khan et al., 2020 [52]	VMQC	65nm	50.02%	63.92%	97.72%	3.95
Kumar et al., 2008 [45]	BR-PUF	SPICE	14.80%	NA	99.20%	NA
Gu et al., 2019 [32]	B-PUF	65nm	49%	NA	$80\%^t$, $95\%^v$	NA
Tripathy et al., 2021 [70]	MARPUF	65nm	48.23%	NA	95.16%	NA
This work	***RC-FAPUF***	***180nm***	***47.32%***	***49.89%***	***$99.91\%^t$, $99.39\%^v$***	$1.31\%^t$, $9.75\%^v$

t = temperature variation, v=supply voltage variation, NA = Not Applied, - = Not Mentioned

environmental conditions that pertain to repeatability and evolvability. PUFs produce a key discrepancy rate that specifies the number of key bits that are different between the two users which results in high randomness.

Cryptographic algorithms for authentication require large memory resources for storing keys, leading to high computational complexity. Also, they require scalable processing time for secure data transmission in real time to implement cryptographic applications. PUFs have good statistical properties that introduce lightweight secure authentication, without the need for cryptography or secure memory. PUF designs are lightweight, cost-efficient, and ubiquitous with little resource overhead making them possible to adapt after deploying the IoT devices and updating them to new counterattacks.

Specifically, to implement identification, verification, and authentication applications like healthcare, industry, wearable implants, telemedicine, Augmented Reality (AR), etc. in normal and foggy or cloudy conditions need response time of 1s to 5s and 9s to 25s respectively. This is fast enough as implemented in IoT devices to produce cryptographic keys for authentication and access control applications. This process is boosted when the circuit produces instant PVs and delay circuits equipped with fast-switching transistors in the SCs. Consequently, the delay variations are produced, and the corresponding responses are recorded parallelly across arbiters and are tabulated for further evaluation of PUF security. Certainly, the key length may be increased to develop the complexity and presumption of CRPs against attacks. The proposed RC-FAPUF stands reliable due to its indeterministic behaviour while achieving 1.31%, and 9.75% BER rates concerning the variations in temperature and supply voltage respectively. The layout of the final system designed in UMC 180nm excluding the pad ring is shown in Fig.4.10. It contains 16 sets of the arbiter circuit generating a 16-bit response with the dimension of 558μm × 270μm, which gives an approximate area of 0.15mm^2 and is designed for IoT-enabled applications.

4.4 Summary

This chapter provided a robust PUF topology based on the feed-forward APUF mechanism. The RC-FAPUF is fed by the automated or independent challenges and realized through PVs that occur in the SCs. The structure of the PUF increases the complexity of the arbitration and makes it more difficult to model attacks. The experimental evaluation of RC-FAPUF provides uniformity, diffuseness, and reliability of 47.32%, 49.89%, and 99.91% respectively, better than that of state-of-the-art designs. Moreover, it is highly resistant to ML attacks when LR and ML classifiers are applied

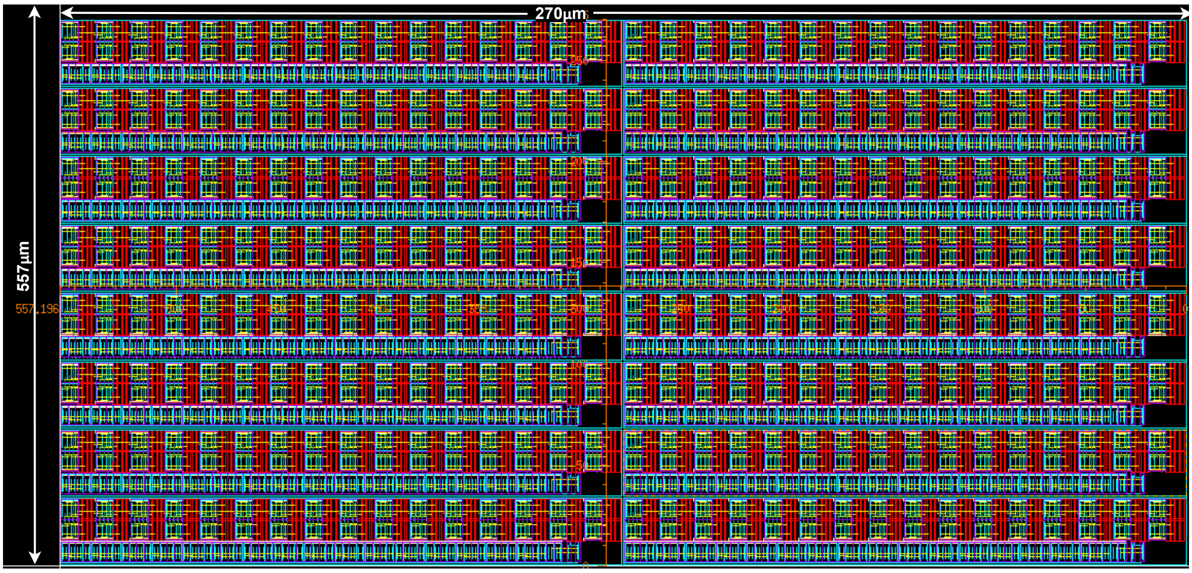


Figure 4.10 Layout of RC-FAPUF

achieving the best prediction accuracy of 48% and 52.7%, respectively.

The RC-FAPUF significantly improves the reliability of CRP-based PUF designs and also has the potential to implement security in IoT-enabled devices for identification and authentication. Despite being strong and highly random the RC-FAPUF doesn't have a memory function to store the responses for authentication applications. So, these results prove that RC-FAPUFs could be considered as strong PUF when key generation is required for identification or authentication applications. The next chapter will cover the design of weak PUF with pre-existed or simple circuits that are suitable for identification applications.

The next chapter will describe the design and implementation of weak ReOPUF, which is considered for identification applications that make use of frequency variations inherited as PVs and generate the key with respect to the challenge feed. Moreover, the evaluation metrics also performed with respect to the CRPs.

Chapter 5

Relaxation Oscillator PUF (ReOPUF)

Arbiter-based PUFs work on the principle of the conventional delay-based approach realized between two symmetrical engaged paths, while oscillator-based PUFs work on frequency differences observed among a group of identical oscillators arranged in a specific pattern. In this chapter, a novel PUF is presented based on the Relaxation Oscillator PUF (ReOPUF) topology for device identification or authentication that can produce unique, unpredictable, and reliable keys to improve the robustness against the supply voltage and temperature variations. Besides, we proposed an LDO feed challenge mechanism to increase the randomness. However, the ReOPUF is designed to generate a 4.4 MHz frequency that is suitable for powering up IoT sub-systems including sensors while protecting them from malicious attacks. The contributions of this chapter are,

- We propose a Relaxation Oscillator PUF design which we refer to as ReOPUF. The ReOs in ReOPUF are designed to explicitly produce the low frequency i.e., 4.4 MHz suitable for IoT sensor node security.

- An LDO-based challenge generation mechanism is proposed to attain enhanced randomness in the ReOPUF.

- The respective PUF quality metrics are evaluated and analyzed for the proposed PUF to demonstrate the high reliability in key generation.

- We perform extensive simulations (in 65nm CMOS technology) to compare the proposed PUF with conventional RO PUFs in terms of PUF quality metrics with respect to supply voltage and temperature variations. We evaluate two more quality metrics, namely, Diffuseness (D) and Uniformity (u). We compare the strong CRP generation of the proposed ReOPUF with that of arbiter PUF. Further, we perform the entropy and correlation analysis.

5.1 Ring Oscillator (RO) PUF

A conventional Ring Oscillator (RO) PUF is shown in Fig.5.1 for key generation [33]. It consists of N identically designed ROs (RO1, RO2, . . ., RON), two multiplexers, two counters, and one comparator. Each RO oscillates at a different frequency due to manufacturing process variations, even though ROs are designed with an equal number of inverter stages [34]. An N-bit multiplexer can select a pair of frequencies generated from the RO stage based on the challenge input (through selection lines). The counters are used to get the count of the pulses obtained from the MUX stage. The difference in the pulses between the two counters is verified by the comparator and a response is generated. For example, if counter 1 output is greater than that of counter 2 then a '1' is generated, otherwise, a '0'. In this manner, an N-bit key can be obtained from N copies of RO PUF.

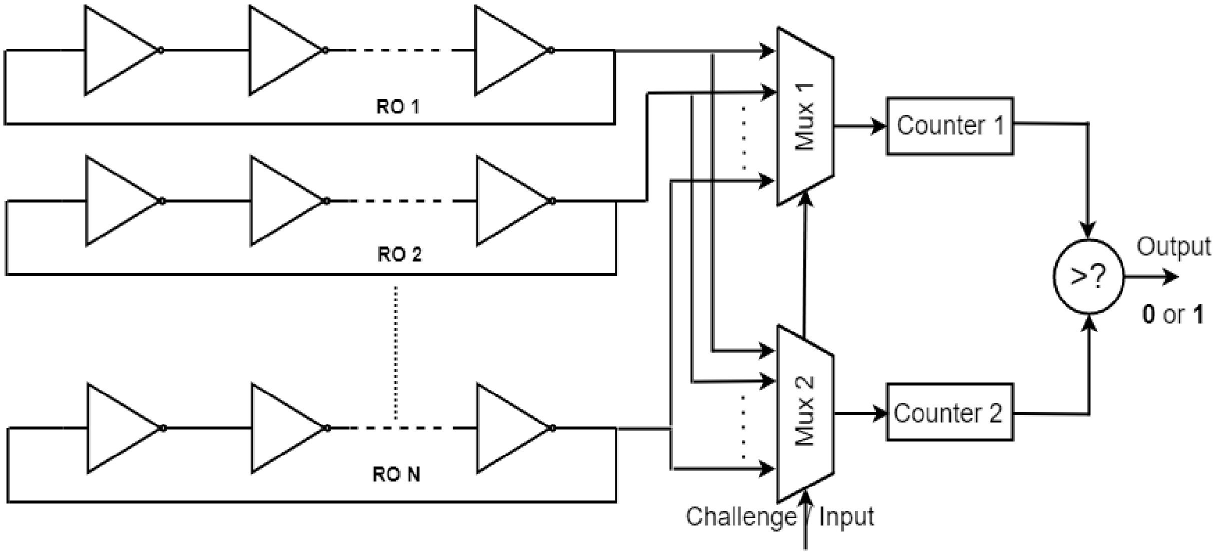


Figure 5.1 Ring Oscillator PUF

5.2 Relaxation Oscillator PUF (ReOPUF)

A PUF circuit can able to generate a large number of challenge-response pairs (CRPs) using different PUF designs which are unique and unpredictable. The generated responses should be different for each challenge and different PUFs can generate individual responses for the same challenge. PUF has quality measures to evaluate randomness, uniqueness and, reliability. Randomness is measured from the equal distribution of 1's and 0's generated from the PUF. Uniqueness is evaluated by the inter-HD should be ideally of 50%, which represents the difference between PUF responses. Reliability is measured by the intra-HD should be ideally 0%, when applied with the same challenge on the same PUF. Moreover, reliability should also depend on variations like temperature, supply voltage, ageing effect, noise, environmental effect, and so on.

An oscillator is a circuit that generates a repetitive waveform of fixed amplitude and frequency without any external input signal. Oscillators are used in radio, television, computer, and communications. Relaxation Oscillator (ReO) shown in Fig.5.2 is specifically preferred for low-frequency applications such as waveform generators, triggering circuits, etc. ReO is considered as a non-linear oscillator that can generate a periodic non-sinusoidal waveform (either voltage or current) at its output such as a square wave, triangular wave, etc. It is also called a non-sinusoidal waveform generator. ReOs do not require external components and are easily implemented in CMOS technology. In addition, ReOs are capable of producing sustained square wave oscillations determined by the time constant RC even though the frequency accuracy is restricted by the tolerances of on-chip capacitors and resistors. ReOs consume less current and power to generate jitterless clock generation. A major drawback of ReO is its susceptibility to process and temperature variations. By the use of polysilicon resistors and the utilization of electron mobility in a MOS transistor offers an accurate frequency reference subjected to achieve fewer process variations and frequency stability over temperature. Most of the reported oscillators suffer from external components, reliability, and excessive power consumption and are not suitable for low-frequency applications requiring long battery lifetime.

5.2.1 Design considerations

To design the required ReOPUF operated with a frequency of 4.4 MHz, the following considerations shown in Tab.5.1 are preferred to achieve the specific key generation

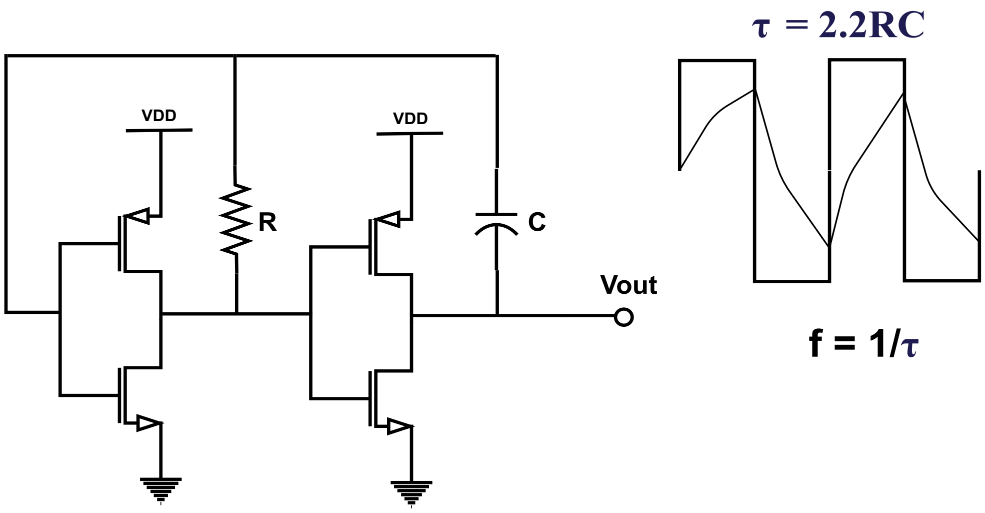


Figure 5.2 Basic Relaxation Oscillator

mechanism suitable to power management circuits, sensors etc.

Table 5.1 Specifications for ReOPUF

Design Parameters		
Aspect ratio (nm) (Oscillators)	PMOS	50/65
	NMOS	10/65
	R	10 kΩ
	C	10 pF
Aspect ratio (nm) (32x1 Muxes)	PMOS	240/65
	NMOS	240/65
Aspect ratio (nm) (Counter)	PMOS	600/65
	NMOS	100/65
V_{DD} (V)	1.2	
Input (I)	16-bit	
Challenges (C)	"n-bit" (Depends on stages)	
Responses (R)	32-bit	
Frequency (f_{out})	4.4 MHz	

5.2.2 Implementation of ReOPUF

The circuit can be designed with an energy-storing device such as a capacitor or inductor which charges and discharges continuously to produce a cycle regarding a predetermined threshold voltage. The frequency (f) or period (t) of oscillation with ReO shown in Fig.5.3 is determined by the time constant ($\tau = 2.2RC$) of the capacitive or inductive circuit. Likewise, the frequency is calculated for the basic ReO is f=1/τ i.e., 4.4 MHz. ReOs are widely used to produce internal clock signals in several low-frequency digital circuits. ReOs are also found in applications of thyristor triggering circuits, oscilloscopes, etc. ReOPUF is a hardware PUF that exploits PVs occurring in the silicon manufacturing process to produce reliable keys. The random number extracted via ReOPUF is unique and unclonable and can be used as a silicon "fingerprint" for a wide range of security purposes, including encryption, identification, authentication, and security key generation.

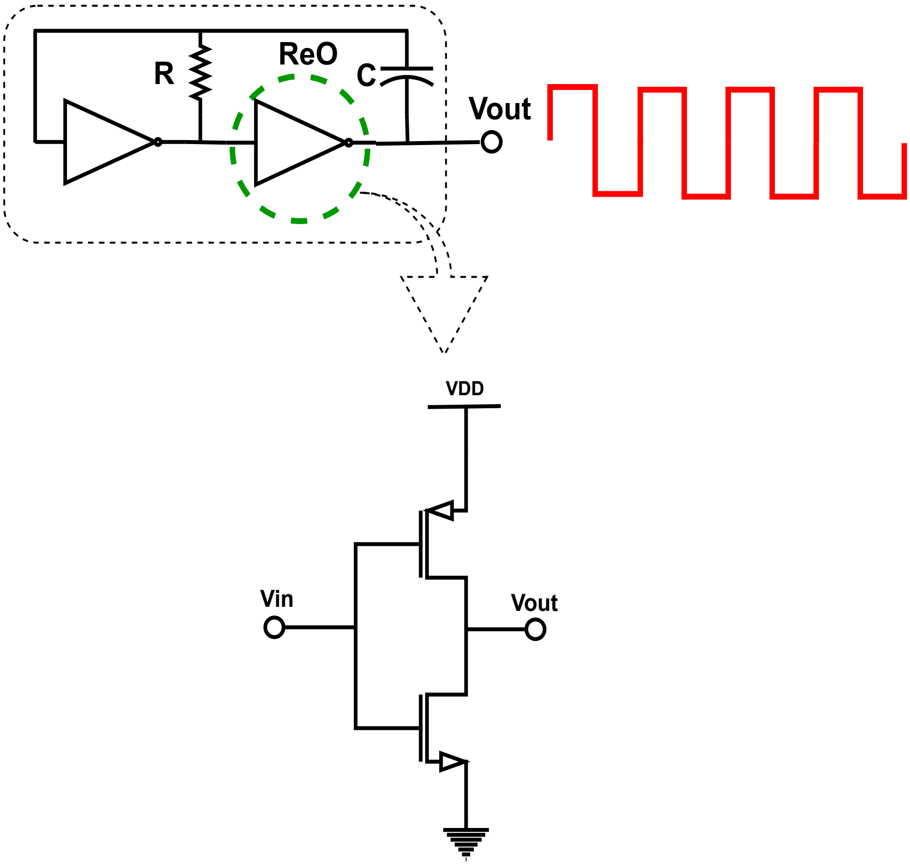


Figure 5.3 Proposed design of ReOPUF

5.2.3 n-stage ReOPUF

Fig.5.4 presents ReOPUF consisting of 'N' identical ReOs (ReO1, ReO2,....., ReON), two n-bit multiplexers (MUXs), two counters, and a comparator. Each ReO generates a unique frequency when fed with different challenges or inputs. The frequency of 4.4 MHz is specially designed and generated for IoT sensor node applications. The MUXs can produce non-identical frequencies due to the process variations of the device, even though they are designed with the same device characteristics. The challenge of input applied to both MUXs selects one pair of ReO the frequency difference of which will determine the output. The obtained frequency difference in terms of 1-bit response (either 0s or 1s) is considered for key generation. The counter can help to count the number of oscillations of selected ReO pairs processed from MUXs in a fixed time interval. The pulse counts from the counters are compared with the comparator, which gives the response '0' or '1'.

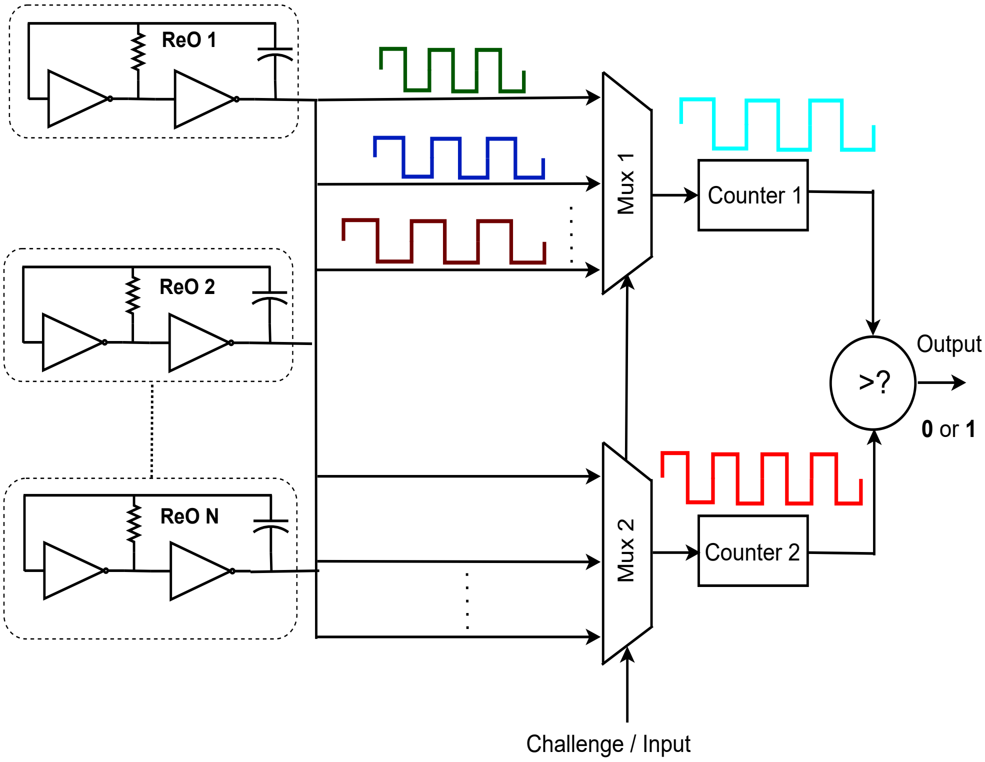
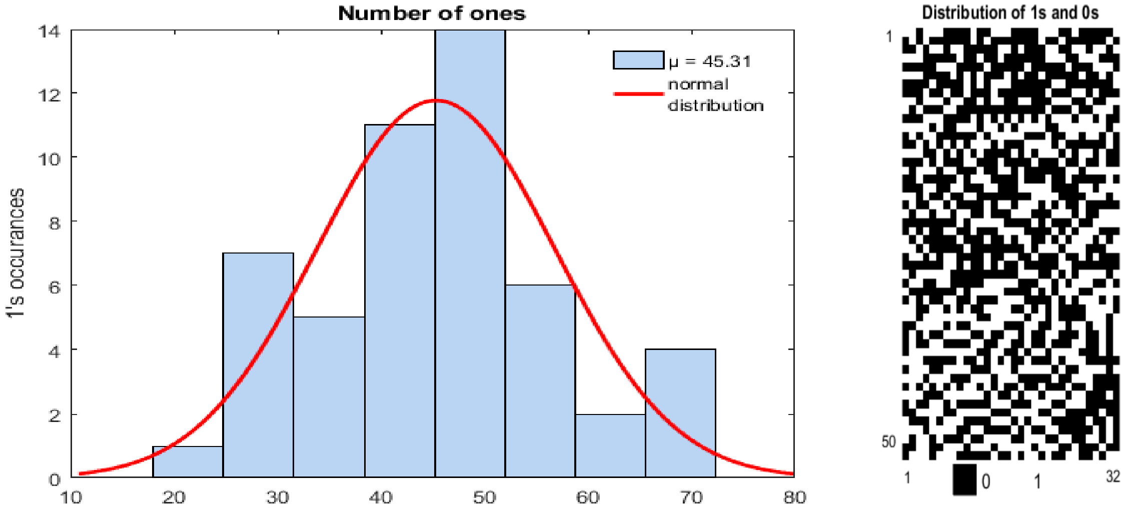


Figure 5.4 n-stage ReOPUF

5.2.4 Evaluation of ReOPUF

The proposed ReOPUF circuit is implemented in UMC 65nm technology and simulated with Cadence Spectre. To perform the characterization of 50 different PUFs, 100 runs of Monte-Carlo simulations are performed. During simulation, intra-die and inter-die PVs are generated to evaluate the responses. Each 32-stage ReOPUF becomes active with the 5-bit challenge or input (C_0 to C_4) and is evaluated under the nominal operating conditions of 27°C and 1.2V supply voltage. The performance of the ReOPUF is measured and evaluated with the following metrics as defined by NIST.



(a) Distribution of 1's

(b) Pixel representation

Figure 5.5 Uniformity of ReOPUF

5.2.4.1 Uniformity (u)

Uniformity is the measure of the distribution of '1s' and '0s' in the response vector $R_{i,j}$ is described in Chapter 2 as Eq.2.1. Where, $R_{i,j}$ is the j^{th} binary bit of an n-bit response for an i^{th} input. An ideal PUF should have equal probabilities for '1' and '0' in response, i.e., 50%. We evaluate the 32-bit responses from 50 ReOPUF instances at nominal operating condition i.e., 27°C, 1.2V is shown in Fig.5.5. The distribution of 1's and 0's generated by the ReOPUF is shown in Fig.5.6 as a pixel distribution with a white pixel interpreted as a '1' and a black pixel as a '0'. The probability of generating 1s is 45.31%, which indicates that ReOPUF output is not predictable and it is hard to attack.

5.2.4.2 Diffuseness (D)

Diffuseness (shown in Fig.5.6) is the degree of variation observed in the same ReOPUF with different challenges applied nominally. It can be measured by calculating the mean of HD from the response vectors obtained as 49.53%. It is defined in Chapter 2 as

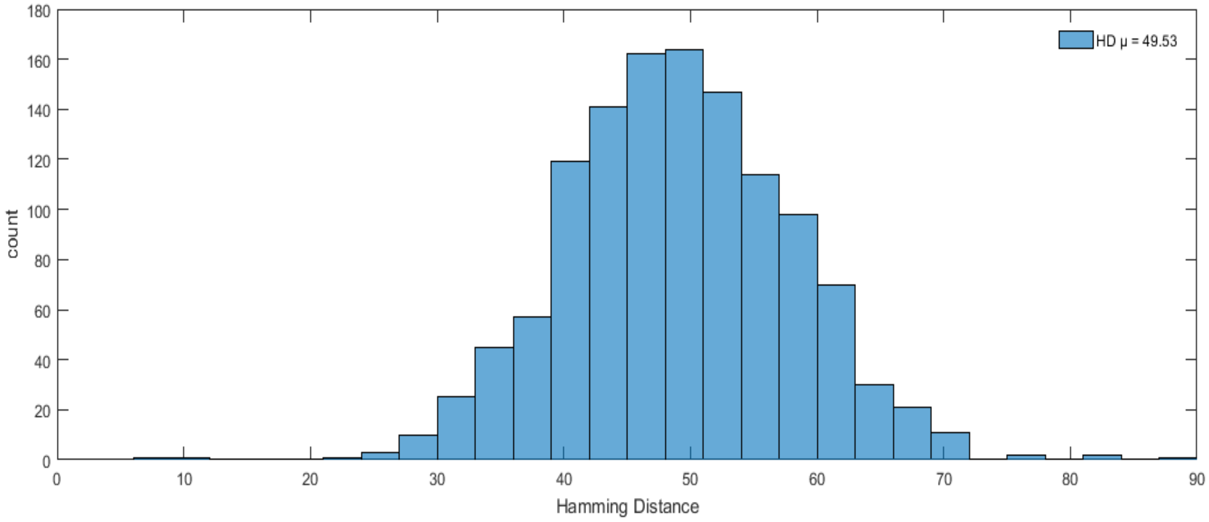


Figure 5.6 Diffuseness of ReOPUF

Eq.3.2. Where 'l' represents a randomly selected response vector from CRP space. R_i and R_j are two different n-bit response vectors obtained from two different challenges.

5.2.4.3 Uniqueness (U)

The randomness in different PUF responses reflects the performance in terms of uniqueness. Ideally, the probability of each response (i.e., '0' or '1') generated by identical PUFs with the same challenge should be 50%. Uniqueness (shown in Fig.5.7) measures inter-chip variation among different ReOPUF instances implemented with the same challenge. It can be calculated with inter-chip hamming distance (inter-HD) 49.22% as described in Chapter 2 as Eq.2.3. Where R_i and R_j are two different n-bit response vectors obtained from the same challenge and 'm' represents different ReOPUF instances with the same challenge.

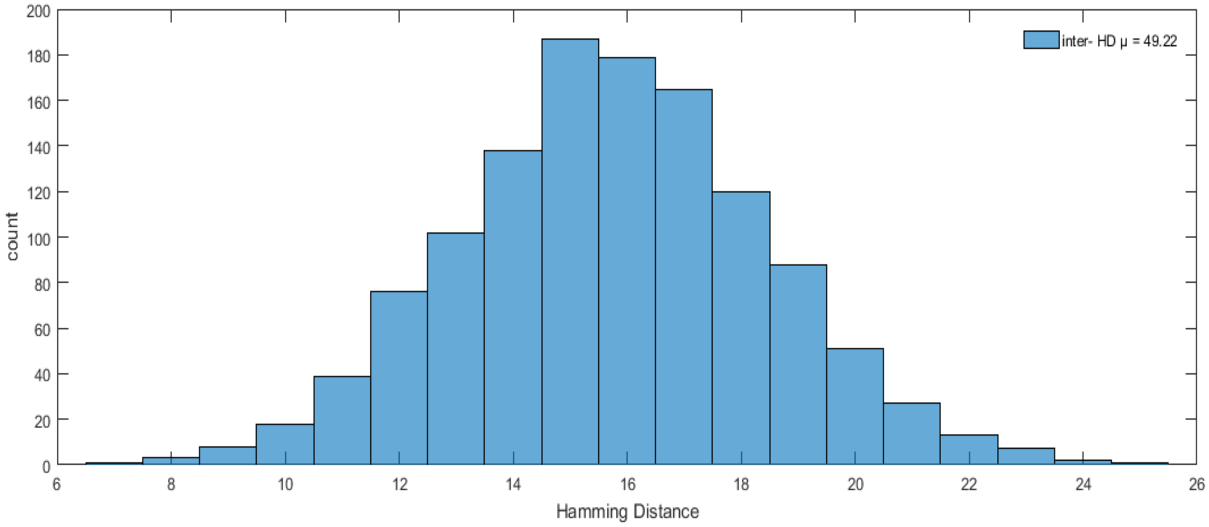


Figure 5.7 Uniqueness of ReOPUF

5.2.4.4 Reliability (R)

A PUF should generate the same response in any state for the same challenge applied. Unfortunately, variations in the supply voltage or temperature can change the behaviour of the IC in the form of circuit delay and lead to unpredicted responses. Therefore, the same response bits should be produced at different operating conditions. Reliability is measured by *intra-HD*, which is performed between two n-bit response vectors generated from the same PUF instances with the same challenges. It can be calculated as represented in Eq.2.4 and Eq.2.5 of Chapter 2. Where 'm' represents some measured trials applied on ReOPUF instances with the same challenge. $R_{i,ref}$ is the reference response measured at normal operating conditions (27°C and 1.2V), $\mathrm{R}_{i,t}$ is the t^{th} measured response at a different operating conditions. We measure the reliability of the 32-bit responses from 50 ReOPUF instances in different operating conditions.

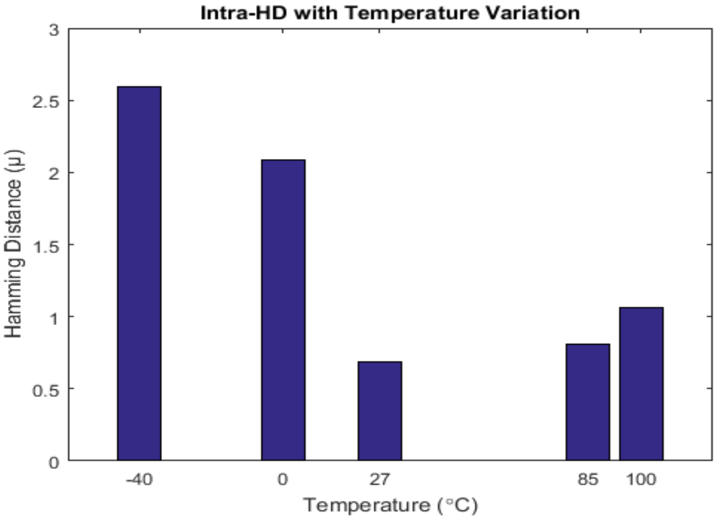


Figure 5.8 Reliability of ReOPUF temperature variation

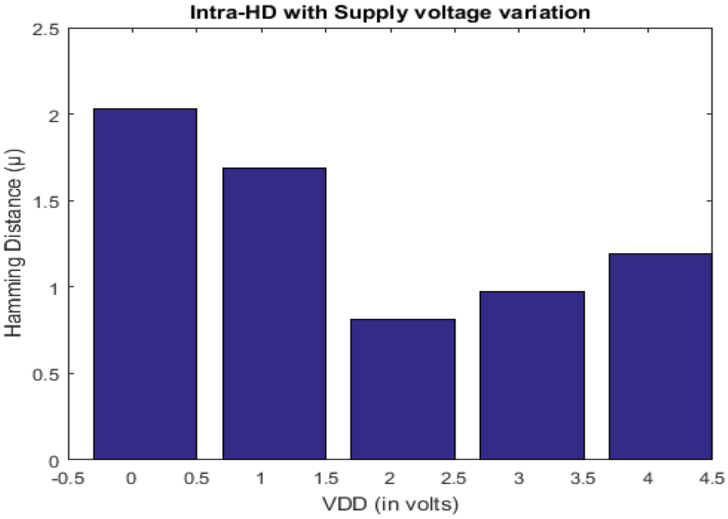


Figure 5.9 Reliability of ReOPUF with V_{DD} variation

5.2.5 Security evaluation

PUFs are specifically proposed for security applications that can withstand attacks under various threat models [75]. A PUF uses a CRP mechanism derived from inbuilt process variations performed by the ICs. Invasive attacks (such as reverse engineering attacks) may alter the physical properties of the device resulting in the breaching of CRPs. However, PUF-based systems may be susceptible to two threat models such as PUF for authentication and PUF for secret key generation. If a PUF is used for authentication, the attacker can perform different trials to extract valid CRPs which can be used to crack the PUF function. If it is a secret key generation the attacker can concentrate on the

PUF response pairs by exploiting the PUF weakness. In this section, we evaluate the security of PUF by performing the entropy analysis on the responses.

5.2.5.1 Entropy Analysis

Entropy can be used as a measure of the unpredictability of a response key from PUFs, though the uncertainty from process variations is immeasurable. For example, a 32-bit key that is uniformly and randomly generated has 32 bits of entropy. It also takes (ignoring actual computing) 2^{32}-1 guesses to break by brute force. Entropy fails to capture the number of guesses required if the possible keys are not chosen uniformly. Entropy is measured for ReOPUF generated 32-bit response when varying with different temperature and supply voltage variations as shown in Fig.5.10 and Fig.5.11. From the analysis, we assure that the ReOPUF responses offer high uncertainty and high average information carried out for communication. It is observed that at different temperatures the entropy varies from 2.39 to 2.48, while at different supply voltages, it varies from 2.41 to 2.44.

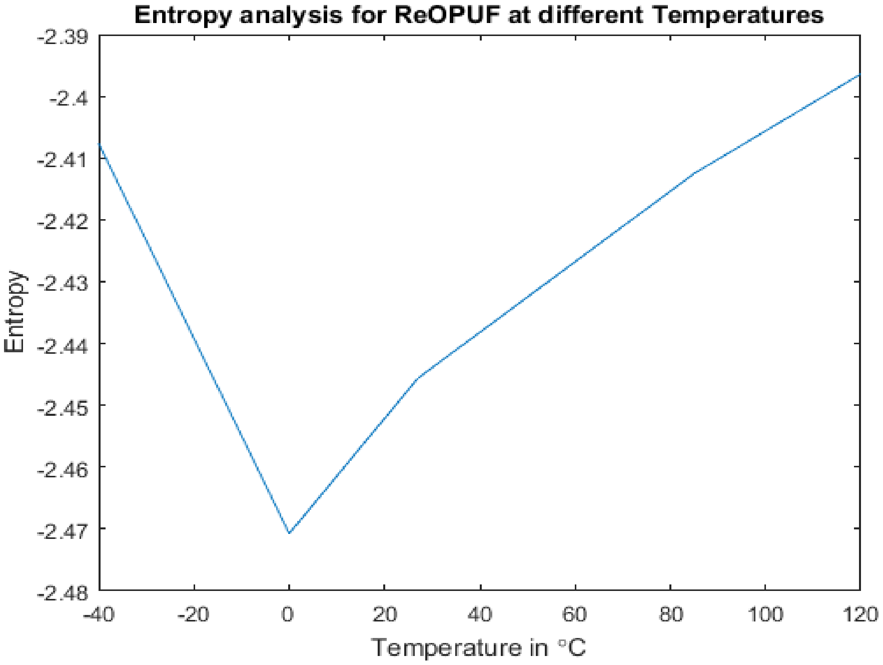


Figure 5.10 Entropy of ReOPUF with temperature variation

5.2.5.2 Correlation Coefficient Analysis

The correlation coefficient is calculated for every PUF instance to determine if there is any correlation among the PUF cells. If zero correlation is attained, then there is no

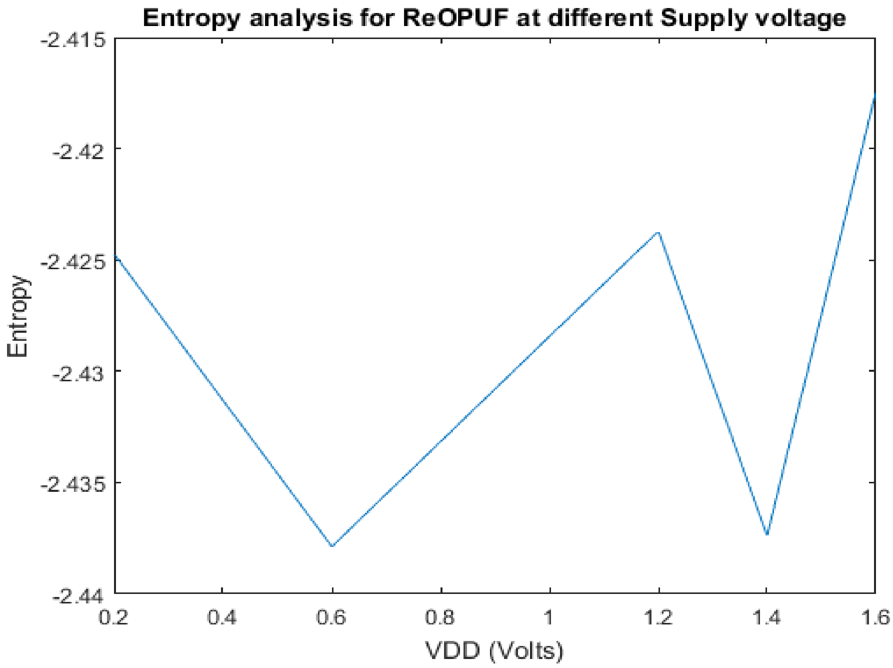


Figure 5.11 Entropy of ReOPUF with supply voltage variation

such dependency exists among PUF cells. In the occurrence of -1 or +1 attainment there exists a linear dependency among the PUF cells i.e., weakly dependent (-1) or strongly dependent (+1) based on the CRPs generated by PUFs. For this test, 32 PUF cells are used. Pairwise, the covariance of two cells is divided by the product of their standard deviations as shown:

$$\rho(X, Y) = \frac{E[(X - \mu X)(Y - \mu Y)]}{\sigma_x \sigma_y} \tag{5.1}$$

where ρ is defined as the correlation coefficient of two independent variables X and Y, μ and σ represent the mean and standard deviation of the independent responses obtained from the PUFs respectively. A positive (negative) value of ρ indicates a positive (negative) correlation between the two variables. The higher (lower) the value of ρ stronger the positive (negative) correlation. The result is a value between -1 and 1, where 1 denotes a very strong positive relationship and -1 denotes a very strong negative relation, which means that when the bias of cell i increases, the bias of cell j decreases. The closer this value lies to zero the weaker the relationship between the two PUF cells. The obtained ρ for ReOPUF falls between 1.57 to 2.59 stating that the responses are strongly correlated to the respective challenges and the uncertainty becomes a matter of reliability in security evaluation.

5.2.5.3 Analysis and Comparison

The average reliability calculated from 50 ReOPUF responses over the commercial range (0°C to 85°C) is 99.31% at 27°C as shown in Fig.5.8, and the worst-case reliability is 97.19% at 0°C. A supply voltage variation up to ±10% V_{DD} is applied to the ReOPUF as shown in Fig.5.9. The corresponding reliability is 99.19% at 1.2V, and the worst-case reliability is 97.97%. In addition, over the industrial range (-40°C to 100°C) the reliability is 97.41%. Tab.5.2 presents the comparison of different PUF designs with ReOPUF. Tab.5.3 shows the ReOPUF analysis with different temperatures.

Table 5.2 Comparison of metrics of different PUF designs

References	Technology	U (ideal 50%)	R (ideal 100%)
Liu et al., 2017 [40]	40nm	49.97%	95.88%
Cao et al., 2015 [42]	65nm	50.42%	97.28%^{t}, 96.30%^{v}
Sahoo et al., 2016 [41]	90nm	46.22%	95.89%
Laguduva et al., 2019 [43]	90nm	46.14%	99.52%
Rahman et al., 2014 [39]	90nm	47%	96.91%
This work	**65nm**	**49.22%**	**97.41%**^{t}, **97.97%**^{v}

t = temperature variation, v=supply voltage variation

Table 5.3 ReOPUF quality metrics at different temperatures

	-40°C	0°C	85°C	100°C
Intra-HD Temp (%)	97.41	97.91	99.19	98.94
Intra-HD Vdd (%)	97.97	98.31	99.03	98.81
Inter-HD (%)	85.74	94.25	81.89	78.36
Diffuseness (%)	46.27	49.32	48.79	48.03
Uniformity (%)	40.26	45.21	44.35	43.36

The layout of the ReOPUF designed in UMC 65nm excluding the pad ring is shown in Fig.5.12. It contains 2 sets (Total 8 ReOPUF instances) of the ReO circuit generating an 8-bit response with the dimension of 69μm × 98μm, which gives an approximate area of 6.8mm^3 and is designed for IoT sensor applications.

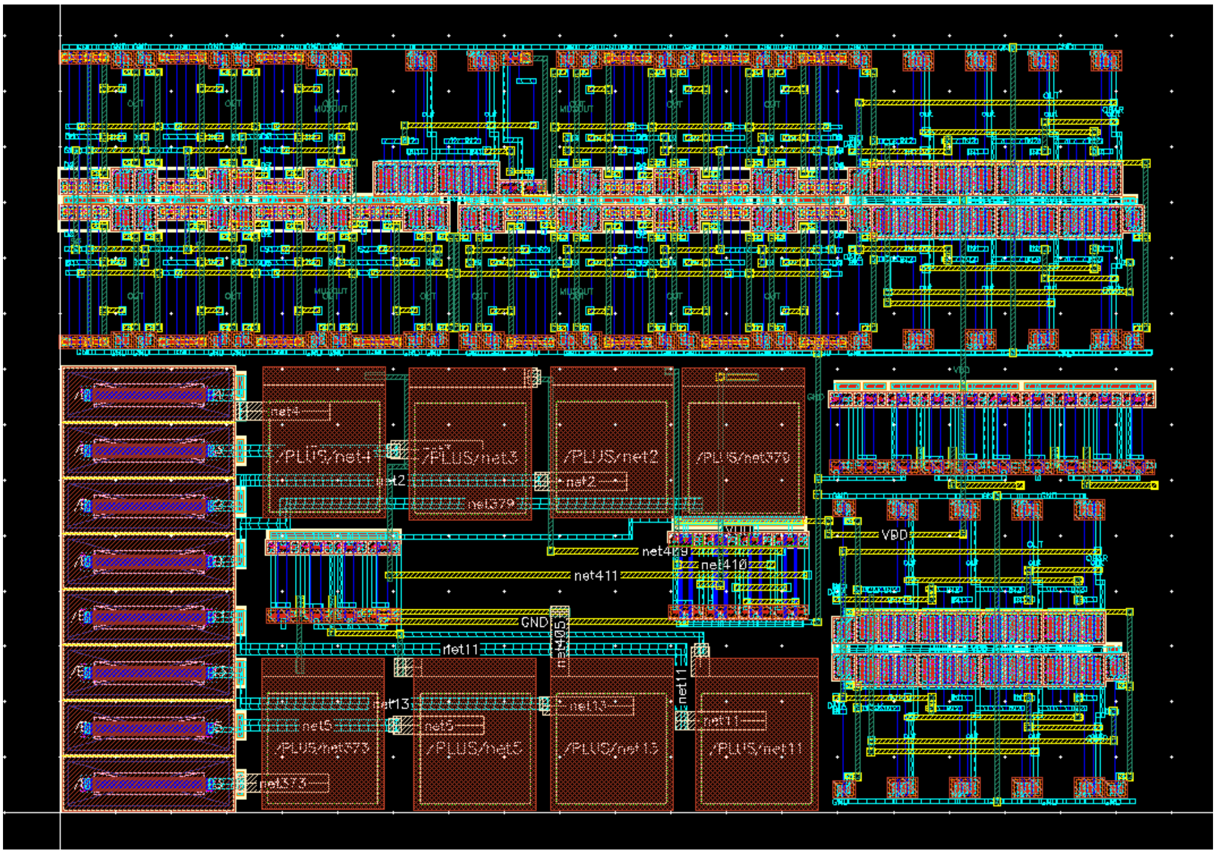


Figure 5.12 Layout of ReOPUF

5.2.5.4 Power Analysis

We measure the power consumption of the single-stage implementation of ReOPUF and RO-PUF as shown in Tab.5.4. For 32-bit key implementations, the estimated average powers of ReOPUF and RO-PUF are 3.79mW and 15mW respectively.

Table 5.4 Power comparison with RO PUF

	RO-PUF	**ReOPUF**
Power (single PUF instance) (in μW)	497.53	118.42
Power (32 PUF instances) (in mW)	15	3.79

5.3 Summary

In this chapter, we have introduced a relaxation oscillator-based PUF mechanism with the advantage that challenges fed through simple oscillation can achieve more reliability than any other oscillator PUF. The experimental evaluation of ReOPUF shows the uniqueness and reliability of 49.22% and 97.97% respectively, which is better than that of the previous works. ReOPUF significantly improves upon the previous ROPUF designs, and has the potential to be the basis for CRPs-based identification and authentication applications designed for IoT.

In fact, the ROs and ReOs have the advantage of less circuitry but are less reliable for authentication applications. So, the reliability may increase when more complexity is introduced in the circuitry that strengthens key generation. The next chapter will cover the design of Schmitt Trigger (ST) PUF with enhanced uniqueness and reliability in the key generation by bombarding the arbitration mechanism.

Chapter 6

ST-APUF: Schmitt Trigger (ST) Arbiter Physical Unclonable Function

The strong PUFs are generally posed by an exponential number of challenges that create a large number of CRPs that are useful for key generation, storage, and authentication procedures. Whereas, weak PUFs have a finite challenge space and can only be used to generate and store keys for unique ID applications. Most of the interface units are designed with conventional CMOS circuits besides working with lower supply voltages that reduce Noise Margins (NM) which makes the circuit operation unreliable. So, Schmitt Trigger (ST) [88–90] is a much better solution for VLSI sensor interface applications because they have NMs that are much higher than static CMOS circuits operating at lower voltages.

In this chapter, an ST-based APUF instance is introduced that uses PVs in Hysteresis Width (HW) to attain the non-linearity in the CRP mechanism. Thereby, impersonation of the responses (keys) is complex perhaps various trials are performed to predict the keys. The ST-APUF is proposed to achieve high uniqueness and reliability for key generation. The main contributions are as follows:

- A novel ST-APUF for reliable key generation is presented to attain non-linearity in the arbitration process between two different STs.

- We propose an ST-APUF that produces automated challenges feed from the response of STs using the Hysteresis Width (HW) difference. Thus, the complexity is attained with the process variations that existed in STs to make STAPUF more resilient to attacks.

- We evaluate the simulation results with PUF measures such as Uniformity (u), Uniqueness (U), Diffuseness (D), and Reliability (R) to assess the performance of the ST-APUF. And also, show that the proposed one has less Bit-Error-Rate (BER) than the STPUFs [91–94].

6.1 Design considerations

To implement strong CRP generation, the provision of circuit complexity and high randomness are taken into consideration. This chapter will introduce the ST based PUF based on the following specifications provided in Tab.6.1.

Table 6.1 Specifications for ST-APUF

Design Parameters		
Aspect ratio (nm) (Schmitt Trigger)	PMOS	240/180
	NMOS	240/180
Aspect ratio (μm) (3T inverter)	PMOS	3/0.18
	NMOS	1/0.18
Aspect ratio (nm) (2x1 Muxes)	PMOS	240/180
	NMOS	240/180
Aspect ratio (nm) (Transmission Gate)	PMOS	240/180
	NMOS	240/180
V$_{DD}$ (V)	1.8	
Input (I)	16-bit	
Challenges (C)	“n-bit” (Depends on stages)	
Responses (R)	16-bit	

6.2 Implementation of ST-APUF

ST is a comparator circuit that amplifies the difference between the input voltage (V$_{IN}$) and the threshold voltages (V$_L$ and V$_H$). It is also referred to as a regenerative comparator with hysteresis, which describes the dependence of the current output on the prior output. The transition difference between V$_L$ and V$_H$ generates the output voltage (V$_{OUT}$) that is considered as Hysteresis Width (HW). Specifically, in constrained

IoT applications that are operated at a wide range and lower supply voltage the efficacy of the CMOS inverter degrades. To overcome these limitations, ST circuits have been proposed and proven effective whereas they always produce rapid edges on their output signals followed by early transitions occurring at the input.

In this chapter, we implemented an ST-based Arbiter PUF (ST-APUF) to generate the 16-bit response (key). The proposed ST-APUF comprises a 16×16 PUF array cell to generate independent response bits, a 4 to 16 decoder that feeds challenges to ST-APUFs, a transmission gate for the ST-APUF arbitration, a comparator for the HW calculation, and the buffers for the reading of PUF bits in parallel. Fig.6.1 shows the architecture of the proposed ST-APUF bit cell used as an instance. It presents two different ST inverters (ST1 and ST2) arranged in parallel that are selected arbitrarily by the Transmission Gate (TG) depending on the selection driven by the Multiplexer (Mux).

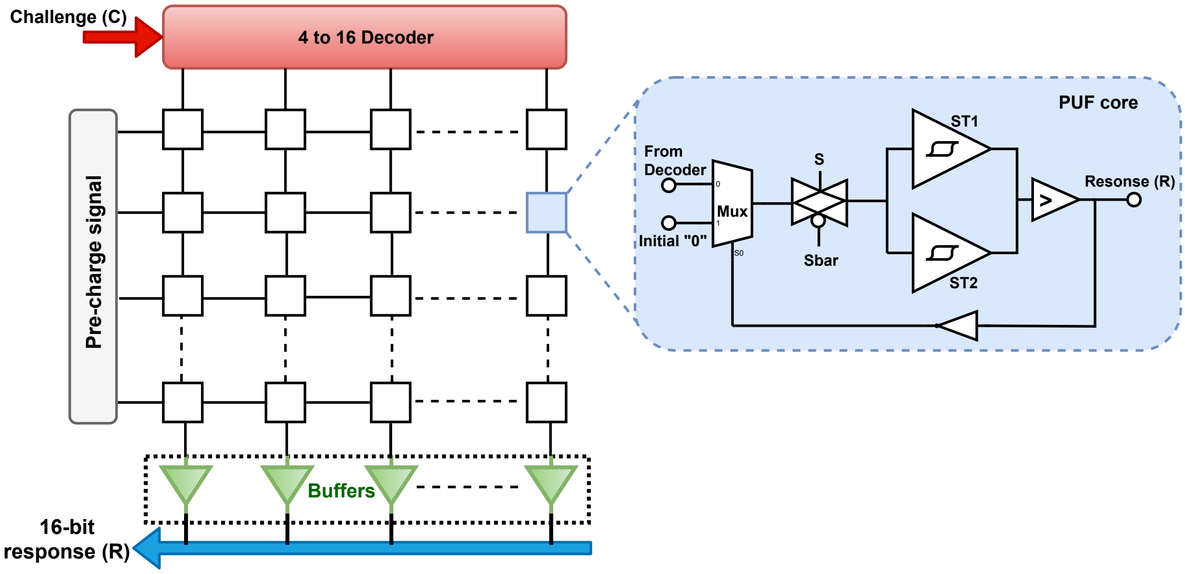


Figure 6.1 Architecture of the proposed ST-APUF

A 4 to 16 decoder generates the challenges C_0 to C_{15} and feeds as one of the inputs to the Mux along with the second input fixed as '0'. Initially, the selection input (S_0) of the Mux is set as '0' and later it gets populated from the feedback i.e. Response (R) attained at the comparator. The pre-charge signal is assisted to pull up the ST instances to V_{DD} until the decoder performs the selection (or challenge). After an instance selection, according to the decision made by the Mux, the evaluation of the ST inverters is started by pulling down the voltages from V_{DD}. However, the arbitration among the STs is done through TGs to deliver the voltage difference ($V_H - V_L$) according to the PVs. Each ST has its threshold points like V_L and V_H under voltage-transfer characteristics (VTC). Due to the deceptive mismatch between the STs the width of HW is obtained by HW=$V_H - V_L$. Possibly, the variation in the threshold voltages is observed by increasing or decreasing the input voltage sweeps. Thereby, the possible HW is achieved concerning the corresponding output transitions. Finally, the response (R) is evaluated at the comparator as '1' if HW of ST1>ST2 or '0' if HW of ST1<ST2.

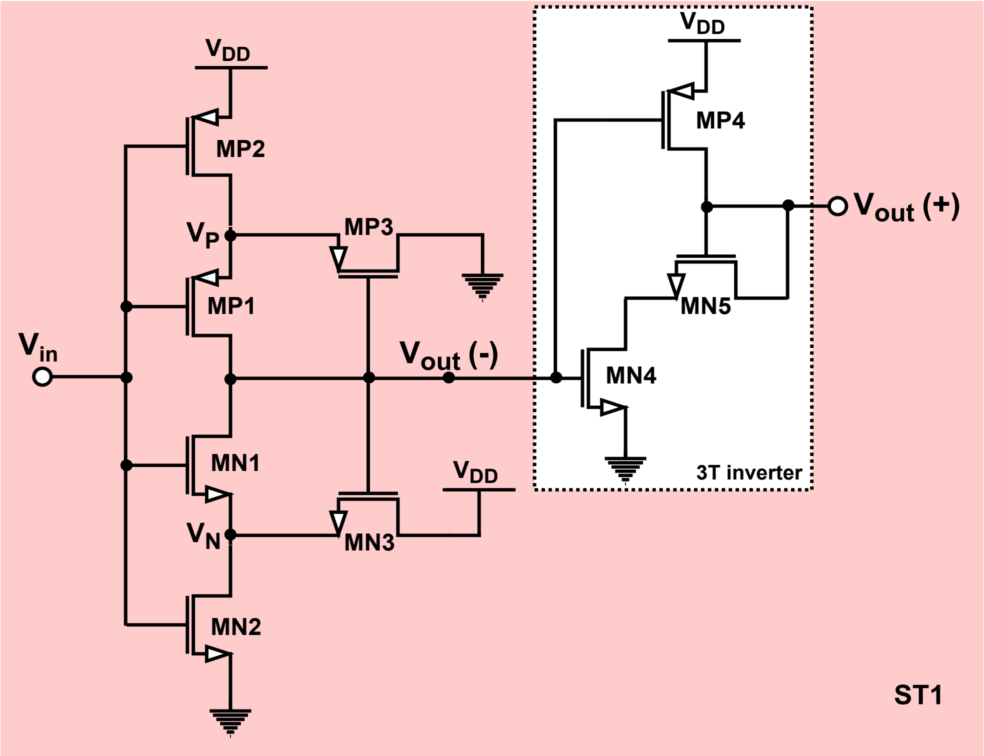


Figure 6.2 Transistor level schematic of ST1 inverter

The transistor level design of conventional ST1 and improved ST2 shown in Fig.6.2 and Fig.6.3 are built with standard 180nm CMOS transistors and ST2 with Low Voltage Threshold (LVT) 180nm CMOS transistors respectively to get the huge difference in HW. Eventually, both STs are comprehended with a 3T inverter to produce additional variation in delay. Consequently, valid responses are attained when more difference in HW is observed due to the arbitration performed between ST1 and ST2.

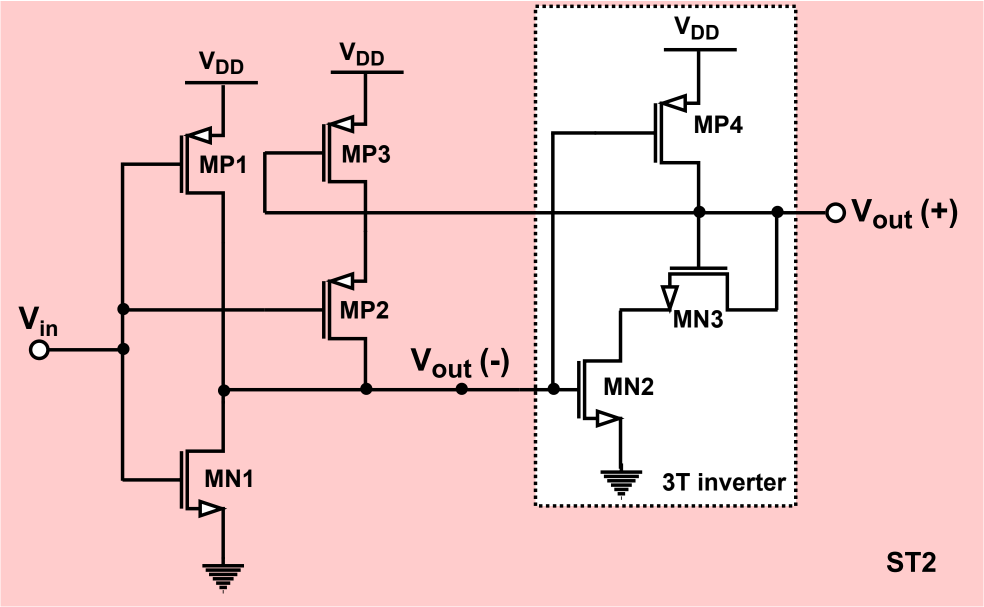
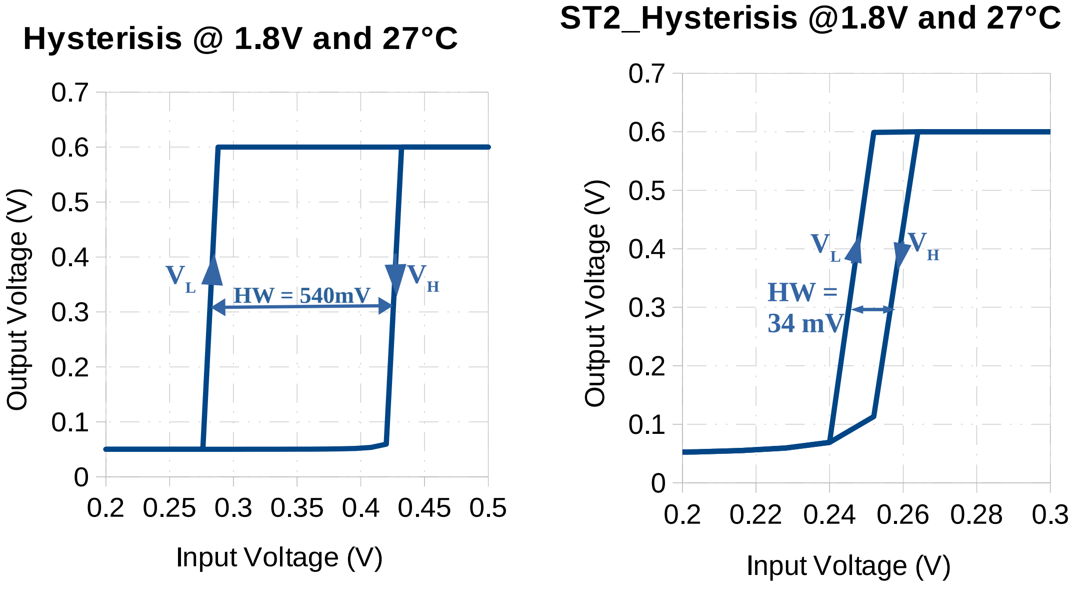


Figure 6.3 Transistor level schematic of ST2 inverter

In Fig.6.4, the hysteresis exists when VTC is performed for ST1 and ST2 at room temperature (27°C) and standard supply voltage (1.8V). There are two distinct threshold points, V$_L$ and V$_H$, which represent the input voltage changes from V$_{DD}$ to 0 and 0 to V$_{DD}$. It is noticed that the HW for ST1 and ST2 are recorded as 540mV, and 34mV respectively.

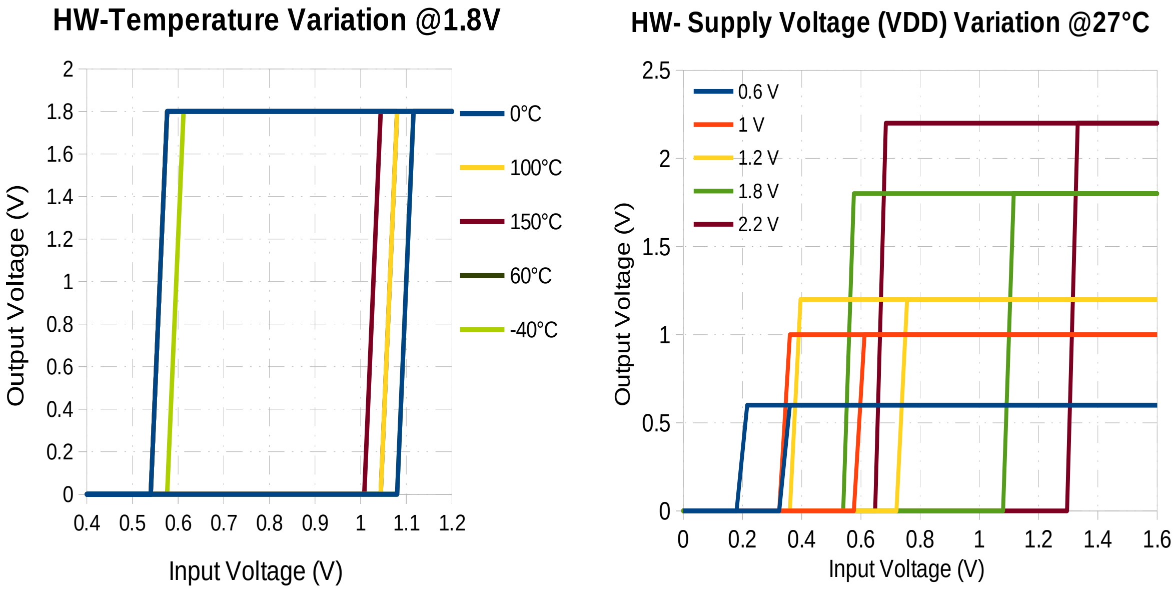


(a) Hysteresis of ST1

(b) Hysteresis of ST2

Figure 6.4 Hysteresis analysis of ST

These widths are not constant and vary according to the supply voltage, temperature and PVs inherited in the ST. Fig.6.5a presents the HW variation in ST1 with respect to the temperature considered from −40°C to 150°C. Whereas Fig.6.5b presents the HW variation in ST1 with respect to the supply voltage considered from 0.6V to 2.2V.

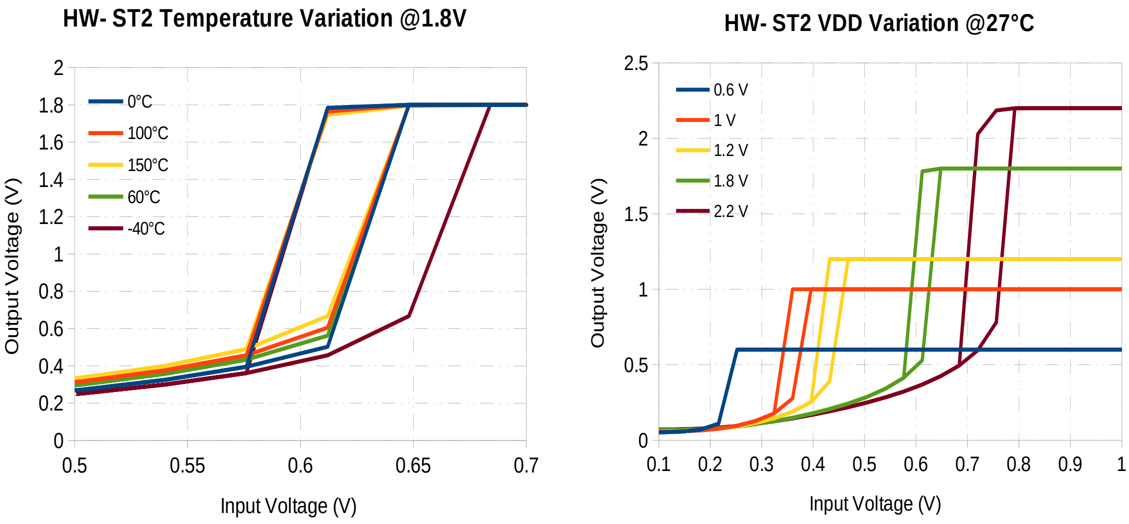


(a) ST1 with Temperature variation

(b) ST1 with Supply voltage variation

Figure 6.5 Hysteresis Width variation in ST1

Consequently, Fig.6.6a presents the HW variation in ST2 with respect to the temperature considered from −40°C to 150°C. Whereas Fig.6.6b presents the HW variation in ST2 with respect to the supply voltage considered from 0.6V to 2.2V.



(a) ST2 with Temperature variation

(b) ST2 with Supply voltage variation

Figure 6.6 Hysteresis Width variation in ST2

6.2.1 Circuit analysis of ST1

The analysis of ST1 based on the basic ST design [31] shown in Fig.2. Consider the bottom circuit MN1, MN2, MN3 (specified as N-subcircuit) is loaded by the top circuit MP1, MP2, MP3 (P-subcircuit). The voltage-current characteristics of these nonlinear loads are determined while the N-subcircuit is applied with voltage source V$_{ss}$ by assuming a constant voltage V$_{gs}$ at the gates of MN1 and MN2 and the respective source current I$_{ss}$ is calculated.

6.2.1.1 Current-Voltage Subcircuit Characteristics for ST1

When the voltage V$_{ss}$, is very low, transistor MN3 turns OFF, and MN1 and MN2 operate in the triode or linear mode. The current I$_{ss}$, is equivalent to Eq.1 when MN1 is considered.

$$I_{ss} = 2k_1 \left(V_{gs} - V_{thN}\right) V_N \tag{6.1}$$

when MN2 is considered I$_{ss}$ is equivalent to Eq.2.

$$I_{ss} = 2k_2 \left(V_{gs} - V_{thN} - V_{ds}\right) \left(V_{ss} - V_N\right) \tag{6.2}$$

where, K$_i$ = 1/2 $\mu_n C_{ox}$(W/L), V$_{gs}$ is the gate to source voltage, V$_{ds}$ is the drain to source voltage, V$_N$ is the node voltage, and V$_{thN}$ is the threshold voltage of the ‘n’ transistor. For p-channel transistors, μ_p is the mobility, V$_{sg}$ is the gate to source voltage, V$_{sd}$ is the drain to source voltage, V$_P$ is the node voltage, and V$_{thP}$ is the threshold voltage of the ‘p’ transistor. It is expected that Eq.1 and Eq.2 are operating in saturation i.e.V$_{gs}$>V$_{thN}$. For the triode mode of operation, V$_{ds}$≪V$_{thN}$ and the I$_{ss}$ can be simplified as Eq.3.

$$I_{ss} = 2k_2 \left(V_{gs} - V_{thN}\right) \left(V_{ss} - V_N\right) \tag{6.3}$$

The values of K$_1$ and K$_2$ with respect to MN1 and MN2 are represented in Eq.4 and Eq.5.

$$k_1 = \frac{1}{2}\mu_n C_{ox}\frac{W}{L} \tag{6.4}$$

$$k_2 = \frac{1}{2}\mu_n C_{ox}\frac{W}{L} \tag{6.5}$$

From Eq.1 and Eq.3, V$_N$ and I$_{ss}$ are determined as Eq.6 and Eq.7,

$$V_N = V_{ss}\frac{k_2}{k_1 + k_2} \tag{6.6}$$

$$I_{ss} = \frac{2k_1k_2\left(V_{gs} - V_{thN}\right)}{k_1 + k_2}V_{ss} \tag{6.7}$$

When V$_{ss}$ increases, the transistor MN2 enters into saturation region, then I$_{ss}$ is represented as Eq.8 and Eq.9 with respect to transistor.

$$I_{ss} = 2k_1\left(V_{gs} - V_{thN} - \left(\frac{V_N}{2}\right)\right)V_N \tag{6.8}$$

$$I_{ss} = k_2\left(V_{gs} - V_{thN} - V_N\right)^2 \tag{6.9}$$

From Eq.8 and Eq.9 we can find V_N and it does not depend on V_{ss}. That means when the V_{ss} reaches the value of V_{ssS} (minimum saturation voltage)= V_{gs}-V_{thN}, then I_{ss} is equal to Eq.10. An additional increase of V_{ss} will achieve the value of V_{ssT} (minimum threshold voltage). Consequently, MN3 will be turned ON which results to increase V_N and diminish I_{ss}. Thus, MN2 will be completely turned OFF (V_{oC} = minimum cut-off voltage) and I_{ss} becomes ‘0’. At this stage V_{thN} is equal to V_{gs}-V_{thN} and MN1 is enter into the saturation region. The transistor MN1 carries the current as Eq.10.

$$I_N = k_1\left(V_{gs} - V_{thN}\right)^2 \tag{6.10}$$

which is completely seized by MN3. Even though an additional increase appeared in the V_{ss} up to V_{DD} that doesn’t bring any changes in the characteristic of N-subcircuit.

6.2.1.2 3T inverter analysis for ST1

To produce more PVs in the circuit a 3T inverter is added to the ST1. Accordingly, consider V_{out-} as input to the 3T inverter and V_{out+} as the output to obtain HW of the ST1. When V_{out-}<V_{th}, MN4 is in cut-off and MP4 turn into linear region with the voltage of Eq.11.

$$V_{sgP} = V_{DD} - V_{out-} > V_{th} \tag{6.11}$$

However, MN5 transistor is always in saturation because the gate and drain terminals have the same potential i.e.V_{dsN}=V_{out+}. Whereas, the input voltage attained V_{out-}>V_{DD}−V_{th}, MP4 turns to cut-off perhaps MN4 enter into linear with respect to the Eq.12.

$$V_{dsN} = V_{out+} < V_{gsN} - V_{th} \tag{6.12}$$

When there is slightly increase in V_{out-} the transistors seems to be operate in saturation. If V_{out-}>V_{th} MN4 turns to saturation and MP4 operate in linear as represented in Eq.13

and Eq.14.

$$V_{dsN} = V_{DD} > V_{gsN} - V_{th} \tag{6.13}$$

$$V_{sdP} = V_{DD} - V_{out+} \rightarrow 0 < V_{sgP} - V_{th} \tag{6.14}$$

When V_{out-} attains $V_{DD}{-}V_{th}{-}\Delta$V, MP4 and MN4 are operate in the saturation and linear region respectively as represented in Eq.15 and Eq.16.

$$V_{sdP} = V_{DD} - V_{out+} \rightarrow V_{DD} > V_{sgP} - V_{th} \tag{6.15}$$

$$V_{dsN} = V_{out+} \rightarrow 0 < V_{gsN} - V_{th} \tag{6.16}$$

At middle area (i.e.$V_{out-}{=}V_{DD}/2{\pm}\Delta$V), both MN4, MP4 are operate in saturation region as represented in Eq.17 and the potential at drain terminal is represented as Eq.18.

$$V_{sdP} = V_{DD} - V_{out+} \approx \frac{V_{DD}}{2} > V_{sgP} - V_{th} \tag{6.17}$$

$$V_{dsN} = V_{out+} \approx \frac{V_{DD}}{2} > V_{gsN} - V_{th} \tag{6.18}$$

Thus, ST1 is analyzed with respect to V_{in} and V_{th} voltage assumptions.

6.2.2 Circuit analysis of ST2

The analysis of ST2 based on the improved ST design [31] shown in Fig.3.Assume that the input signal V_{in} is low at startup, the MN1 would be switched OFF and the MP1 would be turned ON, causing node V_{out-} to be charged to a HIGH state and node V_{out+} to be discharged to ground potential. The MP2 enters the circuit when the 'LOW' at node V_{out+} turns 'ON' MP3. When the input is growing from 0 to V_{dd}, MP2 which is stronger than MN1 moves the inverter's positive tripping point towards the right on the hysteresis curve. Once the inverter trips, the nodes V_{out-} and V_{out+} are set to the 'LOW' and 'HIGH' states, respectively, MP3 is turned 'OFF', and MP2 is no longer functional. MP1, which is weaker than MN1, moves the inverter's negative tripping point to the left on the hysteresis curve during the input transition from 'HIGH' to 'LOW'.

6.2.2.1 Current-Voltage Subcircuit Characteristics for ST2

When voltage source V$_{ss}$ by assuming a constant voltage V$_{gs}$ at the gates of MN1 and MP1 and the respective source current I$_{ss}$ is calculated. When the voltage V$_{ss}$, is very low, transistor MN1 turns OFF, and MP1 and MP2 operate in the triode or linear mode. The current I$_{ss}$, is equivalent to Eq.19 when MP1 and MP2 are considered.

$$I_{ss} = -\frac{1}{2}\mu_p C_{ox}\frac{W}{L}\left(V_{gs} - v_{thP}\right)^2 \tag{6.19}$$

where, V$_{sg}$ is the gate to source voltage, V$_{sd}$ is the drain to source voltage, and V$_{thP}$ is the threshold voltage of the 'p' transistor. It is expected that Equ (1) is operating in triode or linear. For the triode mode of operation, V$_{sd}$≤V$_{thP}$. When V$_{ss}$ increases, the transistor MN1 enters into saturation region, MP1 and MP2 are stay in the kiner region. I$_{ss}$ with respect to MN1 is represented in Eq.20 as

$$I_{ss} = \frac{1}{2}\mu_n C_{ox}\frac{W}{L}\left(V_{gs} - v_{thN}\right)^2 \tag{6.20}$$

When an additional increase appeared in the V_{ss} up to V_{DD} that bring changes in the characteristic of transistors with respect to V_{in} and V_{th} voltages.

6.2.2.2 3T inverter analysis for ST2

When V_{out-}<V_{th}, MN3 is in cut-off and MP5 turn into linear region with the voltage of Eq.21.

$$V_{sgP} = V_{DD} - V_{out-} > V_{th} \tag{6.21}$$

However, MN2 transistor is always in saturation because the gate and drain terminals have the same potential i.e. V_{dsN}=V_{out+}. Whereas the input voltage attained V_{out-}>V_{DD}−V_{th} MP5 turns to cut-off perhaps MN3 enter into linear with respect to the Eq.22.

$$V_{dsN} = V_{out+} < V_{gsN} - V_{th} \tag{6.22}$$

When there is slightly increase in V_{out-} the transistors are ready to operate in saturation. If V_{out-}>V_{th} MN3 turns to saturation and MP5 operate in linear as represented in Eq.23 and Eq.24.

$$V_{dsN} = V_{DD} > V_{gsN} - V_{th} \tag{6.23}$$

$$V_{sdP} = V_{DD} - V_{out+} \to 0 < V_{sgP} - V_{th} \tag{6.24}$$

If V_{out-} attains V_{dd}−V_{th}−ΔV, MP5 and MN3 are operate in the saturation and linear region respectively that are represented in Eq.25 and Eq.26.

$$V_{sdP} = V_{DD} - V_{out+} \to V_{DD} > V_{sgP} - V_{th} \tag{6.25}$$

$$V_{dsN} = V_{out+} \rightarrow 0 < V_{gsN} - V_{th} \tag{6.26}$$

At middle area (i.e.V_{out-}=V_{DD}/2±ΔV), both MN3, MP5 are operate in saturation region as represented in Eq.27 and Eq.28 respectively.

$$V_{sdP} = V_{DD} - V_{out+} \approx \frac{V_{DD}}{2} > V_{sgP} - V_{th} \tag{6.27}$$

$$V_{dsN} = V_{out+} \approx \frac{V_{DD}}{2} > V_{gsN} - V_{th} \tag{6.28}$$

with respect to V_{in} and V_{th} the analysis of the VTC for ST2 is observed with region of operation.

6.2.3 Threshold, Transition of Proposed Schmitt-Trigger

The transition of trigger behaviour in the sub-circuits (N and P) is shown in Fig.6.2 caused to allow the provision of two dissimilarities useful in the trigger design. Assume that the trigger transition occurs from one stable state to another that requires a threshold value (V_H) at the gate terminal of the transistors MN1, MN2, MN3and MN4 by allowing an instant current variation (I). Similarly, when similar condition is applied another transition point attained with the required threshold voltage of (V_L).

The operation of the ST shown in Fig.6.2 is described with appropriate assumptions necessary for the trigger design. The voltage V_G in Fig.6.2 is assumed to be zero. MN1 and MN2 are then turned OFF. The voltage drop at transistors MN4 and MN5 is zero even though they are operating in the linear mode since the current flowing through them is the same as that through MN1 and MN2. Therefore, the output voltage V_{out+} is equal to V_{DD} (or high). At this instant, the drain and gate of transistor MN3 have the same voltage of V_{DD} while it is ON, but it is also not conducting any current.

Subsequently, the transistor MN1 activates and starts conducting when V_G exceeds V_{thN} which controls MN1's current represented in Eq.10. The MN3 entirely blocks it, and there is no change in the state of the P-subcircuit's transistors. However, the potential V_N is, beginning to decline. When the voltage V_G reaches V_{Hi}, the trigger operation begins. Transistor MN2 turns ON at this point as a result of the simultaneous rise in V_G and fall in V_N. It is clear that by substituting V_{DD} for V_{oC} in Eq.10 (the gate of MN3 is still at V_{DD}) and V_{Hi} for V_G, the necessary relationship between the transistor characteristics to initiate the triggering operation is achieved. It can be rewritten as Eq.29.

$$\frac{k_1}{k_3} = \left(\frac{V_{DD} - V_{Hi}}{V_{Hi} - V_{thN}}\right)^2 \tag{6.29}$$

By applying the same logic, one derives that the condition

$$\frac{k_4}{k_6} = \left(\frac{V_{Li}}{V_{DD} - V_{Li} - |V_{thP}|}\right)^2 \tag{6.30}$$

Equ. be fulfilled to initiate the triggering action once the input voltage reaches V_{Li}. The voltages V_{Hi} and V_{Li} are regarded as the real thresholds of the CMOS ST. However, in reality, V_{Hi} and V_{Li} just signify the start of the triggering action. The actual triggering takes place at the close but dissimilar voltages V_{Hi} and V_{Li}.

In fact, the ST's transition from one stable state to another occurs very quickly, and one can assume that throughout this time the trigger input voltage remains constant. However, at V_H the duration of the output voltage is considered to vary from high to low. The trigger becomes a linear circuit with positive feedback as soon as MN2 is turned on. According to the P-subcircuit voltage-current characteristic, the transistors MN4 and MN5 are operating in a linear mode. The transistor MN1 carries the current as in Eq.31.

$$I_{NH} = k_1 \left(V_H - V_{thN}\right)^2 \approx k_1 \left(V_{Hi} - V_{thN}\right)^2 \tag{6.31}$$

6.3 Evaluation of ST-APUF

The validation of the proposed ST-APUF is implemented in a 180 nm 1.8 V standard CMOS process. The characterization of 150 ST-APUF array instances is assisted to generate responses based on the Montecarlo simulation [92]. During simulation, the inter-die and intra-die PVs are evaluated through the HD calculated between the acquired responses concerning the independent challenges. Significantly, the ST-APUF instances are initiated with PV that occurred due to the variations in transistor threshold voltage.

6.3.1 Uniformity (u)

The distribution of "1s" and "0s" in the obtained response vector R$_x$, R$_y$ is measured by uniformity, which is defined in Chapter 2 as Eq.2.1. Where R$_{x,y}$ is the 'yth' binary response of an n-bit for an 'xth' challenge. A perfect PUF would have a 50% chance of getting either a ”1” or a ”0”. Fig.6.7 illustrates the evaluation of the 16-bit responses from 150 ST-APUF instances at nominal operating conditions of 27°C and 1.8V. The value ”1” can be assigned to a white pixel and ”0” to a black pixel. The likelihood of producing 1’s is 49.92%, which shows that ST-APUF production is unpredictable and difficult to combat.

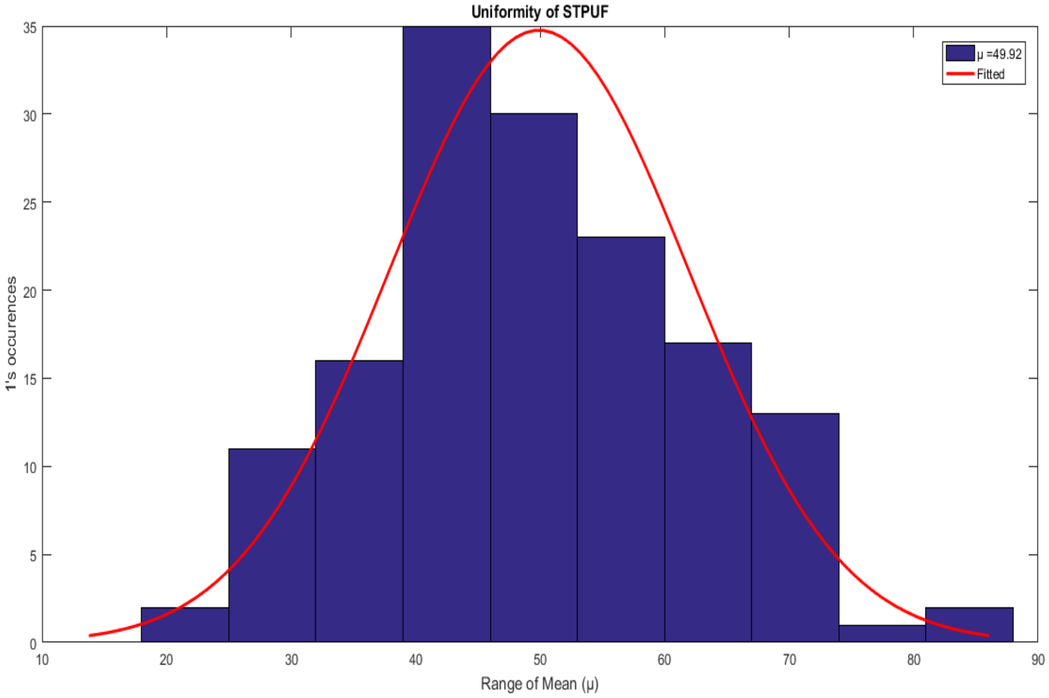


Figure 6.7 Uniformity of ST-APUF with distribution of 1’s and 0’s

6.3.2 Diffuseness (D)

The degree of variations shown in the same ST-APUF instance under various challenges is referred to as diffuseness. The ideal value to attain good security assistance is 50%. It is referred to as Eq.2.2 in Chapter 2. Where ’l’ is the randomly chosen response vector from CRP. The 16-bit response vectors, R$_x$, R$_y$ are randomly selected from the CRP space from two distinct challenges. Fig.6.8 depicts the diffuseness of 16-bit responses from 150 ST-APUF instances run at 27°C and 1.8V. The mean (μ) that is computed from the HD values that were collected is 49.92%.

6.3.3 Uniqueness (U)

The estimation of randomness in the responses generated through various ST-APUF instances under the same reference typical voltage (V$_T$) condition defines the performance

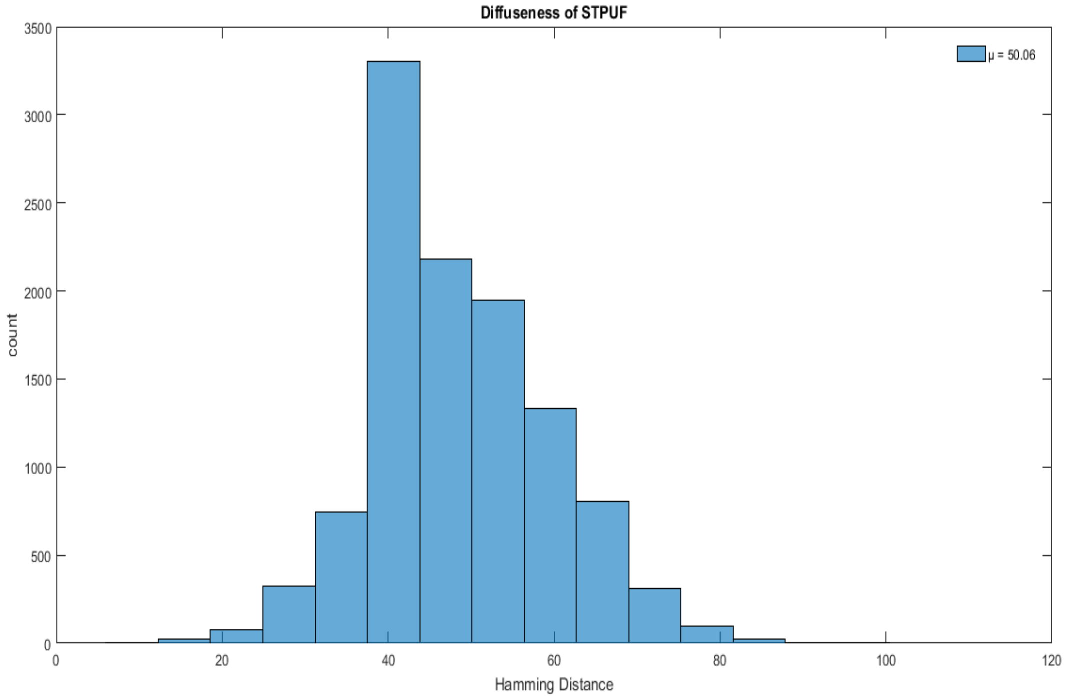


Figure 6.8 Diffuseness of ST-APUF

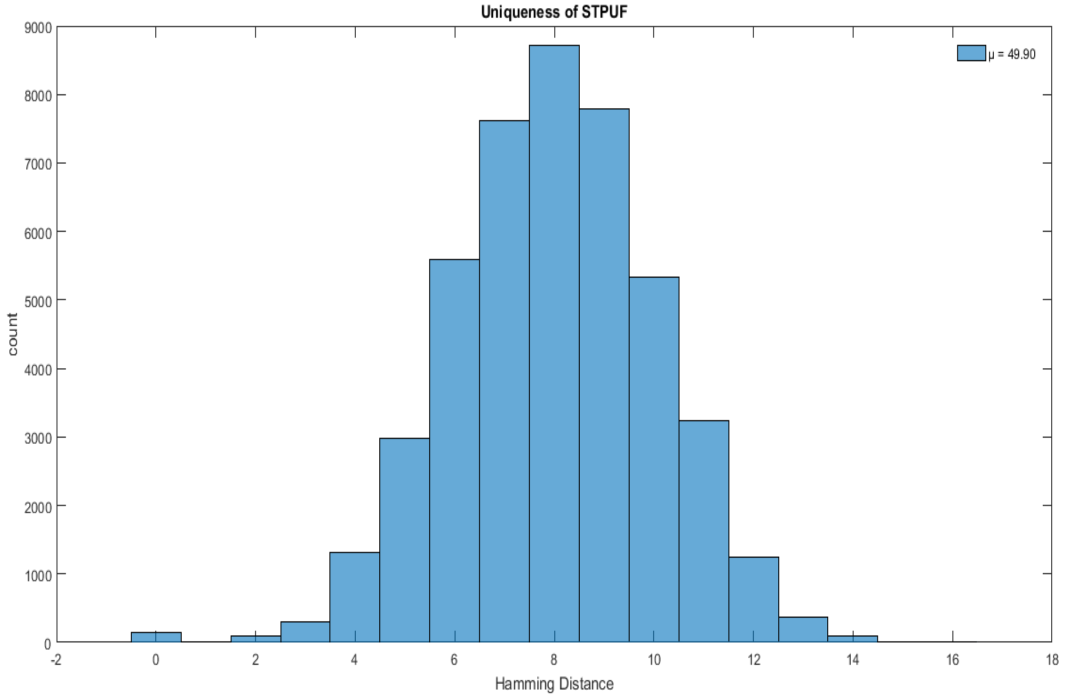


Figure 6.9 Uniqueness of STAPUF (inter-HD)

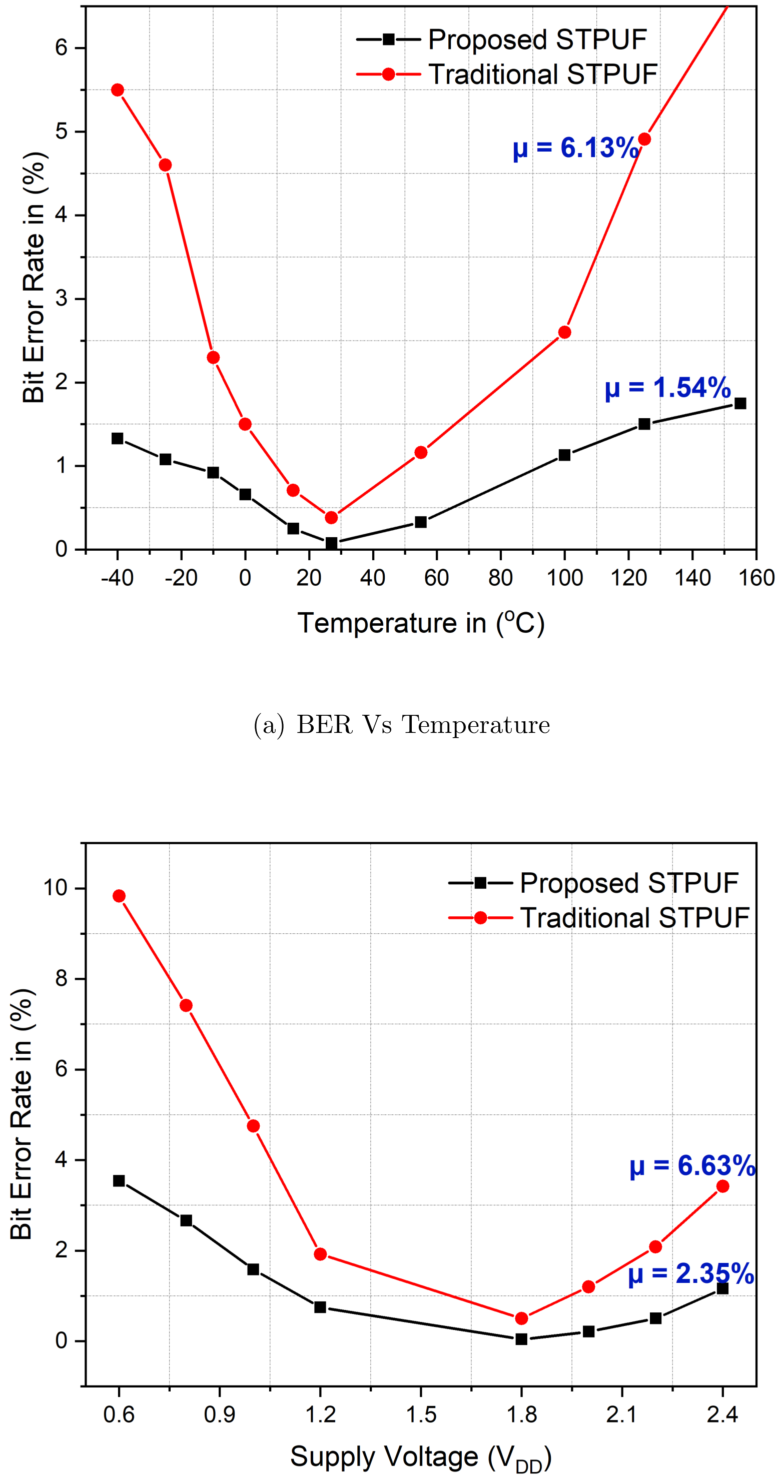
in terms of uniqueness. For identical PUFs, the successful generation of responses (i.e., ”0” or ”1”) to the same challenge is 50%. Uniqueness is determined by averaging the HD across various pairs of 'm' ST-APUF instances that are normalized to the response bit length 'n'. To be more precise the uniqueness is determined by Eq.2.3 as represented in Chapter 2.

Here R$_x$ and R$_y$ are two distinct response vectors evaluated from 'm' ST-APUF instances under the same challenge. We evaluated the inter-HD of '16' bit responses from 150 ST-APUF instances i.e. $^{150}C_2$= 11175 pairs. Generally, the average HD performed between the responses is also known as the normalized inter-HD. The normalized HD mean value 'μ' is computed to be 49.90% under the supply voltage of 1.8V as shown in Fig.6.9 indicating that it has good randomness among ST-APUF instances.

6.3.4 Reliability (R)

The validation of the responses produced from the same ST-APUF instances with identical challenges is used to test reliability. Generally, the same challenge is issued to the identical ICs, a PUF should always produce the same response. Unpredictably, sweeping in the supply voltages (V_{DD}) or temperature (T) might cause the IC to behave contrarily and cause unexpected reactions by producing circuit delays. So, the redundancy is observed in response bits under various operating environments. It should ideally be close to 0% when intra-HD is calculated between two n-bit response vectors generated from the same PUF instances with the same challenges.

For intra-HD, a total of 150 ST-APUF instances are simulated for analysis that are represented in Fig.6.10a and Fig.6.10b. The representation for reliability assessment is shown in Chapter 2 as Eq.2.4 and Eq.2.5. Where "m" denotes the number of trials applied on ST-APUF instances with the identical challenge. $R_{i,ref}$ is the reference response measured at standard operating circumstances, which are 27°C and 1.8V, and $R_{i,t}$ is the tth response observed at different operating conditions. In addition to the responses, the reliability is measured in terms of Bit Error Rate (BER). We calculate the BER from the 16-bit responses from 150 ST-APUF instances under various operating conditions.



(a) BER Vs Temperature

(b) BER Vs Supply Voltage

Figure 6.10 Reliability assessment through BER

6.3.5 Security evaluation

PUFs are one of the best approaches developed for security applications that can retain high reliability against threat models used by attackers. Amongst existing security techniques, PUFs use inherited PVs in the ICs to generate valid challenge-response pairs. If a PUF is used for a key generation then the strong CRP set needs to be maintained once the attacker focuses on CRP space to guess the correct combination. Otherwise, PUF is preferred for authentication by maintaining uncertainty in the circuit behaviour whereas the attacker performs different trials to disrupt the PUF behaviour. So, the reliability of the PUFs should be strengthened even though different types of attacks are performed by intruders.

A common machine learning attack against PUF, known as LR [78], is used to assess the security of the proposed ST-APUF. LR assumes that the data will follow a particular distribution and employs the maximum likelihood function. The prediction rate evaluated for the proposed ST-APUF is 49% while applying LR indicates good resistivity against attacks. The average prediction rate illustrated in Fig.6.11 is observed as 52% when 2400 training samples are undergone with LR. Hence, by increasing the training CRPs with small samples, prediction rates improve. However, the ST-APUF is evaluated with various ML classifiers shown in Fig.6.12 achieving an average prediction accuracy of 56% indicating that more resilient to attacks.

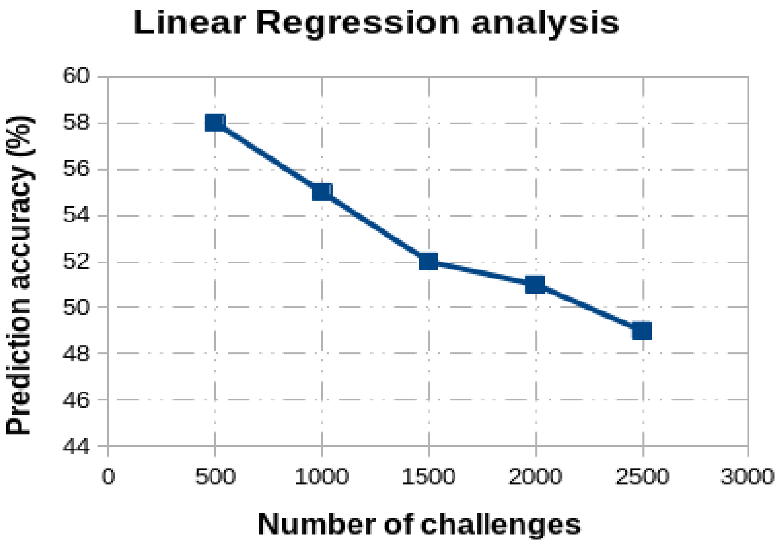


Figure 6.11 Prediction analysis of ST-APUF

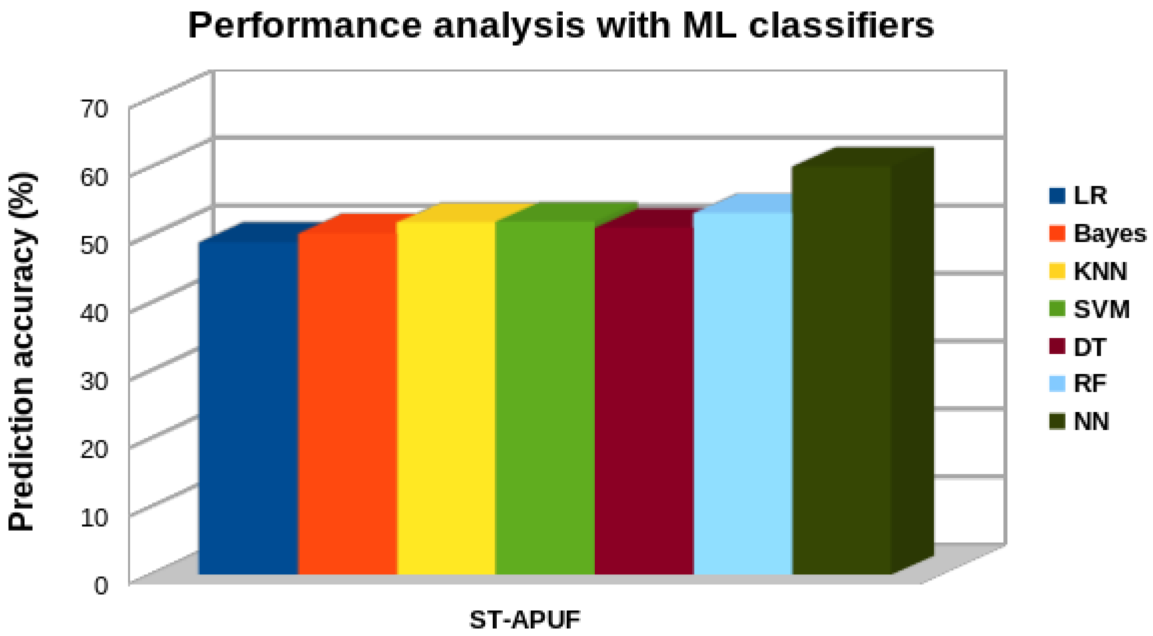


Figure 6.12 Performance with ML classifiers

6.3.6 Analysis and Comparison

Fig.6.10(a) displays the BER of the proposed ST-APUF response as a function of temperature. The average reliability estimated from 150 ST-APUF responses over the commercial range (0°C to 80°C) is 99.91%, whereas the worst-case reliability is 98.46% at 0°C, with error rates of 0.09% and 1.54%, respectively. Fig.6.10(b) depicts a supply voltage variation of up to 10% V_{DD} applied to the ST-APUF instance. The average reliability is 99.35% at 1.8V, while the worst-case reliability is 96.46% at 0.6 V, with error rates of 0.65% and 3.54%, respectively. Moreover, the BER for the industrial range (-40°C to 100°C) is observed as 0.72%.

6.3.6.1 Performance analysis

Extensive simulations performed on the proposed ST-APUF show significant improvement in quality metrics e.g. Uniformity, Uniqueness, and inter and intra-die HD. The response is a function of the delay featured by the arbitration mechanism. The delay is raised by a distinct saturation level for changing input that is triggered by transmission gates. So, the random switching occurred between STs to produce valid binary responses based on the PVs inherited in the circuit. We test each PUF for voltage fluctuation of ±10% and temperature variation from -40°C to 155°C and calculate the difference in

Table 6.2 Comparison of metrics of different PUF designs

References	**PUF Type**	**Technology (nm)**	**U (%) (Ideal-50%)**	**R (%) (Ideal-100%)**	**BER (%)**	**Prediction Accuracy (%)**
Lin et al., 2015 [89]	ST	90	49.5	-	-	-
Suh et al., 2007 [14]	RO	90	46.15	99.52	-	-
Zhang et al., 2021 [38]	RO	90	49.17	100	-	-
Tao et al., 2016 [55]	Temperature sensor	65	50.04	98.3	-	-
Zhao et al., 2018 [58]	Current Comparator	65	49.96	99.05	-	-
Huang et al., 2022 [60]	ST	65	49.95	-	0.03 (6.8)*	-
Khan et al., 2023 [61]	ProHys	180	49.85	96.9	-	-
Kumar et al., 2019 [64]	ST	90	44.75	99.7	-	-
This Work	***ST-APUF***	***180***	***49.9***	***99.91^t, 99.35^v***	***0.09^t, 0.65^v (1.54^t, 3.54^v)****	***49***

*t = temperature variation, v=supply voltage variation, *= Worst-case, - = Not Mentioned*

PUF responses.

For a particular challenge generated by the decoder, the input data is stimulated across the ST-APUF instance with a 10ns rising edge, and the response time is predicted to be 0.2μs. This is fast compared to the other ST-PUF techniques and is hardly suitable for generating secret keys within the stipulated time to the ICs for identification or authentication applications. However, the performance of the ST-APUF may increase when multiple switching delays are incorporated in the TG level or ST level.

The most distinctive PUFs released in the previous fifteen years are included in Table 1. In comparison to traditional ROPUFs [15,23], thyristor [55], and tri-state inverter PUF

[54] the proposed ST-APUF performs typically better and has achieved better uniqueness. When compared to the findings of the traditional STPUFs, which were 49.5% by [88], 49.85% by [60], and 44.75% by [63], the proposed ST-APUF results had a uniqueness of 49.9%. Higher uniqueness is attained via the temperature sensor PUF [56], current comparator PUF [57], and STPUF [68] but dependability and BER are sacrificed. The ST-APUFs reliability over T and V$_{DD}$ variation is raised by more than 4% and 3.4%, respectively, in comparison to the PUF designed in [60]. Moreover, the BER is achieved approximately 92% higher in the worst-case but three times lesser in a regular scenario as contrasted to [68].

Tab.6.3 and Tab.6.4 display the quality metrics observed when an ST-APUF operated at various temperatures and supply voltages. PUF measurements, such as inter-HD and intra-HD expressed in Eq.34 and Eq.35, are used to assess the performance of ST-APUF. These metrics have a substantial benefit in terms of voltage and temperature reliability. The average BER deteriorates by 2.35% when the supply voltage changes by 0.2 V and by 1.54% when the temperature deviations by 10°C.

Table 6.3 ST-APUF quality metrics at different temperatures

	-40°C	**0°C**	**27°C**	**80°C**	**125°C**	**155°C**
Intra-HD (%)	98.67	99.34	99.91	98.92	98.5	98.25
Inter-HD (%)	53.28	51.35	49.9	49.78	49.12	48.96
BER (%)	1.33	0.66	0.09	1.08	1.5	1.75

Table 6.4 ST-APUF quality metrics at different supply voltage

	0.8 V	**1 V**	**1.2 V**	**1.8 V**	**2 V**	**2.2 V**
Intra-HD (%)	97.34	98.42	99.25	99.96	99.79	99.5
Inter-HD (%)	58.86	54.15	48.72	49.9	48.36	47.94
BER (%)	2.66	1.58	0.75	0.04	0.21	0.5

The layout of the ST-APUF designed in UMC 180nm excluding the pad ring is shown in Fig.6.13. It contains two different ST circuits to generate a 16-bit response with the dimension of 29μm × 29μm, which gives an approximate area of 0.84mm^3 and is designed for IoT-enabled applications.

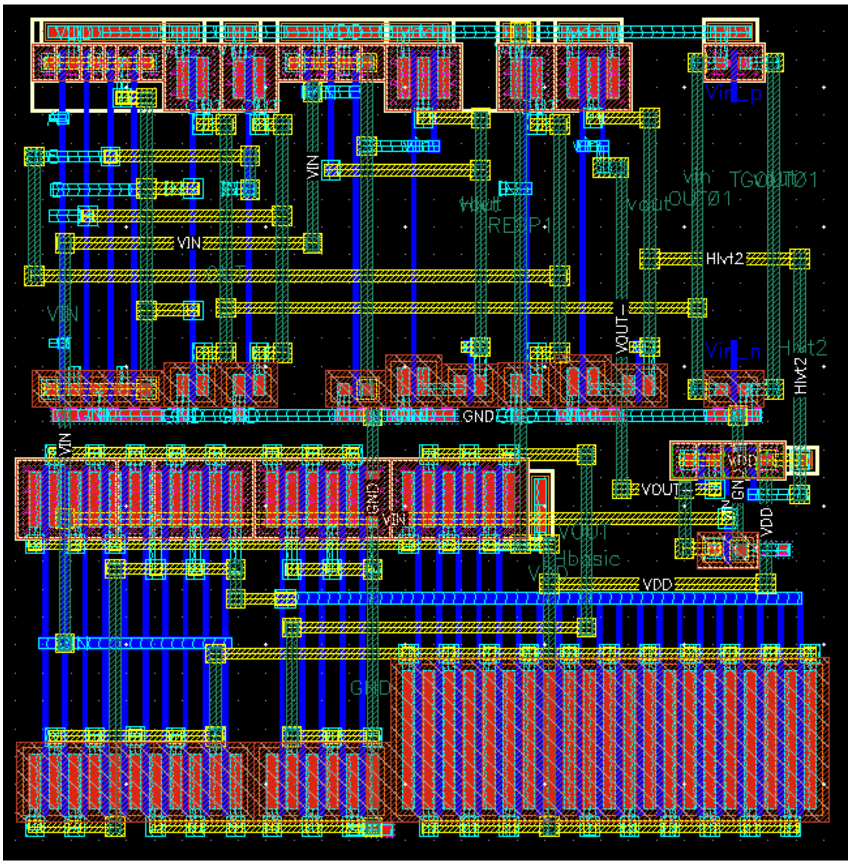


Figure 6.13 Layout of ST-APUF

6.4 Summary

In this chapter, we have introduced the ST arbiter PUF mechanism that has the advantage in complex arbitration and can achieve higher reliability than any other STPUF. The experimental evaluation of ST-APUF shows the uniqueness and reliability of 49.9% and 99.91% respectively, higher than that of the previous works. Moreover, ST-APUF is also highly resistant to attacks since a prediction accuracy of 49% is achieved when LR is applied. Moreover, it shows a higher prediction accuracy of 52% when performed with various ML classifiers. ST-APUF significantly improves upon the previous STPUF designs and has the potential to be the basis for CRP-based identification and authentication applications in constrained IoT devices.

The next chapter will introduce a prominent challenge generation mechanism that feeds the challenges through the PVs obtained according to the power traces that are generated by LDO.

Chapter 7

Low Dropout (LDO) Regulator integrated PUF for improving attack resilience

The strength of the PUFs does not only depend on the PVs inherited by the proposed designs but also depends on the sources of challenge-feeding circuits. In this regard, the power traces from power management circuits can be exploited to augment security. In this direction, the randomness associated with power traces can be explored to enhance security. In this chapter, the power management circuit, a Low Dropout (LDO) regulator is chosen to generate the challenges that are fed to the ReOPUF and ST-APUF which are discussed in Chapter 5 and Chapter 6 respectively. Thereby, the randomness in the challenge generation is enhanced against existing challenge-feeding mechanisms. The main contributions are,

- Challenge-feeding mechanism is deduced from LDO to enhance the randomness of challenges.
- The load transients of LDO reflected by PVs are converted as power traces to get the respective challenges.
- Evaluated the randomness of challenge feeding for ReOPUF and ST-APUF based on the instantaneous power traces generated from LDO.

7.1 Low Dropout (LDO) Regulator

LDO voltage regulators [95–98] are employed to supply voltages to the sudden changes in load conditions, ensuring that the output voltage remains stable even if the current demand from the device changes abruptly. It is a classical linear voltage regulator designed to maintain a constant output voltage with a negligibly small ”drop-out” voltage between the input and output voltages. An LDO consists of an Operational Amplifier (OP-AMP), a voltage reference (V_{REF}), a feedback voltage divider (V_{FB}), and a series pass element (M_{pass}). The fundamental concept of challenge generation is shown in Fig.7.1, where the output voltage (V_{OUT}) should be resistant to changes in ambient temperature and stable over time while being stable with line and load variations. The V_{OUT} values are translated as power traces that are fed as challenges to the existing ReOPUF and ST-APUF. LDO regulators are frequently used in mixed-signal systems to produce local supply voltages for different building blocks. Each LDO's architecture is specific to the cell that it feeds for maximum performance.

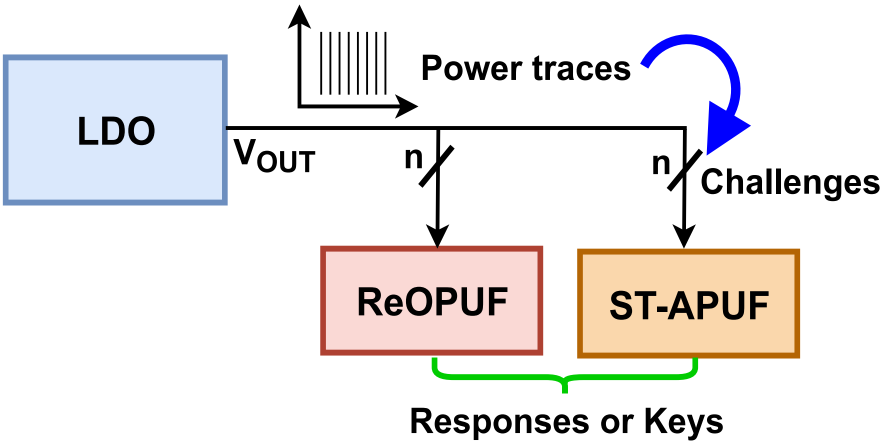


Figure 7.1 Block diagram of LDO challenge generation through power traces

7.1.1 Characterization of LDO

The LDO is chosen to power the ReOPUF and ST-APUF and it is designed to provide 1.5 V regulation. The complete specifications of the regulator circuit for the challenge generation as well as powering the ReOPUF and ST-APUF are deduced and tabulated in Tab.7.1.

- **Dropout voltage:** The dropout voltage ($\mathrm{V}_{DROPOUT}$) [99,100] is the voltage difference between the input and output at which the LDO ceases to be able to control against additional input voltage drops is represented in Eq.7.1. An optimum 100 mV dropout voltage is chosen with the assumption that the minimum input voltage with a safety margin is 1.6 V.

$$V_{DROPOUT} = I_{LOAD} \times R_{DSON} \tag{7.1}$$

- **Efficiency:** The efficiency of an LDO is determined by the ground current and input/output voltages. To have high efficiency, drop-out voltage and quiescent current must be minimized. In addition, the voltage difference between input and output must be minimized, since the power dissipation of LDO regulators accounts for the efficiency. The input-to-output voltage difference is an intrinsic factor in determining the efficiency, regardless of the load conditions. For example, the efficiency of a 1.5 V LDO will never exceed 75% when powered from 2 V. The efficiency of the LDO is calculated by using the following Eq.7.2 [99, 100].

$$Efficiency = \frac{I_{OUT}}{I_{OUT} + I_{GND}} \times \frac{V_{OUT}}{V_{IN}} \times 100\% \tag{7.2}$$

- **Line regulation (LR):** It refers to the ability of a power supply or voltage regulator to maintain its output voltage stable regardless of changes in the input voltage. A smaller value for line regulation indicates a better ability to maintain a constant output voltage as the input voltage changes. An optimum change of 2 mV to 3 mV LR is accepted to fulfill the requirement and its % is expressed using the following Eq.7.3 [99, 100].

$$\text{Line Regulation} = \left(\frac{V_{out(max)} - V_{out(min)}}{V_{out(nominal)}} \right) \times 100\% \tag{7.3}$$

Where:

- $V_{out(max)}$ is the output voltage at the maximum input voltage.
- $V_{out(min)}$ is the output voltage at the minimum input voltage.
- $V_{out(nominal)}$ is the nominal or typical output voltage.

- **Load regulation (LDR):** LDR is the ability of a power source or voltage regulator to maintain a consistent output voltage despite fluctuations in the amount of current drawn by the load. In many applications, the load's current may change, and it is crucial that the output voltage be steady throughout these fluctuations. A 3 mV to 5 mV change of LDR is the finest and its % is calculated using the following Eq.7.4 [99, 100].

$$\text{Load Regulation} = \left(\frac{V_{no-load} - V_{full-load}}{V_{full-load}} \right) \times 100\% \tag{7.4}$$

Where:
- $V_{no-load}$ is the output voltage when no current (or minimal current) is being drawn by the load.
- $V_{full-load}$ is the output voltage when the maximum specified current is being drawn by the load.

The LR and LDR should not contribute more than a 5 mV deviation that guarantees the challenge generation through power traces.

- **Peak Overshoot** The LDO-driven challenge generation is designed to keep load transients as small as 600 mV. To meet the requirement, the peak overshoot/undershoot standard is therefore set at 600 mV, which is considerable for getting the power traces for challenge generation.

- **Power supply rejection ratio (PSRR):** It is also known as ripple rejection and is a measure of LDO regulating ability to attenuate the ripples caused in the power supply. It may be recalled that the LDO receives input from the DC-DC converter setting to improve efficiency. Thus, a significant ripple in the power supply is possible. Therefore, transients can significantly generate power traces to be used for the generation of random challenges. It is sufficient to offer -30 dB attenuation till 1 MHz. PSRR is usually expressed in decibels (dB) and is defined in Eq.7.5 [99,100].

$$\text{PSRR (dB)} = 20 \times \log\left(\frac{\Delta V_{supply}}{\Delta V_{out}}\right) \tag{7.5}$$

Where:
- ΔV_{supply} is the change in the supply voltage.
- ΔV_{out} is the resulting change in the output voltage.

- **Accuracy:** The overall accuracy considers the effects of line regulation (ΔV_{LR}), load regulation (ΔV_{LDR}), reference voltage drift (ΔV_{REF}), and temperature coefficient (ΔV_{TC}). It is defined by the following Eq.7.6 [99, 100].

$$Accuracy \approx \frac{|\Delta V_{LR}| + |V_{LDR}| + \sqrt{\Delta V_{o,ref}^2 + \Delta V_{TC}^2}}{V_{OUT}} \times 100 \tag{7.6}$$

However, the LDO drives a switching circuit (Schmitt trigger) that can tolerate temperature changes. So, it is required that a circuit can significantly generate power traces to be utilized for the generation of random challenges. The overall accuracy normally accounts for the chosen LDO is approximately 1% to 3%.

Table 7.1 Specifications for LDO

Design Parameters		
Aspect ratio (μm) (OP-AMP)	M0, M1	10/0.18
	M2, M3, M4	30/0.18
	M5, M6	10/0.18
	M7	25/0.18
	R_A, R_B	40KΩ
Resistors (in KΩ)	R1	30KΩ
	R2	120KΩ
M_{pass} (μm)	100/0.18	
V_{IN} (V)	1.6 V to 2 V	
V_{REF} (V)	1.2	
V_{OUT} (V)	1.5	
I_{LOAD}	0 mA to 100 mA	
I_{BIAS}	< 100 μA	
PSRR	30 dB @1 MHz	
Settling time (T_S)	< 3 μS	

7.1.2 Implementation of LDO

A chosen LDO [96] needs to use a M_{pass} that operates as a current source rather than a source follower since the voltage drops from V_{DD} to V_{OUT}. The PMOS transistor, which in turn is regulated by the OP-AMP, regulates the output current. The feedback voltage (V_{FB}) from the output (V_{OUT}) is compared to the reference voltage (V_{REF}) in this amplifier, and the difference is amplified. When the V_{FB} falls below the V_{REF}, the gate of the PMOS device is pulled lower, allowing more current to flow and raising the V_{OUT}. The PMOS device's gate is pulled higher if the V_{FB} is higher than the V_{REF}, which reduces the amount of current that may flow and lowers the V_{OUT}. The OP-AMP controls V_{OUT} by varying the gate voltage of M_{pass}. Transistor M_{pass} must deliver a promising

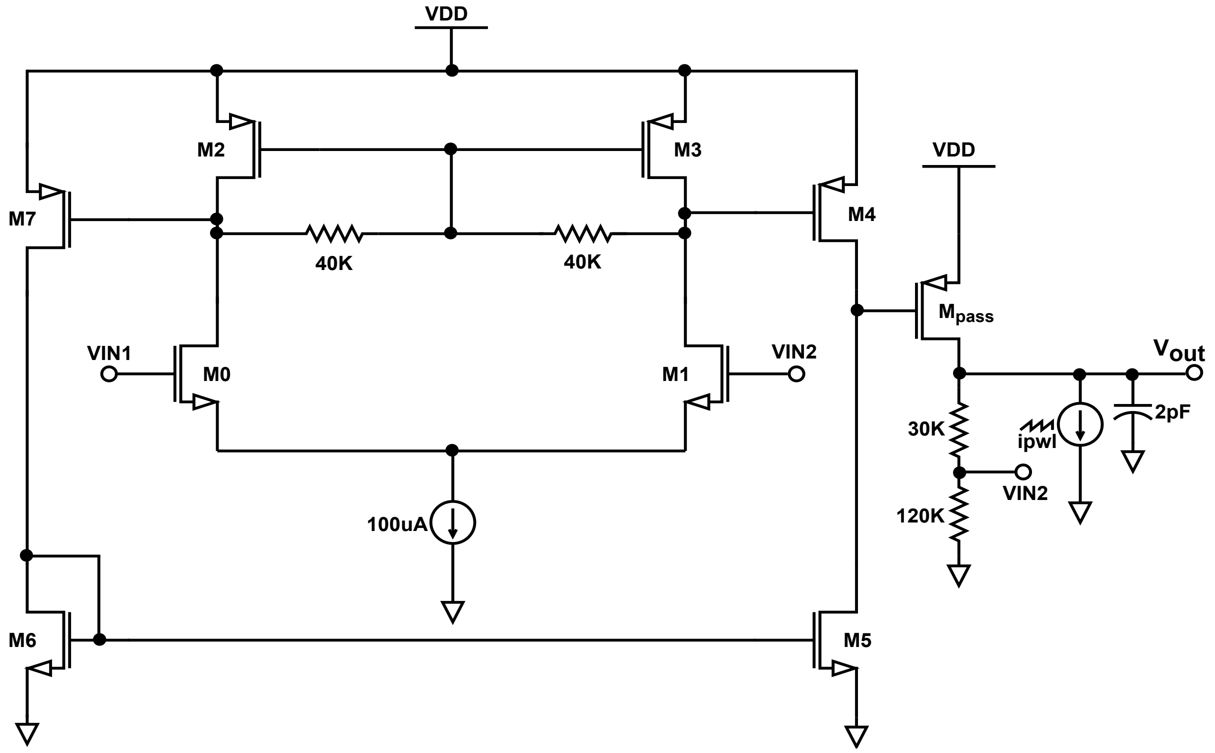


Figure 7.2 Design of LDO [96]

load current of 1 mA in addition to the currents that pass via R1 and R2. As shown in Fig.7.2, the circuit comprises a differential pair and a stage with a current-mirror load. In order to load these nodes as little as possible, resistors R$_a$ and R$_b$ set the Common Mode (CM) level at nodes A and B, respectively.

7.2 Operating regions of LDO

The pass element behaves like a resistor in the dropout zone, with a value equal to the drain-to-source on-resistance (R$_{DSON}$). The pass transistor M$_{pass}$ W/L ≥100μm/0.18 μm is obtained using the following Eq.7.7.

$$I_D = \frac{1}{2}\mu_p C_{ox}\frac{W}{L}\left(V_{SG} - V_{TH}\right)^2 \tag{7.7}$$

The V$_{DROPOUT}$ with R$_{DSON}$ and load current I$_{LOAD}$ are expressed in Eq.7.1. The LDO's V$_{DROPOUT}$ can be used to determine R$_{DSON}$, which includes resistance from the pass element. For example, the R$_{DSON}$ is approximately 1.0, and its worst-case V$_{DROPOUT}$ is 200 mV with a 100 mA load. Other factors like line-and-load regulation, precision, PSRR, and noise have little practical significance because the LDO cannot control the output voltage. The 1.6 V LDO's output voltage and input voltage are displayed in Fig.7.3

respectively. R_{DSON} is around 25kΩ since the usual dropout voltage is 100 mV at 1 A. The dropout region runs from the input voltage of roughly 0.5 V to 1.5 V. The device is inoperable below 0.5 V because the transistors are operating in a cut-off region. The $V_{DROPOUT}$ decreases proportionally with decreasing load currents; for example, at 2 mA, it is 110 mV. The regulator's efficiency is increased by having a low dropout voltage.

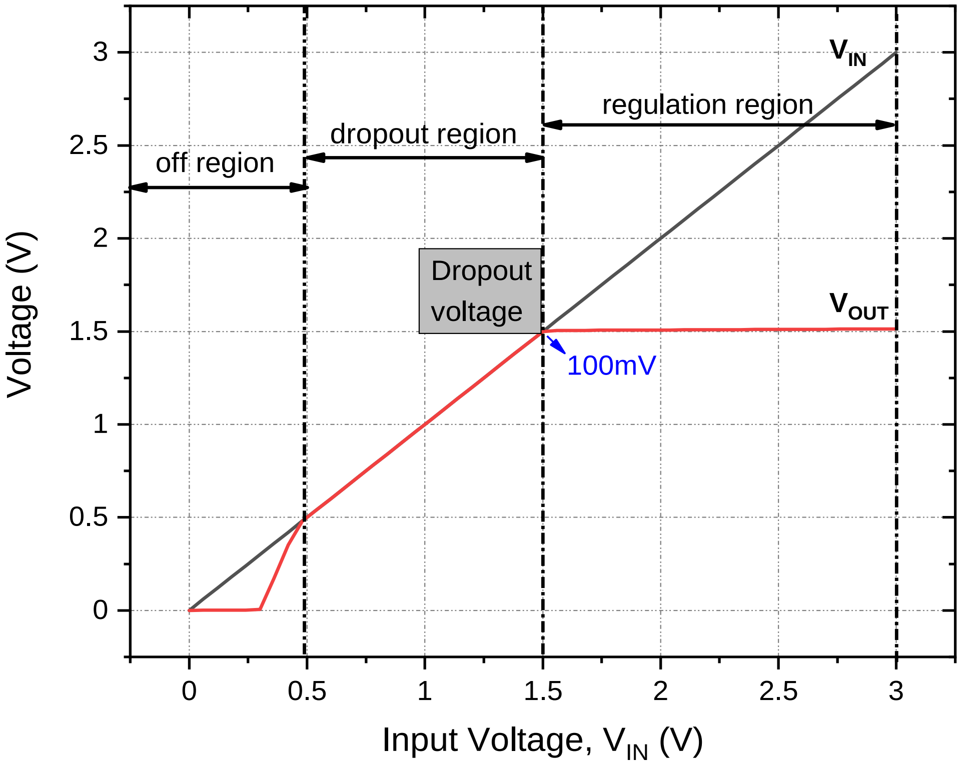


Figure 7.3 Operating regions of LDO

7.2.1 Measurement of power traces from LDO

The extraction of power traces is done from transient responses mimicking the randomness of load transients for LDO are further randomized by ST-APUF and ReOPUF. Thus, the vulnerabilities of challenges to the attacker are significantly downplayed.

7.2.1.1 Analysis of load transients

The LDO regulator's load transient behaviour is shown in Fig.7.4 and Fig.7.5. A reduction in the gate charging current of the M_{pass} and the generation of an overshoot voltage occurs after the load current is decreased to its lowest possible value (i.e. from HIGH to LOW). The I_{M1} increases I_{M3} and I_{M4} when an overshoot voltage occurred. As a result, this current boosts the gate charging current of the M_{pass} to shorten the time that occurs during the settling phase of the minimal load current operation. According to Fig.7.4, there may be some ringing as the voltage settles as it moves from 1.8 V to zero in 1.8 ns. And also, it is observed that an overshoot of 550 mV with I_{LOAD} of 1 mA.

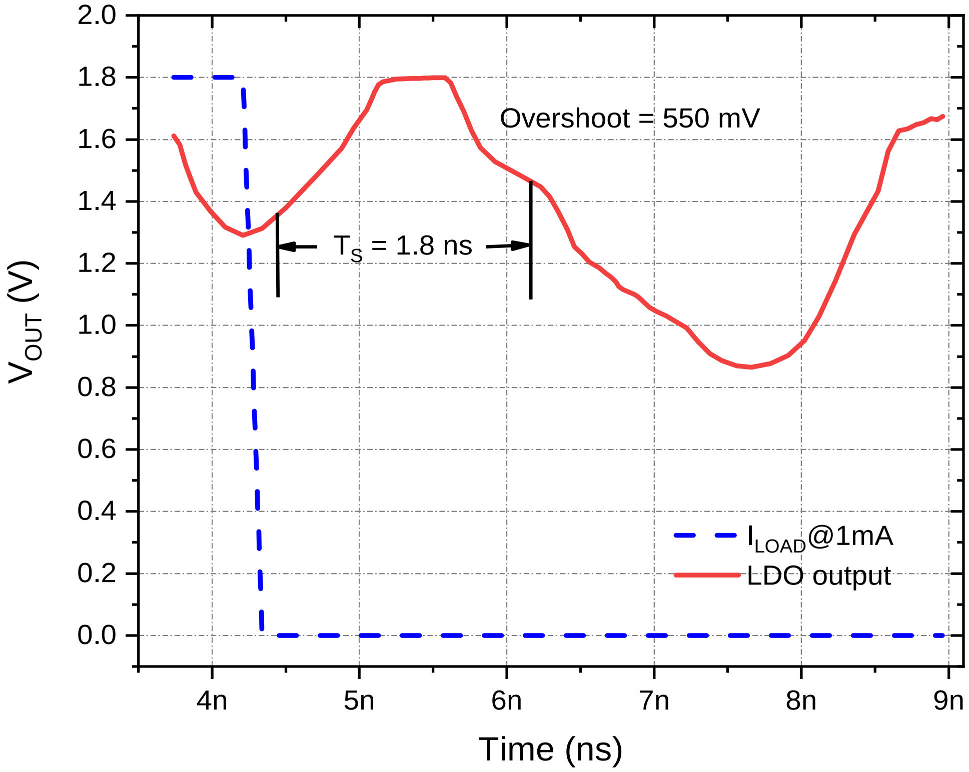


Figure 7.4 Overshoot transient of LDO

The LDO regulator's response to loading transients with load current steps increased from minimum to maximum is shown in Fig.7.5. Due to the voltage difference across the feedback network when an undershoot voltage occurs in the load transient response, the current I_{M1} flowing into the M1 rapidly increases. The gate discharge current I_{GDpass} and the current I_{M0} passing through M0 are both rapidly enhanced by this current. To decrease the undershoot voltage, the gate voltage of the M_{pass} is lowered and the current is raised. When the load current varies from 1 mA to 100 mA with an edge time of 100 μs, the voltage spikes are observed as 470 mV and 156 mV respectively with a settling time (T_S) of 1.8 ns. Similarly, for load currents from 1 mA to 100 mA at 100 μs fall time an overshoot of 450 mV and 120 mV.

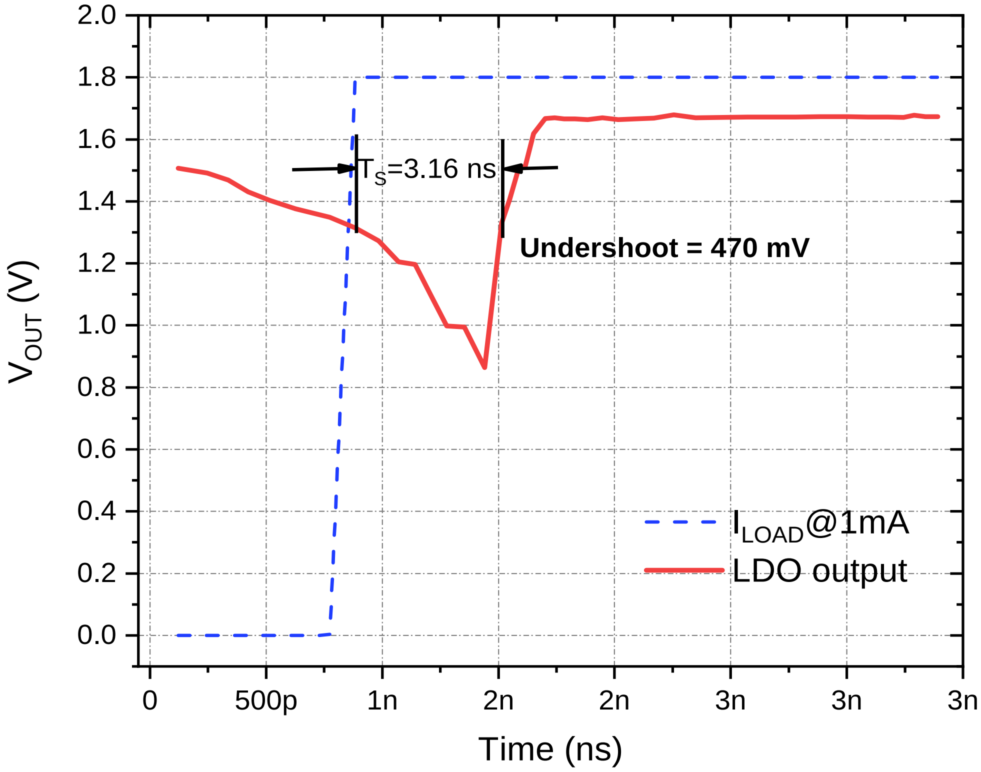


Figure 7.5 Undershoot transient of LDO

7.2.1.2 Analysis of power traces towards security

Secure PUF implementation is possible when the PUF cores are able to withstand possible attacks performed by intruders. In this regard, the PUFs will generate keys based on the inherent PVs borne by either complex design PUF architectures or providing complicated challenge-feeding mechanisms. In both cases, the randomness is evaluated based on the circuit behaviour. Till now, the major concentration is the randomness performed on the obtained keys from PUF instances. However, there is a chance to enhance the randomness of the challenge generators by their indeterministic power traces. With the intention of challenge generation, the obtained power traces from LDO are to be extracted and translated into binary challenges are shown in Fig.7.6. Possibly, to enhance the randomness in the proposed LDO-based challenge generation the key parameters are the power traces. These are captured when load transients are performed at instantaneous I_{LOAD} variations.

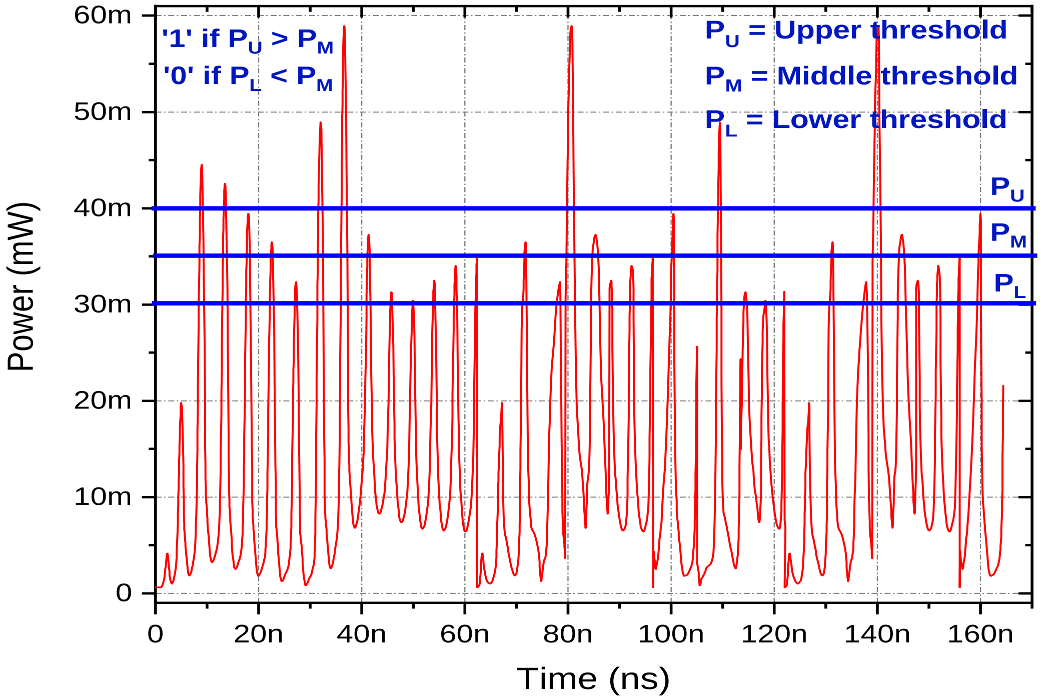


Figure 7.6 Power traces of LDO measured at various I_{LOAD}

The respective power traces are presented in Fig.7.6 that are observed at an I_{LOAD} of 1 mA and they are translated into corresponding challenges based on the threshold level management. Three threshold levels upper threshold (P_U), middle threshold (P_M), and lower threshold (P_L) are considered for extraction of challenges to feed PUFs. The P_M will act as the barrier between two threshold levels (P_U and P_L) to decide whether the challenge is either '0' or '1'. When the power level P_U is greater than P_M then assume the challenge is '1' or the power level P_L is less than PM then the challenge is '0'. For example, at an I_{LOAD} of 1mA, the power traces are decoded as a 16-bit challenge i.e. 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1. This process is continued for an I_{LOAD} of 1mA to 100mA then more challenges will be extracted to feed ReOPUF and ST-APUF that are proposed in Chapter 5 and Chapter 6 respectively. Thus the randomness [101, 102] is evaluated based on the PVs that are observed in terms of power traces. To make them attack-resistant above threshold levels is to be arbitrary.

7.2.2 Evaluation of randomness of challenges of ReOPUF and ST-APUF

The challenge generation mechanism is crucial to feed the PUFs and excite them for response or key generation. Generally, the feeding is done through RNGs with a specific number of trials that lead to randomness based on the frequency of the two values (i.e. '0' or '1'). Accordingly, the frequency is measured from the obtained challenges and it should be ideally 100% (average of '0's and '1's) or 50% (for a '1'). Fig.7.7 illustrates how this unpredictability translates into a likelihood of a "1" of 42.5% (as opposed to a "0" of 57.5%) and 44% (as opposed to a "0" of 56%) when considering the proposed PUFs ReOPUF and ST-APUF respectively. It can be seen that the randomness in the challenges generated from the LDO power traces when driving ReOPUF and ST-APUF are improved as compared to the RNG alone is increased to 45% (as opposed to a "0" of 55%) and 46.5% (as opposed to a "0" of 53.5%) respectively. Considerably, this is promising randomness achieved that is slightly closer to an ideal value of 50%. Since nearly 7 bits (for ReOPUF) and 8 bits (for ST-APUF) of a 16-bit challenge are therefore likely to be '1', this proves that the proposed PUFs when excited with LDO exhibit a high level of randomness.

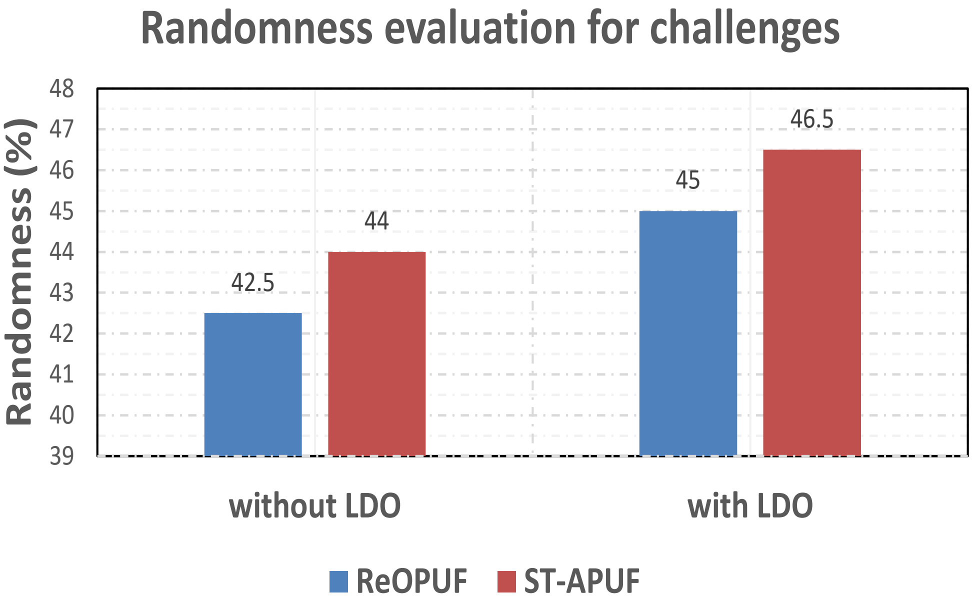


Figure 7.7 Randomness estimation of challenges for ReOPUF and ST-APUF

7.2.3 Evaluation of randomness for responses or keys from ReOPUF or ST-APUF

The assessment of randomness is evaluated for the obtained responses or keys from the proposed PUFs (ReOPUF and ST-APUF) are illustrated in Fig.7.8. The performance is evaluated with 16-bit challenges and keys that are obtained from the ReOPUF and ST-APUF respectively. The implementation and design are performed in Cadence UMC 180 nm technology. The performance metrics are presented in Tab.7.2. It is observed that when the PUFs are feeding without LDO the likelihood of a '1' is 45% (as opposed to a "0" of 55%) and 47% (as opposed to a "0" of 53%). Similarly, when the proposed PUFs are fed with LDO the randomness is estimated as 47% (as opposed to a "0" of 53%) and 48% (as opposed to a "0" of 52%). Significantly, it is approximately 1.5% and 1% rise when contrasted to without LDO feeding. Meanwhile, there is a slight improvement in randomness when feed with LDO is attained. The randomness comparison of ReOPUF and ST-APUF keys with other PUF designs is presented in Tab.7.3. The ReOPUF driven by LDO with power traces has better randomness compared with the conventional APUFs [101, 102], a 27% and 11% enhancement is observed. When the same is observed for ST-APUF the randomness is raised to 29% and 12% respectively. Also, the randomness improvement is observed with [103, 104] there is an enhancement in the randomness of 8.5% and 14.5% for ReOPUF and 9.5% and 15.5% for ST-APUF is attained. So, when the ReOPUF and ST-APUF are excited with the LDO power traces there is promising

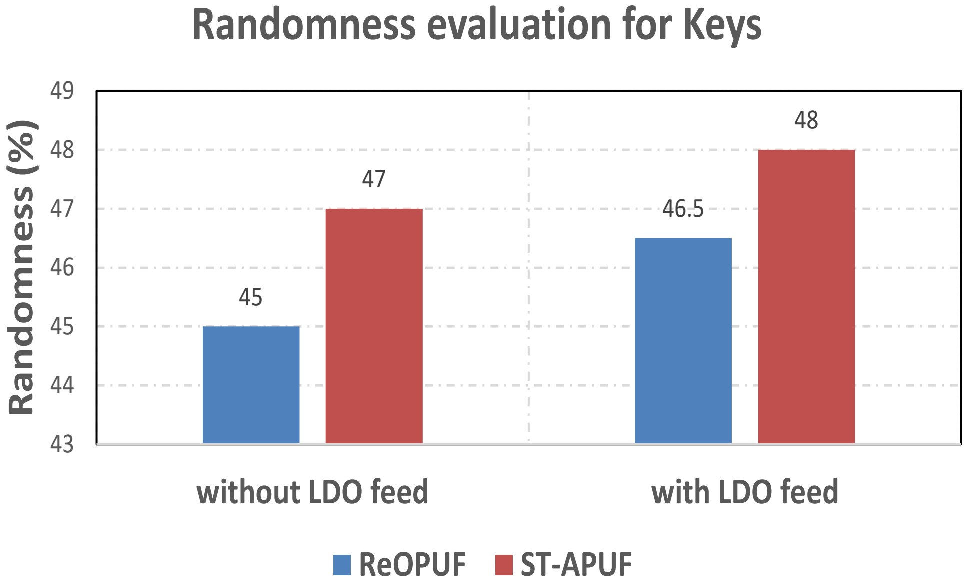


Figure 7.8 Randomness estimation of keys for ReOPUF and ST-APUF

Table 7.2 Performance of randomness for ReOPUF and ST-APUF

Circuit type	**without LDO power traces**		**with LDO power traces (This work)**	
Proposed PUF	**ReOPUF**	**ST-APUF**	**ReOPUF**	**ST-APUF**
No. of bits	16	16	16	16
Randomness (%) (For challenges)	42.5	45	**44**	**46.5**
Randomness (%) (For keys)	45	46.5	**47**	**48**

randomness is attained and it is suitable for security-related applications.

Table 7.3 Comparison of randomness with different PUF designs

References	**PUF Design**	**Randomness (Ideal - 50%)**
Hori et al., 2010 [101]	APUF	34.03
Maiti et al., 2010 [102]	APUF	42.3
Maiti et al., 2010 [102]	ROPUF	46.04
Ibrahim et al., 2022 [103]	APUF	19.57
Cherif et al., 2013 [104]	SRAM	43
Lee et al., 2019 [105]	MRPUF	55
Semb et al., 2021 [106]	APUF	45.4
without LDO power traces	ReOPUF	45
without LDO power traces	ST-APUF	46.5
This work (with LDO power traces)	***ReOPUF***	***47***
This work (with LDO power traces)	***ST-APUF***	***48***

LDOs are frequently the target of side-channel attacks that take advantage of the correlation between input and output voltages and power consumption patterns to deduce sensitive data, including operating settings or cryptographic keys. PUFs can add extra unpredictability or noise to the voltage regulation process by being incorporated into the LDO architecture. This makes it harder for attackers to wrest useful information from side-channel measurements. The danger of side-channel leakage can be further decreased by using PUF-generated identifiers to cryptographically encrypt communication routes between the LDO and other components.

Invasive methods like probing, reverse engineering, or tampering with the circuitry to retrieve critical data or change its operation are frequently used in physical attacks (discussed in Chapter 2) against LDOs. PUFs provide a hardware-based security mechanism that is impervious to tampering and reverse engineering, hence increasing the robustness of LDOs against such attacks. Attackers find it more difficult to disrupt the integrity of the LDO or extract critical data due to the unique PUF responses' difficulty in replication or cloning.

7.3 Summary

In this chapter, the challenges are obtained through the power traces that are generated by LDO. The experimental evaluation confirms that the randomness of the ReOPUF and ST-APUF are enhanced by 2.5% and 1.5% (for challenges), 2% and 1.5% (for keys) respectively. So, LDO-driven PUFs significantly improve the randomness of previous designs and it has the potential to suitable for identification or authentication applications in constrained IoT nodes [107–113].

Finally, the following chapter will provide the overall conclusions concerning the proposed PUF designs and implementations. Subsequently, the possible extensions required for the proposed PUFs are described in the future scope.

Chapter 8

Conclusions and Future Scope

This chapter concludes the thesis by underlining the main contributions. It also presents the possible directions for future work.

8.1 Conclusions

In this thesis, we have implemented different key generation PUF mechanisms for the provision of security to the ICs and evaluated those designs with PUF metrics. Specifically, the intrinsic PVs are aided to showcase the promising uniqueness and reliability. However, the proposed contributions exhibited strong CRPs which help combat various attacks performed by unauthorized users.

- Initially, we started the courses on Analog IC design and Mixed signal design to gain strength in PUF architecture designing and understand the PVs concerning the SVT, LVT and HVT transistors. These are very helpful in leading the novel PUF design implementation in security aspects. Along with them, we also learned Machine learning and its applications in the IC design course which has different ML algorithms and classifiers to validate the performance of PUF designs against various attacks performed by the intruders.

- Introduced delay-based feed-forward arbiter PUF mechanism, XFAPUF has an advantage that compacts challenges feed through complex arbitration can achieve higher reliability than any other APUFs. The experimental evaluation of XFAPUF shows the uniqueness and reliability of 50.03% and 99.81% respectively, higher than that of the previous works. Moreover, XFAPUF is also highly resistant to attacks since a prediction accuracy of 48% is achieved when LR is applied. The compactness by ERD to develop PUF for prototyping ensures that the design incurs better compatibility than reported in the literature to date. Additionally, the chaotic behaviour in the arbitration mechanism of APUF is introduced which has the advantage of higher uniformity and reliability than any other RNG PUFs. Since chaotic activity lacks statistical properties, it is challenging to make assumptions about creating pseudo-random numbers from it. The experimental evaluation of Chaotic APUF shows the uniqueness and reliability of 47.33% and 96.14% respectively, higher than that of the previous works. The chaotic values produced by the previous chaotic systems are related to their system characteristics. The output sequence is confused and rearranged so that the system parameters from the previous run cannot be obtained from the following run, ensuring security. XFAPUF significantly improves upon the previous APUF designs and has the potential to be the basis for CRP-based identification and authentication applications in the IoT. Moreover, the proposed XFAPUF mitigates the common machine learning attack like LR. Despite XFAPUF being strong, it does not have memory retention, which is a major function in memory PUFs to store the secret keys for authentication.

- A robust PUF topology based on the feed-forward arbiter PUF mechanism RC-FAPUF is introduced in Chapter 4. The RC-FAPUF is fed by the automated or independent challenges and realized through PVs that occur in the SCs. The structure of the PUF increases the complexity of the arbitration and makes it more difficult to model attacks. The experimental evaluation of RC-FAPUF provides uniformity (u), diffuseness (D), and reliability (R) of 47.32%, 49.89%, and 99.91% respectively, better than that of state-of-the-art designs. Moreover, it is highly resistant to ML attacks when LR and ML classifiers are applied achieving the best prediction accuracy of 48% and 52.7%, respectively. The RC-FAPUF significantly improves the reliability of CRP-based PUF designs and also has the potential to implement security in IoT-enabled devices for identification and authentication. Despite being strong and highly random the RC-FAPUF doesn't have a memory function to store the responses for authentication applications.

- A relaxation oscillator-based PUF mechanism is introduced in Chapter 5 as a replacement for RO PUFs. ReOPUF has the advantage that challenges fed through simple oscillation can achieve more reliability than any other oscillator PUFs. The experimental evaluation of ReOPUF shows the uniqueness and reliability of 49.22% and 97.97% respectively, which achieves higher than that of the previous works. ReOPUF significantly improves upon the previous ROPUF designs, and has the potential to be the basis for CRPs-based identification and authentication applications designed for IoT.

- The Schmitt Trigger Arbiter PUF mechanism is designed and implemented in Chapter 6 to attain the advantage in complex arbitration and can achieve higher reliability than any other STPUF. The experimental evaluation of ST-APUF shows the uniqueness and reliability of 49.9% and 99.91% respectively, higher than that of the previous works. Moreover, ST-APUF is also highly resistant to attacks with a prediction accuracy of 49% is achieved when LR is applied. Moreover, it shows a higher prediction accuracy of 52% when performed with various ML classifiers. ST-APUF significantly improves upon the previous STPUF designs and has the potential to be the basis for CRP-based identification and authentication applications in constrained IoT devices.

- An LDO-based feed challenge mechanism is proposed to enhance the randomness with respect to challenges and keys. The performance of randomness for ReOPUF and ST-APUF is enhanced up to 2% and 1.5% respectively against non-driven feed with LDO. Further, an attempt is made to exploit the LDO power traces to improve the randomness. However, the addition of LDO could lead the PUF to be strong and attack-resistant.

8.2 Future Scope

The work proposed in this thesis can be extended for future research. Some of the possible directions in which the problems can be further pursued are:

- The APUFs presented in Chapter 3 are based on the manual or circuit-based challenge feeding mechanism. Even though the feed-forward concept is proposed there is a provision for replacing feeding with D-Flip-flops, SR Flip-flops, Transmission gates etc.

- As presented in Chapter 4, automation is achieved in challenge feeding by placing XoR gates at each end of the SC. In fact, more timing mismatches occurred between the SCs during execution. So, to eliminate the timing constraints some buffers should be placed by the SCs.
- The design of weak PUF presented in Chapter 5 for key generation based on frequency deviation can convert strong PUF design by making arbitration between the sets.
- The strong CRP generation achieved through ST-APUF which is proposed in Chapter 6 can be extended by replacing advanced or modified ST designs in the place of conventional STs.
- The randomness can be further improved by employing any critical subsystem switching pattern to generate the power traces.

Publications

List of International Journals:

1. Raveendra Podeti, Sreehari Rao Patri and Muralidhar Pullakandam, ”Highly reliable XoR Feed Arbiter Physical Unclonable Function (XFAPUF) in 180nm process for IoT security”, *Microprocessors and Microsystems*, 87 (2021): 104355. **(SCI-Indexed)**

2. Raveendra Podeti, Sreehari Rao Patri and Muralidhar Pullakandam, ”Recursive Challenge Feed Arbiter Physical Unclonable Function (RC-FAPUF) In 180nm Process for Reliable Key Generation In IoT Security”, *IETE Technical Review*, pp.1-12 (2023). **(SCI-Indexed)**

3. Raveendra Podeti, Sreehari Rao Patri and Muralidhar Pullakandam, ”Schmitt Trigger (ST)-Arbiter Physical Unclonable Function (APUF) with enhanced reliability in key generation for IoT-constrained devices”, *Microelectronics*, (2023). **(SCI-Indexed)** (Under review)

4. Raveendra Podeti, Sreehari Rao Patri and Muralidhar Pullakandam, ”LDO driven challenge generation for PUFs to augment security through power traces for IoT-constrained devices”, ***Patent filed***, (2023). (Under review)

List of International Conferences:

1. Raveendra Podeti, Sreehari Rao Patri and Muralidhar Pullakandam, ”ReOPUF: Relaxation Oscillator Physical Unclonable Function for Reliable Key Generation in IoT Security”, in *IFIP International Internet of Things Conference (pp. 163-179). Cham: Springer International Publishing, 2021.*

2. Raveendra Podeti, Sreehari Rao Patri and Muralidhar Pullakandam, ”The chaotic-based challenge feed mechanism for Arbiter Physical Unclonable Functions (APUFs) with enhanced reliability in IoT security” in *IEEE International Symposium on Smart Electronic Systems (iSES) (pp. 118-123), IEEE 2022.*

Bibliography

[1] A. Babaei and G. Schiele, “Physical unclonable functions in the internet of things: State of the art and open challenges,” *Sensors*, vol. 19, no. 14, p. 3208, 2019.

[2] M. Potkonjak and V. Goudar, “Public physical unclonable functions,” *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1142–1156, 2014.

[3] S. Razdan and S. Sharma, “Internet of medical things (IoMT): Overview, emerging technologies, and case studies,” *IETE technical review*, vol. 39, no. 4, pp. 775–788, 2022.

[4] H. Idriss, T. Idriss, and A. Magdy, “A highly reliable delay-based arbiter PUF architecture.”

[5] A. Ometov, P. Masek, L. Malina, R. Florea, J. Hosek, S. Andreev, J. Hajny, J. Niutanen, and Y. Koucheryavy, “Feasibility characterization of cryptographic primitives for constrained (wearable) iot devices,” in *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*. IEEE, 2016, pp. 1–6.

[6] A. Hamza and B. Kumar, “A review paper on DES, AES, RSA encryption standards,” in *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*. IEEE, 2020, pp. 333–338.

[7] A. Sadr and M. Zolfaghari-Nejad, “Physical unclonable function (PUF) based random number generator,” *arXiv preprint arXiv:1204.2516*, 2012.

[8] L. Wang and H. Cheng, “Pseudo-random number generator based on logistic chaotic system,” *Entropy*, vol. 21, no. 10, p. 960, 2019.

[9] V. A. Thakor, M. A. Razzaque, and M. R. Khandaker, “Lightweight cryptography algorithms for resource-constrained iot devices: A review, comparison and research opportunities,” *IEEE Access*, vol. 9, pp. 28 177–28 193, 2021.

[10] M. H. Abu-Rahma and M. Anis, “Variability in VLSI circuits: Sources and design considerations,” in *2007 IEEE International Symposium on Circuits and Systems.* IEEE, 2007, pp. 3215–3218.

[11] W. Liang, B. Liao, J. Long, Y. Jiang, and L. Peng, “Study on PUF based secure protection for IC design,” *Microprocessors and Microsystems*, vol. 45, pp. 56–66, 2016.

[12] J. W. Lee, D. 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,” in *2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No. 04CH37525).* IEEE, 2004, pp. 176–179.

[13] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, “Extracting secret keys from integrated circuits,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, no. 10, pp. 1200–1205, 2005.

[14] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in *2007 44th ACM/IEEE Design Automation Conference.* IEEE, 2007, pp. 9–14.

[15] C. W. O’donnell, G. E. Suh, and S. Devadas, “PUF-based random number generation,” *MIT CSAIL CSG Technical Memo*, vol. 481, 2004.

[16] E. I. Milovanović, M. K. Stojčev, I. Ž. Milovanović, T. R. Nikolić, and Z. Stamenković, “Concurrent generation of pseudo random numbers with LFSR of fibonacci and galois type,” *Computing and Informatics*, vol. 34, no. 4, pp. 941–958, 2015.

[17] A. Maiti, R. Nagesh, A. Reddy, and P. Schaumont, “Physical unclonable function and true random number generator: a compact and scalable implementation,” in *Proceedings of the 19th ACM Great Lakes symposium on VLSI*, 2009, pp. 425–428.

[18] I. Diop, Y. Linge, T. Ordas, P.-Y. Liardet, and P. Maurine, “From theory to practice: horizontal attacks on protected implementations of modular exponentiations,” *Journal of Cryptographic Engineering*, vol. 9, pp. 37–52, 2019.

[19] B. Habib and K. Gaj, “A comprehensive set of schemes for PUF response generation,” *Microprocessors and Microsystems*, vol. 51, pp. 239–251, 2017.

[20] A. K. Boke, S. Nakhate, and A. Rajawat, “Efficient key generation techniques for securing iot communication protocols,” *IETE Technical Review*, vol. 38, no. 3, pp. 282–293, 2021.

[21] Z. Paral and S. Devadas, “Reliable and efficient PUF-based key generation using pattern matching,” in *2011 IEEE international symposium on hardware-oriented security and trust*. IEEE, 2011, pp. 128–133.

[22] A. Fratalocchi, A. Fleming, C. Conti, and A. Di Falco, “NIST-certified secure key generation via deep learning of physical unclonable functions in silica aerogels,” *Nanophotonics*, vol. 10, no. 1, pp. 457–464, 2020.

[23] Y. Xu, H. Ning, L. Mao, Y. Li, and L. Zhang, “Improve symmetry of arbiter in APUF,” *Mathematical Foundations of Computing*, vol. 1, no. 3, p. 281, 2018.

[24] M. Majzoobi, F. Koushanfar, and M. Potkonjak, “Lightweight secure PUFs,” in *2008 IEEE/ACM International Conference on Computer-Aided Design*. IEEE, 2008, pp. 670–673.

[25] M. A. Alamro, K. T. Mursi, Y. Zhuang, A. O. Aseeri, and M. S. Alkatheiri, “Robustness and unpredictability for double arbiter PUFs on silicon data: Performance evaluation and modeling accuracy,” *Electronics*, vol. 9, no. 5, p. 870, 2020.

[26] D. P. Sahoo, R. S. Chakraborty, and D. Mukhopadhyay, “Towards ideal arbiter PUF design on xilinx FPGA: A practitioner’s perspective,” in *2015 Euromicro Conference on Digital System Design*. IEEE, 2015, pp. 559–562.

[27] T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama, “Implementation of double arbiter PUF and its performance evaluation on FPGA,” in *The 20th Asia and South Pacific Design Automation Conference*. IEEE, 2015, pp. 6–7.

[28] M. A. Alamro, Y. Zhuang, A. O. Aseeri, and M. S. Alkatheiri, "Examination of double arbiter PUFs on security against machine learning attacks," in *2019 IEEE International Conference on Big Data (Big Data)*. IEEE, 2019, pp. 3165–3171.

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

[30] C. Gu, Y. Cui, N. Hanley, and M. O'Neill, "Novel lightweight FF-APUF design for FPGA," in *2016 29th IEEE International System-on-Chip Conference (SOCC)*. IEEE, 2016, pp. 75–80.

[31] S. S. Avvaru, Z. Zeng, and K. K. Parhi, "Homogeneous and heterogeneous feed-forward XOR physical unclonable functions," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2485–2498, 2020.

[32] C. Gu, W. Liu, Y. Cui, N. Hanley, M. O'Neill, and F. Lombardi, "A flip-flop based arbiter physical unclonable function (APUF) design with high entropy and uniqueness for FPGA implementation," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 4, pp. 1853–1866, 2019.

[33] P. Simons, E. van der Sluis, and V. van der Leest, "Buskeeper PUFs, a promising alternative to d flip-flop PUFs," in *2012 IEEE International Symposium on Hardware-Oriented Security and Trust*. IEEE, 2012, pp. 7–12.

[34] F. Bernard, V. Fischer, C. Costea, and R. Fouquet, "Implementation of ring-oscillators-based physical unclonable functions with independent bits in the response," *International Journal of Reconfigurable Computing*, vol. 2012, 2012.

[35] M. Gao, K. Lai, and G. Qu, "A highly flexible ring oscillator PUF," in *Proceedings of the 51st Annual Design Automation Conference*, 2014, pp. 1–6.

[36] S. S. Mansouri and E. Dubrova, "Ring oscillator physical unclonable function with multi-level supply voltages," in *2012 IEEE 30th International Conference on Computer Design (ICCD)*. IEEE, 2012, pp. 520–521.

[37] E. Avaroğlu, "The implementation of ring oscillator based PUF designs in field programmable gate arrays using of different challenge," *Physica A: Statistical Mechanics and its Applications*, vol. 546, p. 124291, 2020.

[38] Y. Zhang, H. Liang, L. Yao, M. Yi, Z. Huang, and Y. Lu, "A high reliability physically unclonable function based on multiple tunable ring oscillator," *Microelectronics Journal*, vol. 117, p. 105263, 2021.

[39] M. T. Rahman, D. Forte, J. Fahrny, and M. Tehranipoor, "ARO-PUF: An aging-resistant ring oscillator PUF design," in *2014 design, automation & test in Europe conference & Exhibition (DATE).* IEEE, 2014, pp. 1–6.

[40] C. Q. Liu, Y. Cao, and C. H. Chang, "ACRO-PUF: A low-power, reliable and aging-resilient current starved inverter-based ring oscillator physical unclonable function," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 12, pp. 3138–3149, 2017.

[41] S. R. Sahoo, S. Kumar, K. Mahapatra, and A. Swain, "A novel aging tolerant RO-PUF for low power application," in *2016 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS).* IEEE, 2016, pp. 187–192.

[42] Y. Cao, L. Zhang, C.-H. Chang, and S. Chen, "A low-power hybrid RO PUF with improved thermal stability for lightweight applications," *IEEE Transactions on computer-aided design of integrated circuits and systems*, vol. 34, no. 7, pp. 1143–1147, 2015.

[43] V. Laguduva, S. A. Islam, S. Aakur, S. Katkoori, and R. Karam, "Machine learning based iot edge node security attack and countermeasures," in *2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI).* IEEE, 2019, pp. 670–675.

[44] Y. Cui, C. Gu, C. Wang, M. O'Neill, and W. Liu, "Ultra-lightweight and reconfigurable tristate inverter based physical unclonable function design," *Ieee Access*, vol. 6, pp. 28 478–28 487, 2018.

[45] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "The butterfly PUF protecting IP on every FPGA," in *2008 IEEE International Workshop on Hardware-Oriented Security and Trust.* IEEE, 2008, pp. 67–70.

[46] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Rührmair, "The bistable ring PUF: A new architecture for strong physical unclonable functions," in *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*. IEEE, 2011, pp. 134–141.

[47] S. Sutar, A. Raha, and V. Raghunathan, "Memory-based combination PUFs for device authentication in embedded systems," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 4, no. 4, pp. 793–810, 2018.

[48] Z. Guo, X. Xu, M. T. Rahman, M. M. Tehranipoor, and D. Forte, "SCARe: An SRAM-based countermeasure against IC recycling," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 26, no. 4, pp. 744–755, 2017.

[49] H. Zhang, C. Wang, C. Yan, Y. Cui, C. Gu, M. O'Neill, and W. Liu, "A dynamic highly reliable SRAM-based PUF retaining memory function," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2021, pp. 1–5.

[50] S. Sakib, M. T. Rahman, A. Milenković, and B. Ray, "Flash memory based physical unclonable function," in *2019 SoutheastCon*. IEEE, 2019, pp. 1–6.

[51] J. Li, Y. Cui, C. Gu, C. Wang, W. Liu, and F. Lombardi, "A physical unclonable function using a configurable tristate hybrid scheme with non-volatile memory," *IEEE Open Journal of Nanotechnology*, vol. 2, pp. 31–40, 2021.

[52] S. Khan, A. P. Shah, S. S. Chouhan, S. Rani, N. Gupta, J. G. Pandey, and S. K. Vishvakarma, "Utilizing manufacturing variations to design a tri-state flip-flop PUF for iot security applications," *Analog Integrated Circuits and Signal Processing*, vol. 103, no. 3, pp. 477–492, 2020.

[53] S. Tao and E. Dubrova, "MVL-PUFs: Multiple-valued logic physical unclonable functions," *International Journal of Circuit Theory and Applications*, vol. 45, no. 2, pp. 292–304, 2017.

[54] N. G. Jayasankaran, A. S. Borbon, E. Sanchez-Sinencio, J. Hu, and J. Rajendran, "Towards provably-secure analog and mixed-signal locking against overproduction," in *Proceedings of the International Conference on Computer-Aided Design*, 2018, pp. 1–8.

[55] S. Tao and E. Dubrova, "Ultra-energy-efficient temperature-stable physical unclonable function in 65 nm CMOS," *Electronics Letters*, vol. 52, no. 10, pp. 805–806, 2016.

[56] L. Lin, D. Holcomb, D. K. Krishnappa, P. Shabadi, and W. Burleson, "Low-power sub-threshold design of secure physical unclonable functions," in *Proceedings of the 16th ACM/IEEE international symposium on Low power electronics and design*, 2010, pp. 43–48.

[57] R. De Rose, F. Crupi, M. Lanuzza, and D. Albano, "A physical unclonable function based on a 2-transistor subthreshold voltage divider," *International Journal of Circuit Theory and Applications*, vol. 45, no. 2, pp. 260–273, 2017.

[58] Q. Zhao, Y. Cao, X. Zhao, and C. H. Chang, "A current comparator-based physical unclonable function with high reliability and energy efficiency," in *2018 IEEE 23rd International Conference on Digital Signal Processing (DSP)*. IEEE, 2018, pp. 1–4.

[59] Z. Wang, Y. Chen, A. Patil, C.-H. Chang, and A. Basu, "Current mirror array: A novel lightweight strong PUF topology with enhanced reliability," in *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2017, pp. 1–4.

[60] Z. Huang, J. Zhong, C. Xie, R. Wu, and X. Zhao, "A highly reliable and energy-efficient schmitt trigger PUF featuring ultra-wide supply voltage range," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 5, pp. 2428–2432, 2022.

[61] S. Khan, S. Azeemuddin, and M. A. Sohel, "Prohys PUF: A proteresis-hysteresis switch based physical unclonable function," *Integration*, vol. 89, pp. 207–216, 2023.

[62] M. R. Elmezayen, W. Hu, A. M. Maghraby, I. T. Abougindia, and S. U. Ay, "Accurate analysis and design of integrated single input schmitt trigger circuits," *Journal of Low Power Electronics and Applications*, vol. 10, no. 3, p. 21, 2020.

[63] B. Dokic, "CMOS schmitt triggers," in *IEE Proceedings G. Electronic Circuits and Systems*, vol. 131, 1984, pp. 197–202.

[64] A. Kumar and R. S. Mishra, "Challenge-response pair (CRP) generator using schmitt trigger physical unclonable function," in *Advanced Computing and Communication Technologies: Proceedings of the 11th ICACCT 2018.* Springer, 2019, pp. 213–223.

[65] Y. Cao, W. Zheng, X. Zhao, and C.-H. Chang, "An energy-efficient current-starved inverter based strong physical unclonable function with enhanced temperature stability," *IEEE Access*, vol. 7, pp. 105 287–105 297, 2019.

[66] R. Liu, P.-Y. Chen, X. Peng, and S. Yu, "X-point PUF: Exploiting sneak paths for a strong physical unclonable function design," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 65, no. 10, pp. 3459–3468, 2018.

[67] Q. Li, F. Chen, J. Kang, P. Wang, J. Su, F. Huang, M. Li, and J. Zhang, "Intrinsic random optical features of the electronic packages as physical unclonable functions for internet of things security," *Advanced Photonics Research*, vol. 3, no. 6, p. 2100207, 2022.

[68] C. Xu, J. Zhang, M.-K. Law, X. Zhao, P.-I. Mak, and R. P. Martins, "An n× n multiplier-based multi-bit strong PUF using path delay extraction," in *2020 IEEE International Symposium on Circuits and Systems (ISCAS).* IEEE, 2020, pp. 1–5.

[69] C. Gu, N. Hanley, and M. O'neill, "Improved reliability of FPGA-based PUF identification generator design," *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, vol. 10, no. 3, pp. 1–23, 2017.

[70] S. Tripathy, V. K. Rai, and J. Mathew, "MARPUF: physical unclonable function with improved machine learning attack resistance," *IET Circuits, Devices & Systems*, vol. 15, no. 5, pp. 465–474, 2021.

[71] L. Yu, X. Wang, F. Rahman, and M. Tehranipoor, "Interconnect-based PUF with signature uniqueness enhancement," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 28, no. 2, pp. 339–352, 2019.

[72] P. H. Nguyen, D. P. Sahoo, C. Jin, K. Mahmood, U. Rührmair, and M. Van Dijk, "The interpose PUF: Secure PUF design against state-of-the-art machine learning attacks," *Cryptology ePrint Archive*, 2018.

[73] Y. Fang, C. Wang, Q. Ma, C. Gu, M. O'Neill, and W. Liu, "Attacking arbiter PUFs using various modeling attack algorithms: A comparative study," in *2018 IEEE Asia pacific conference on circuits and systems (APCCAS).* IEEE, 2018, pp. 394–397.

[74] P. K. Sadhu and V. P. Yanambaka, "MC-PUF: A robust lightweight controlled physical unclonable function for resource constrained environments," in *2022 IEEE computer society annual symposium on VLSI (ISVLSI).* IEEE, 2022, pp. 452–453.

[75] P. Williams, H. Idriss, and M. Bayoumi, "Mc-PUF: Memory-based and machine learning resilient strong PUF for device authentication in internet of things," in *2021 IEEE international conference on cyber security and resilience (CSR).* IEEE, 2021, pp. 61–65.

[76] S. P. Skorobogatov, "Semi-invasive attacks–a new approach to hardware security analysis," University of Cambridge, Computer Laboratory, Tech. Rep., 2005.

[77] Y.-i. Hayashi, N. Homma, T. Sugawara, T. Mizuki, T. Aoki, and H. Sone, "Non-invasive trigger-free fault injection method based on intentional electromagnetic interference," in *Non-Invasive Attack Testing Workshop (NIAT)*, 2011.

[78] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proceedings of the 17th ACM conference on Computer and communications security*, 2010, pp. 237–249.

[79] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, "PUF modeling attacks on simulated and silicon data," *IEEE transactions on information forensics and security*, vol. 8, no. 11, pp. 1876–1891, 2013.

[80] N. Wisiol, "Towards attack resilient arbiter PUF-based strong PUFs," *Cryptology ePrint Archive*, 2021.

[81] S. Khalfaoui, J. Leneutre, A. Villard, I. Gazeau, J. Ma, and P. Urien, "Security analysis of machine learning-based PUF enrollment protocols: a review," *Sensors*, vol. 21, no. 24, p. 8415, 2021.

[82] F.-X. Standaert, "Introduction to side-channel attacks," *Secure integrated circuits and systems*, pp. 27–42, 2010.

[83] S. Buchovecká, R. Lórencz, F. Kodỳtek, and J. Buček, "True random number generator based on ring oscillator PUF circuit," *Microprocessors and Microsystems*, vol. 53, pp. 33–41, 2017.

[84] J. Cui, M. Yi, D. Cao, L. Yao, X. Wang, H. Liang, Z. Huang, H. Qi, T. Ni, and Y. Lu, "Design of true random number generator based on multi-stage feedback ring oscillator," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 3, pp. 1752–1756, 2021.

[85] K. Gołofit and P. Z. Wieczorek, "Chaos-based physical unclonable functions," *Applied Sciences*, vol. 9, no. 5, p. 991, 2019.

[86] A. Zacharias, C. Gisha, and B. A. Jose, "Chaotic ring oscillator based true random number generator implementations in FPGA," in *2020 24th International Symposium on VLSI Design and Test (VDAT)*. IEEE, 2020, pp. 1–6.

[87] L. L. Bonilla, M. Alvaro, and M. Carretero, "Chaos-based true random number generators," *Journal of Mathematics in Industry*, vol. 7, pp. 1–17, 2016.

[88] C.-K. Pham, "CMOS schmitt trigger circuit with controllable hysteresis using logical threshold voltage control circuit," in *6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007)*. IEEE, 2007, pp. 48–53.

[89] C. W. Lin and S. Ghosh, "A family of schmitt-trigger-based arbiter-PUFs and selective challenge-pruning for robustness and quality," in *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2015, pp. 32–37.

[90] A. S. Vidhyadharan and S. Vidhyadharan, "Improved hetero-junction TFET-based schmitt trigger designs for ultra-low-voltage VLSI applications," *World Journal of Engineering*, vol. 18, no. 5, pp. 750–759, 2021.

[91] X. Xu, W. Burleson, and D. E. Holcomb, "Using statistical models to improve the reliability of delay-based PUFs," in *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 2016, pp. 547–552.

[92] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," *Embedded systems design with FPGAs*, pp. 245–267, 2013.

[93] C. Böhm, M. Hofer, C. Böhm, and M. Hofer, "Testing and specification of PUFs," *Physical Unclonable Functions in Theory and Practice*, pp. 69–86, 2013.

[94] S. Shukla, S. Thakur, S. Hussain, J. G. Breslin, and S. M. Jameel, "Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model," *Internet of Things*, vol. 15, p. 100422, 2021.

[95] A. REVERSE, "The fundamentals of LDO design and application."

[96] B. Razavi, "The design of an LDO regulator [the analog mind]," *IEEE Solid-State Circuits Magazine*, vol. 14, no. 2, pp. 7–17, 2022.

[97] S. R. Patri, S. Alapati, S. Chowdary, and K. Prasad, "250mA ultra low drop out regulator with high slew rate double recycling folded cascode error amplifier," in *18th International Symposium on VLSI Design and Test*, 2014, pp. 1–5.

[98] P. S. Rao and K. Krishna Prasad, "On-chip LDO voltage regulator with improved transient response in 180nm," in *2008 International Conference on Electronic Design*, 2008, pp. 1–6.

[99] G. Morita, "Understand low dropout regulator (LDO) concepts to achieve optimal designs," *Analog Dialogue*, vol. 48, no. 12, 2014.

[100] T. Instruments, "Understanding the terms and definitions of LDO voltage regulators," *Texas Instruments Inc., SLVA079, Dallas, TX, USA*, 1999.

[101] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs," in *2010 International conference on reconfigurable computing and FPGAs*. IEEE, 2010, pp. 298–303.

[102] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of RO-PUF," in *2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. IEEE, 2010, pp. 94–99.

[103] H. M. Ibrahim, H. Abunahla, B. Mohammad, and H. AlKhzaimi, “Memristor-based PUF for lightweight cryptographic randomness,” *Scientific reports*, vol. 12, no. 1, p. 8633, 2022.

[104] Z. Cherif, J.-L. Danger, F. Lozac’h, Y. Mathieu, and L. Bossuet, “Evaluation of delay PUFs on CMOS 65 nm technology: ASIC vs FPGA,” in *Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy*, 2013, pp. 1–8.

[105] J. Lee, D.-W. Jee, and D. Jeon, “Power-up control techniques for reliable SRAM PUF,” *IEICE Electronics Express*, vol. 16, no. 13, pp. 20 190 296–20 190 296, 2019.

[106] R. L. Sembiring, R. R. Pahlevi, and P. Sukarno, “Randomness, uniqueness, and steadiness evaluation of physical unclonable functions,” in *2021 9th International Conference on Information and Communication Technology (ICoICT)*. IEEE, 2021, pp. 429–433.

[107] S. P. Mohanty, *Nanoelectronic mixed-signal system design.* McGraw-Hill Education New York, 2015, no. 0071825711.

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

[109] A. Sengupta and S. P. Mohanty, *IP core protection and hardware-assisted security for consumer electronics.* Institution of Engineering and Technology, 2019.

[110] V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making use of manufacturing process variations: A dopingless transistor based-PUF for hardware-assisted security,” *IEEE Transactions on Semiconductor Manufacturing*, vol. 31, no. 2, pp. 285–294, 2018.

[111] V. K. Bathalapalli, S. P. Mohanty, E. Kougianos, V. Iyer, and B. Rout, “iTPM: Exploring PUF-based keyless TPM for security-by-design of smart electronics,” in *2023 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 2023, pp. 1–6.

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

[113] V. K. Bathalapalli, S. P. Mohanty, E. Kougianos, B. K. Baniya, and B. Rout, "Pufchain 2.0: Hardware-assisted robust blockchain for sustainable simultaneous device and data security in smart healthcare," *SN Computer Science*, vol. 3, no. 5, p. 344, 2022.