SRAM-BASED RO PUF ARCHITECTURE FOR EDGE DEVICES

Ph.D. Thesis

by

NEHA MAHESHWARI

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY
INDORE
December, 2025

SRAM-BASED RO PUF ARCHITECTURE FOR EDGE DEVICES

A THESIS

Submitted in partial fulfillment of the

requirements for the award of the degree

of

DOCTOR OF PHILOSOPHY

by

NEHA MAHESHWARI

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY
INDORE
December, 2025

INDIAN INSTITUTE OF TECHNOLOGY INDORE

CANDIDATE'S DECLARATION

I hereby certify that the work that is being presented in the thesis entitled "**SRAM Based RO-PUF Architectures for Edge Devices**" in the partial fulfillment of the requirements for the award of the degree of **Doctor of Philosophy** and submitted in the **Department of Electrical Engineering**, Indian Institute of Technology Indore, is an authentic record of my own work carried out during the time period from August 2021 to December 2025 under the supervision of Prof. Santosh Kumar Vishvakarma, Professor, Indian Institute of Technology Indore, India.

The matter presented in this thesis has not been submitted for the award of any other degree of this or any other institute.

Signature of the student with date

(Neha Maheshwari
18/12/2025)

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Santosh 18/12/2025

Signature of Thesis Supervisor with date

(Prof. Santosh Kumar Vishvakarma)

Neha Maheshwari has successfully given Ph.D. oral examination held on 09/02/2026

Santosh 09/02/2026

Signature of Thesis Supervisor with date

(Prof. Santosh Kumar Vishvakarma)

ACKNOWLEDGEMENTS

My journey toward earning a doctorate has been deeply fulfilling and has enriched my understanding of various dimensions of life. I dedicated myself to my work with faith in the divine presence guiding every step of this journey. This achievement would not have been possible without the unwavering support and encouragement from my family, friends, and many others. I sincerely express my gratitude to all who contributed to making this academic pursuit both successful and memorable.

First and foremost, I express my deepest gratitude to my PhD supervisor, Prof. Santosh Kumar Vishvakarma, for his constant motivation, insightful guidance, and unwavering support throughout my doctoral journey. His belief in my abilities, encouragement to think independently, and commitment to excellence continuously inspired me to push boundaries and grow as a researcher. Despite his demanding schedule, he always found time for thoughtful discussions and valuable feedback. Beyond research, his mentorship helped shape my professional outlook as a teacher and academic. I remain profoundly thankful to him for his invaluable guidance and support.

It is a privilege to thank my PSPC committee members, Prof. Avinash Sonawane and Prof. Vimal Bhatia for providing constructive feedback and suggestions.

I sincerely acknowledge the NanoScale Devices, VLSI Circuits and Systems (NS-DCS) Group at IITI for providing a collaborative and intellectually stimulating research environment. I am particularly grateful to Dr. Ambika Prasad Shah and Dr. Sajid Khan for their valuable guidance, encouragement, and timely support during my research work. I also extend my thanks to Shivam Vaish for his sincere contributions as an MTP student to this research.

I gratefully acknowledge the financial and academic support provided by the Ministry of Education, Government of India, and the IITI DRISHTI CPS Foundation through the Chanakya PhD Fellowship. I also sincerely thank the Ministry of Electronics and Information Technology (MeitY), Government of India, for providing essential tools and infrastructure through the Special Manpower Development Program for Chips to System Design (SMDP-C2SD) and the Chips-to-Startup (C2S) program, which played a significant role in this work. I am thankful to Shri Vaishnav Vidya Peeth Vishwavidyalaya, Indore, for providing the opportunity to pursue my PhD under the AICTE Quality Improvement Programme (QIP).

I sincerely thank Brij B. Gupta for his generous financial support, which significantly contributed to the successful completion of my research work.

I sincerely thank my parents for their endless sacrifices, faith, and encouragement, which have been the foundation of my success. I am grateful to my brother, sister, and in-laws for their constant emotional support, and to my grandparents for their blessings. My heartfelt thanks to my husband for his patience, unwavering support, and encouragement throughout this journey.

I am forever grateful to my precious daughters, **Ira, Inaya, and Tulsi**, whose early sacrifices and unconditional love made this journey possible and gave deeper meaning to every achievement.

December, 2025 **NEHA MAHESHWARI**

— — — — — — — — — — — — — — — — — — — —

Dedicated to Ira, Inaya and Tulsi

ABSTRACT

In recent years, the rapid expansion of connected systems, edge computing platforms, and Internet of Things (IoT) devices has created a strong demand for lightweight and energy-efficient hardware security solutions. Traditional security techniques rely heavily on software-based cryptography and externally stored secret keys, which are increasingly vulnerable to physical attacks, cloning, and reverse engineering. Resource-constrained devices often cannot afford the computational and storage overhead associated with conventional cryptographic schemes. As a result, modern security architectures must rely on low-power, low-area, and tamper-resistant hardware primitives that can provide identity, authentication, and key generation at the silicon level.

With the increasing proliferation of connected devices and edge computing platforms, ensuring hardware-level security has become a critical requirement. Physical Unclonable Functions (PUFs) offer a lightweight and reliable approach for device authentication and secure key generation by exploiting inherent manufacturing variations in integrated circuits. This thesis presents the design and analysis of reconfigurable and memory-centric PUF architectures that integrate oscillator-based entropy generation with compute-in-memory principles to enhance security and reliability.

The thesis begins by introducing the fundamental concepts of hardware security and highlights the significance of PUFs as a reliable solution for device authentication and cryptographic key generation. The chapter discusses various PUF structures, classification methodologies, performance metrics, and common application scenarios. It also examines the role of memory systems in modern and edge computing platforms and introduces in-memory and near-memory computing paradigms as potential enablers of efficient hardware security. The chapter concludes by outlining the key contributions and objectives of this thesis.

The second part of this thesis, it presents the design and evaluation of a configurable Bidirectional Ring Oscillator (BRO) PUF. This chapter introduces the concept of directional control in oscillator-based PUFs to increase entropy and resistance against modeling attacks. The proposed architecture is verified using FPGA-based implementation, and its performance is evaluated in terms of frequency characteristics, stability, and suitability for PUF operations.

The third part of this work outlines a novel gated logic–based 10T SRAM cell tailored for configurable ring oscillator operation. This chapter explains the gated logic concept and details the architecture of the proposed GL-SRAM cell. The integration of SRAM cells into ring oscillator configurations is discussed, and the design is implemented at the ASIC level with simulation results validating its effectiveness.
The fourth part of the thesis extends the previous work by proposing a tristate logic–based SRAM array that functions both as a memory block and as a bidirectional ring oscillator network. This chapter focuses on design reconfigurability, directional control, and power optimization. ASIC-level implementation and performance evaluation demonstrate the feasibility and efficiency of embedding logic behavior within memory arrays.
The fifth part of the thesis presents the core contribution of the thesis: the Compute-In-Memory-enabled Multistage Bidirectional Ring Oscillator PUF (MBRO-PUF). The architecture utilizes TL-SRAM cells as building blocks, with transmission gates enabling stage programmability and tristate inverters controlling oscillation direction. Multiplexers allow selection among multiple oscillators, forming a multi-stage, multi-directional, multi-challenge PUF framework. Extensive performance analysis confirms increased CRP space and improved resistance to modeling and side-channel attacks.

In addition to oscillator-based designs, this work presents an SRAM-based PUF using a bitline discharge technique. A 10T SRAM cell with an Aging-Resilient Inverter (ARI) is introduced to improve long-term stability. Randomness is extracted by measuring variation in bitline discharge rates during read operations, leveraging process-induced mismatches for entropy generation. Finally, the thesis reports successful RTL-to-GDSII implementation and silicon tapeout of selected designs using industry-standard CAD tools and open-source digital workflows.

List of Publications

(A) Publications from PhD Thesis Work

A1. In Refereed Journals

1. **Neha Maheshwari**, Ambika Prasad Shah, Santosh Kumar Vishvakarma, "Gated logic controlled 10T-SRAM for low-power bidirectional ring oscillators," *Integration The VLSI Journal, Elsevier*, Vol 106, pp. 102588, ISSN 0167-9260, Oct, 2025, https://doi.org/10.1016/j.vlsi.2025.102588.**(SCI, IF 2.5)**.

2. **Neha Maheshwari**, Meena Panchore, and Santosh Kumar Vishvakarma, "BRO PUF: A Bi-directional Ring Oscillator-Based PUF for IoT Security." *IETE Journal of Research*, pp. 1-14, July 2025, https://doi.org/10.1080/03772063.2025.2540042. **(SCI, IF 1.3)**.

3. **Neha Maheshwari**, Brij B. Gupta and Santosh Kumar Vishvakarma, "CIM-Enabled MBRO-PUF: Integrating Multistage BRO and Reconfigurable SRAM for Edge Security Applications," *IEEE Internet of Things Journal*,vol. 13, no. 4, pp. 6284-6293, 15 Feb.15, 2026. https://doi.org/10.1109/JIOT.2025.3636998.**(SCI IF 8.9)**.

4. **Neha Maheshwari**, Shivam Vaish, Ambika Prasad Shah and Santosh Kumar Vishvakarma, "Tri-state Logic-based SRAM Array: Reconfigurable design as SRAM Array and Bidirectional Oscillator Circuits," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems: In-Memory Computing (IMC): From Technology to Applications.* **(SCI IF 3.8)(Under Revision-1)**

A2. In Refereed Conferences

1. **Neha Maheshwari**, Shivam Vaish, Kwok Tai Chui, Brij Bhooshan Gupta, and Santosh Kumar Vishvakarma, "A 10T SRAM-based PUF-enhanced In-Memory Computing for Secure Authentication," *21st IEEE Asia Pacific Conference on Circuits and Systems*, Busan, Korea, 12-15 Oct. 2025.

A5. Any other relevant information

1. Open Source Tapeout Arbiter PUF using Skywater 130 nm.

2. BRO PUF Tapeout using SCL 180nm.

Contents

List of Figures

List of Tables

List of Abbreviations/Acronyms

ADE Analog Design Environment

AI Artificial Intelligence

ALU Arithmetic Logic Unit

ARI Aging Resilient Inverter

ASIC Application Specific Integrated Circuit

BDGRO Bi-Directional Gated Ring Oscillator

BER Bit Error Rate

BL Bit Line

BLB Bit Line Bar

BRO Bidirectional Ring Oscillator

CIM Computing-in-Memory

CMOS Complementary Metal Oxide Semiconductor

CPU Central Processing Unit

CRO Configurable Ring Oscillator

CRP Challenge Response Pair

CTS Clock Tree Synthesis

DRC Design Rule Check

EEPROM Electricaly Erasable Read Only Memory

EN Enable

ESRO Embedded SRAM Ring Oscillator

FOM Figure of Merit

FPGA Field Programmable Gate Array

GL Gated Logic

HD Hamming Distance

HDL Hardware Description Language

HSNM Hold Static Noise Margin

IMC In-Memory Computing

IoT Internet of Things

LUT Look Up Table

LVS Layout Versus Schematic

MAC Muliply-and-Accumulate

MBRO Multistage Bidirectional Ring Oscillator

MOS Metal Oxide Semiconductor

MTP Multiple Time Programmable

MUX Multiplexer

NBTI Negative Bias Temperature Instability

NMOS N-Channel Metal Oxide Semiconductor

NVM Non volatile Memory

OTP One Time Programmable

PDAP Power Delay Area Product

PDP Power Delay Product

PEX Parasitic Extraction

PMOS P-Channel Metal Oxide Semiconductor

PUF Physical Unclonable Function

PVT Process, Voltage, and Temperature

R-InMAC Reconfigurable In-Memory Advance Computation

RO Ring Oscillator

ROM Read Only Memory

RRAM Resistive Random Access memory

RSNM Read Static Noise Margin

SDK Software Development Kit

SINM Static Current Noise Margin

SNM Static Noise Margin

SoC System-on-Chip

SRAM Static Random Access memory

STA Static Timing Analysis

SVNM Static Voltage Noise Margin

TG Transmission Gate

TL Tristate Logic

WL Word Line

WSNM Write Static Noise Margin

Chapter 1

Introduction

This chapter introduces the fundamental concepts of Physical Unclonable Functions and presents an overview of the research on state-of-the-art PUF architectures, including SRAM cells and their design methodologies. These foundational ideas form the basis for the rest of the thesis.

1.1 Overview of Hardware Security and Role of Physical Unclonable Function

Hardware is an essential component of all systems and has evolved into an integral element of our daily lives. It integrates with the software to increase the computational capability of any system. The hardware is utilized in a variety of applications, ranging from handheld devices like as mobile phones to crucial applications such as aircraft control [1]. The IoT refers to the establishment of a network of physical items. These things are interconnected, operated, and remotely controlled over the Internet, which is made possible by the emergence of incredibly small integrated systems that are autonomous in terms of functionality, energy, interaction, and network infrastructure. IoT is predicted to be employed in a range of developing applications, including smart cities, wearable electronics, and remote health care and many more [2]. A conceptual view of the IoT alongwith the key challenges with conventional cryptography approach has been shown in Figure 1.1. With the rapid growth of the IoT, billions of interconnected devices are being deployed in sensitive and mission-critical contexts; hardware security has become increasingly important [3].

More than 50 billion devices are expected to be connected to the internet by 2029, significantly increasing the size and complexity of the IoT [4].

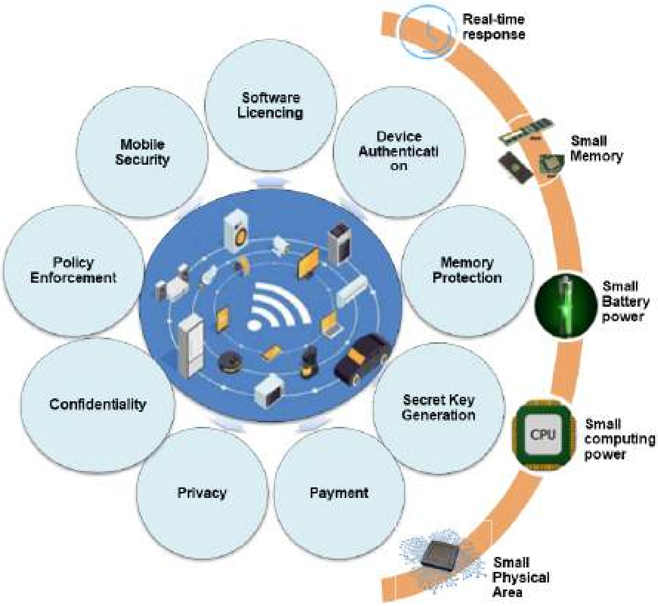


Figure 1.1: Key Challenges with Conventional Cryptography.

As billions of devices become networked, the globe faces a new set of security threats that did not exist previously. The roadmap of the IoT worldwide has been shown in Figure 1.2. As low-cost attacks on IoT devices increase, ensuring the se-

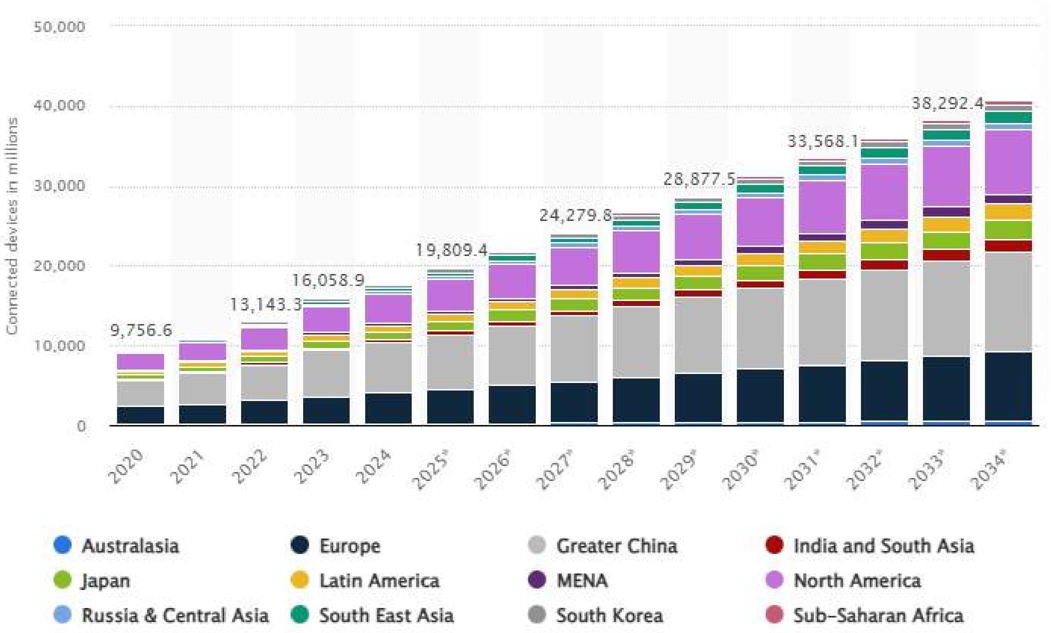


Figure 1.2: Road Map for Global Growth of Connected Devices by Region from 2020 to 2034 (in millions) [5].

curity of data processing, device authentication, and reliable communication has become critical. Modern systems often rely on cryptographic processes, but their security is ultimately dependent on the protection and secure production of private keys [6, 7]. Conventional key storage methods add rigidity, are susceptible to intrusive attacks, and frequently raise system costs [8, 9]. According to a Global Semiconductor Alliance (GSA) paper, one possible option is to integrate a dedicated security subsystem within the microcontroller or system-on-chip (SoC) at the heart of an IoT device[10].

Physical Unclonable Functions overcome these issues by creating device-specific, tamper-resistant cryptographic keys directly from intrinsic manufacturing variances, avoiding the need to store keys in non-volatile memory[11]. PUFs play an important role in improving hardware security across IoT endpoints, hubs, and gateways by allowing for secure key generation, authentication, and identity management. PUF generates a safe, unique key for cryptography and hardware authentication by mapping challenges to responses[12]. Silicon chip manufacturing changes impact the link between challenge and response. Variations between dies are random and unpredictable due to technical limitations in manufacturing units. These process variances, like human biometrics, are unique, non-volatile, and difficult to replicate[13].

PUF creates random and unclonable functions by utilizing physical variations. Variations are converted into responses (output) for varied tasks (input). It is practically hard to have two chips with identical responses for the same circuit. It has the following advantages:

- **Chip Identifier or Key Generator**: Variations during fabrication create an intrinsic chip identifier. Silicon fingerprints provide repeatable but unpredictable responses. The generated responses are easy to evaluate but hard to replicate.

- **Low Cost**: PUFs are cost-effective compared to other non-volatile memory types like flash memory, Read-Only Memory (ROM), One-Time Programmable (OTP), and Multiple Time Programmable (MTP), as they do not require special fabrication procedures or programming logic to implement.

- **Unclonability**: PUF cloning is challenging due to the complex physical system that generates the key or identification, regardless of the original mask.

- **Temper Resilience**: The produced key is only available while power-on and destroyed once power is turned off. This prevents attackers from accessing the key, even with physical access to the device.

PUF offers security, uniqueness, randomness, unclonability, and tamper resiliency at a low cost, making it an excellent choice for lightweight security applications such as IoT. This makes PUF an active research area in cryptography [15].

Comparing the Different Methodologies

Off-chip techniques, such as EEPROM or non-volatile memory, are commonly used to store keys. Advancements in hardware hacking, including side-channel attacks and machine learning, have made non-volatile memory keys vulnerable. Cryptographic algorithms' keys can easily reverse-engineered and replicated, making cyberattacks a devastating concern as IoT becomes more widely adopted [15, 16]. Table 1.1 gives a comparison between the three typical techniques to produce and store the cryptographic root key of a device and the PUF. Based on this evaluation, the PUF offers a superior balance between security, cost, and minimal complexity for creating root keys. In terms of low cost and ease of supply chain, the internal RNG is comparable to the PUF; however, any solution that keeps a key in NVM would have less strong security for stored root keys (as well as any other stored keys or sensitive data) [13]. Figure 1.3 shows the Security robustness versus affordability for the different key storage mechanisms.

Table 1.1: Physical unclonable function compared to other key generation and storage mechanisms.

No.	**Feature**	**PUF**	**Internal RNG + Key in NVM**	**Key Injection + Key in NVM**	**Secure Element**
1	High Security	✓	× – Key stored in clear		✓
2	Supply Chain Simplicity	✓	✓	× – Injection needed	× – Additional chip
3	Low Cost	✓	✓	× – Service fee	× – Additional chip

✓= Supported, ×= Not supported

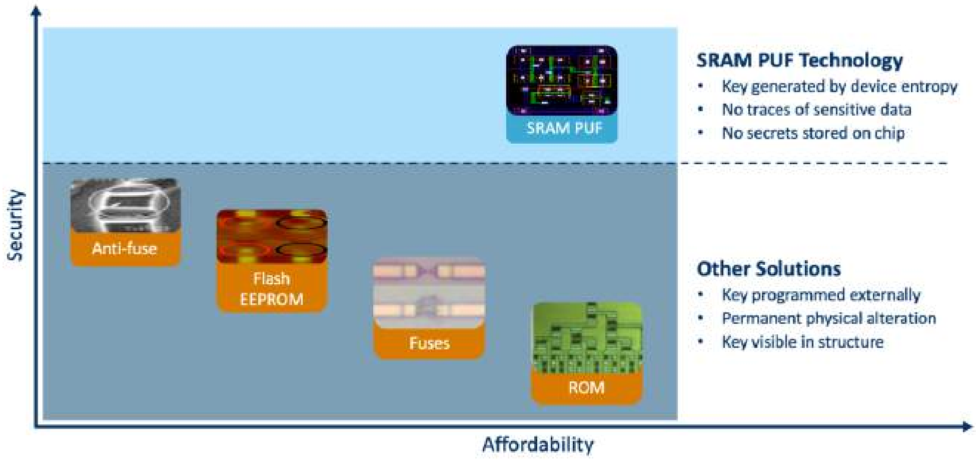

SRAM PUF Technology
Key generated by device entropy
No traces of sensitive data
No secrets stored on chip
SRAM PUF
Anti-fuse
Flash EEPROM
Fuses
ROM
Other Solutions
Key programmed externally
Permanent physical alteration
Key visible in structure
Security
Affordability

Figure 1.3: Security robustness versus affordability for the different key storage mechanisms [13].

1.2 Physical Unclonable Function (PUF)

PUF are a promising security solution for sensitive data. However, using random physical properties to identify objects, systems, and people is not a novel concept. Biometrics is a field that has been around since the 19th century [12]. An application of this concept was introduced as physical-one-way functions [11] and physical-random-functions [17]. Using the PUF as a fingerprint is based on the unpredictability and uncontrollability of semiconductor manufacturing process variability, which are usually undesirable. These random process variations result in random changes in the MOS parameters, like the threshold voltage (V_{TH}) and channel length (L_{eff}).

1.2.1 PUF Definition

PUF is a physical system-based function that maps challenges to responses in a random, easily evaluated approach. A PUF function, unlike a mathematical function, is non-deterministic and varies from instance to instance. For a given challenge C, the responses R_a, R_b produced from two PUF instances, PUF_a and PUF_b, are R_a $= R_a$ [18], Four identical PUF-generated responses have the same functionality and design and are implemented over the same wafer but have their on unique response, as seen in Figure 1.4.

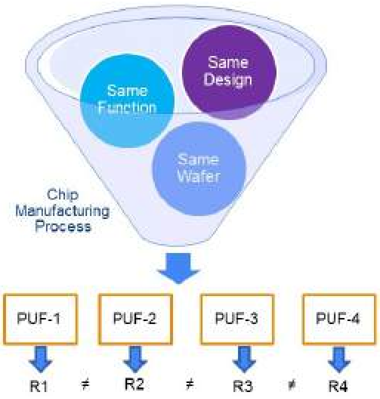


Figure 1.4: Principle of PUF operation showing response uniqueness arising from manufacturing variability in identical chip designs.

1.2.2 PUF Properties

With a broad collection of known PUFs, the following qualities can assist designers in identifying potential applications [16]. This section explores the following PUF characteristics.

- **Physically Unclonable**: A PUF is difficult, if not impossible, to replicate with the same response, even by the manufacturer.
- **Easy to Evaluate**: A PUF is considered easy to evaluate if it is simple to obtain a response to a challenge.
- **Repeatable or Reproducible**: If evaluating a fixed challenge several times yields the same response without error, the PUF is considered repeatable or reproducible.
- **Unpredictable**: PUF challenges have unique responses, meaning no two responses are identical.
- **Uniqueness**: Each PUF challenge has a unique response, which means no two PUF responses are identical.
- **One-way**:It is difficult to identify an appropriate challenge regarding each PUF response.
- **Tamper Resilient**: A minor change in the system implementing a PUF results in a unique challenge-response set.

1.2.3 PUF Quality Metrics

The purpose of a PUF is to provide a reliable, random, and unique response to a challenge. The PUF response should be consistent across different operating environments. This section provides the design criteria for PUFs.

Randomness

The randomness of a PUF is typically characterized using three key metrics: uniqueness, bit-aliasing, and uniformity.

- **Uniqueness** The inter-die Hamming distance (HD) is used to calculate the uniqueness, which differentiates the responses from two PUF instances. The ideal value is 50%, which indicates that half of the PUF response should differ when the same challenge is applied to any two identical PUF instances. Let us assume that, in response to a challenge C, R_a and R_b are two n-bit responses from selected at-random chips a and b from a set of m available chips. The uniqueness (U) from m chips can be written as follows:

$$U = \frac{2}{m(m-1)} \sum_{a=1}^{m-1} \sum_{b=a+1}^{m} \frac{HD(R_a, R_b)}{n} * 100\% \tag{1.1}$$

- **Bit-Aliasing** Systematic variations can cause multiple chips to generate very similar responses to the same challenge, leading to bit-aliasing, which is evaluated using the Hamming Weight (HW). For a given challenge C, the bit-aliasing of the i^{th} bit across n different PUF chips is defined as:

$$\text{Bit-aliasing} = \frac{1}{k} \sum_{j=1}^{k} R_{i,j} \times 100\% \tag{1.2}$$

  where k is the number of chips and $R_{i,j}$ is the value of the i^{th} bit in the j^{th} chip response. Bit-aliasing has an ideal value of 50%.

- **Uniformity** A PUF response's uniformity is determined by the percentage of "0s" and "1s"; it is defined as

$$\text{Uniformity} = \frac{1}{n} \sum_{j=1}^{n} R_{i,j} \times 100\% \tag{1.3}$$

where n is the number of chips and $R_{i,j}$ is the value of the i^{th} bit in the j^{th} chip response. Uniformity has an ideal value of 50%.

Reliability

Reliability is a measure of how stable PUFs are under different environmental conditions. Ideally, the PUF response under different environmental conditions should be stable. However, temperature variation and supply voltage changes are the two most important elements influencing circuit performance in practice.

- **Reliability** The reliability of a PUF is evaluated by comparing two responses generated by the same chip for the same challenge but under different temperature and/or supply voltage conditions. The reliability R of a chip can be expressed as:

$$R = 1 - \frac{1}{k}\sum_{m=1}^{k}\frac{\mathrm{HD}(R_a, R_a')}{n} \times 100\% \tag{1.4}$$

  where k is the number of samples, n is the number of generated bits, R_a and R_a' are the responses obtained at nominal and varying operating conditions, respectively. $\mathrm{HD}(R_a, R_a')$ denotes the Hamming distance between R_a and R_a'. Ideally, the reliability value should be 100%.

- **Bit Error Rate** Bit Error Rate (BER) is defined as the number of PUF response bits that are changed in a single chip.

$$BER = \frac{1}{m}\sum_{j=1}^{m}\frac{HD(R_i, R_j)}{n} \times 100\% \tag{1.5}$$

$$BER = 1 - R \tag{1.6}$$

  Where R denotes the reliability, R_i represents the n-bit PUF response from the i^{th} chip, and R_j is the repeated measurement of the same response. Here, M denotes the number of repetitions. Ideally, the Bit-Error Rate (BER) should be 0.

Table 1.2 presents the typical and ideal values of various PUF quality metrics. The deviation of practical values from their ideal targets arises from several factors, including process variations, environmental fluctuations, noise, and limitations in circuit design and measurement conditions.

Table 1.2: PUF metrics and typical values.

Quality Metric	Measured By	Typical Value	Ideal Value
Uniqueness	Inter-PUF HD	40–60%	50%
Bit-Aliasing	Percentage HW	30–60%	50%
Bit Error Rate	Intra-PUF HD	0.5–10%	0
Unstable Bit Count	Unstable Bits	1–20%	0
Randomness	1/0 Count	40–60%	50%

1.2.4 Classification of PUF

Currently, a wide variety of PUF architectures are available. PUFs can be classified into (i) silicon and non-silicon PUFs, (ii) intrinsic and extrinsic PUFs, (iii) delay-based and memory-based PUFs, and (iv) strong and weak PUFs. This section presents an overview of different PUF types, their sources of randomness, and key PUF properties. Classification of PUF is as shown in Figure 1.5.

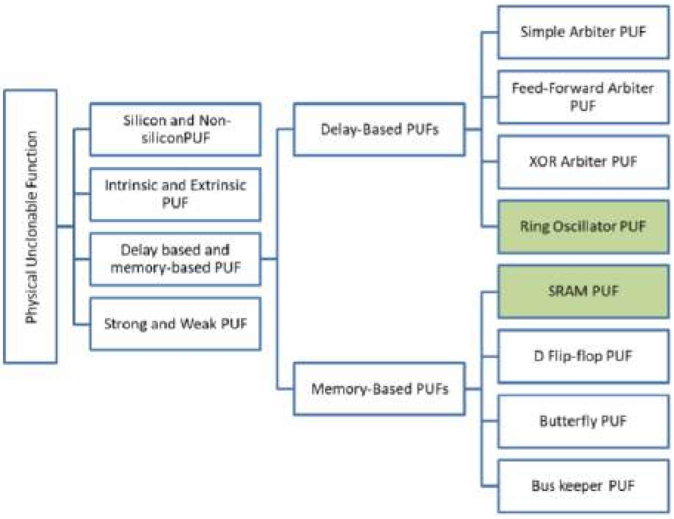


Figure 1.5: Classification of PUF.

Silicon and Non-Silicon PUF

The structural disorder of a non-silicon material is used to create a Non-silicon PUF. These PUFs derive their key from differences in the physical device rather than integrated circuits. For example, the one-way physical function builds challenge-response pairs using the random scattering pattern of an optical medium caused by incident laser light [11]. There are several other PUFs such as paper PUF [19], CD PUF [20], and RF PUF [21]. In contrast, silicon PUFs use manufacturing differences in logic components and interconnects induced by process variations within a chip to generate CRPs. Because silicon PUFs do not require any particular fabrication procedures, they can be easily used as a hardware building block in cryptographic solutions. As a result, this thesis focuses solely on silicon PUFs.

Strong and Weak PUF

PUFs with a large number of CRPs can be considered as strong PUF [22]. PUFs with a small number of challenge-response pairs are considered weak [23].

Intrinsic and Extrinsic PUF

An intrinsic PUF does not require an additional circuit to extract the mismatch due to process variations. Intrinsic PUF, such as SRAM PUFs [22, 24] and D Flip-flop PUF [25], only makes use of hardware elements those are already present in the device. In contrast, an extrinsic PUF extracted the uniqueness using dedicated additional circuitry. The use of additional circuitry leads to hardware overhead. Extrinsic PUFs include Arbiter, Ring Oscillator [17], Butterfly [26], SR-NOR latch [27], and Buskeeper PUF [28].

Delay Based PUF

The delay-based PUFs are built from basic digital circuit design, which extracts the intrinsic variations in logic gates and interconnects delay to provide device-specific problems. The arbiter PUF and ring oscillator PUF [17, 29] are the examples of delay-based PUFs.

- **Arbiter-PUF** Figure 1.6 illustrates the Arbiter-PUF, which consists of n stages of two 2-to-1 multiplexers. A rising pulse is applied at the input and propagated through two nominally identical delay paths that are controlled by switching elements. The delay configuration is determined by the challenge

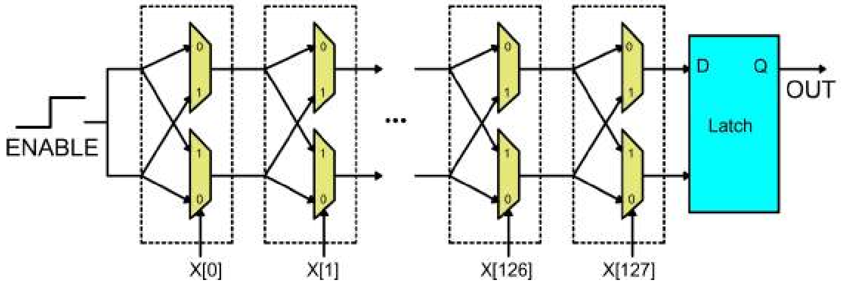


Figure 1.6: Arbiter PUF [29].

bits C=c0, c1, c2, ..., cn. When $c_n = 0$, the signals pass straight through the paths, whereas when $c_n = 1$, the paths are crossed [29].

At the end of the delay path, an arbiter decides which one is faster. Manufacturing process variables cause one delay path to reach the flip-flop before the other. A D flip-flop with one delay signal connected to the clock pin and another to the data pin is typically used as an arbiter. Ideally, the response of an Arbiter PUF is equally likely to be '0' or '1', depending on the randomness of process variables. However, the response may be biased towards one of the two states, reducing the uniqueness of the PUF. To avoid bias in PUF response, the layout should be as symmetrical as possible.

- **Ring Oscillator(RO)-PUF** An RO is made up of an odd number of inverters, with the last inverter connected to the first inverter to form a chain. The oscillation frequency of each RO is device-dependent and varies due to random

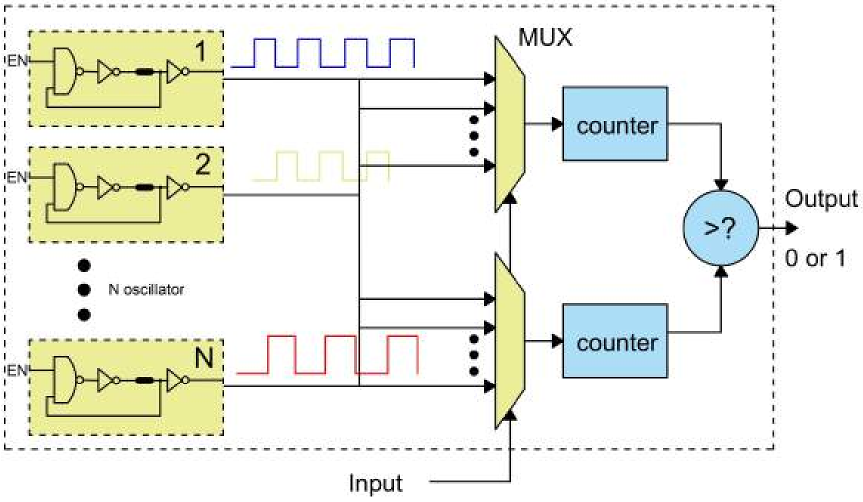
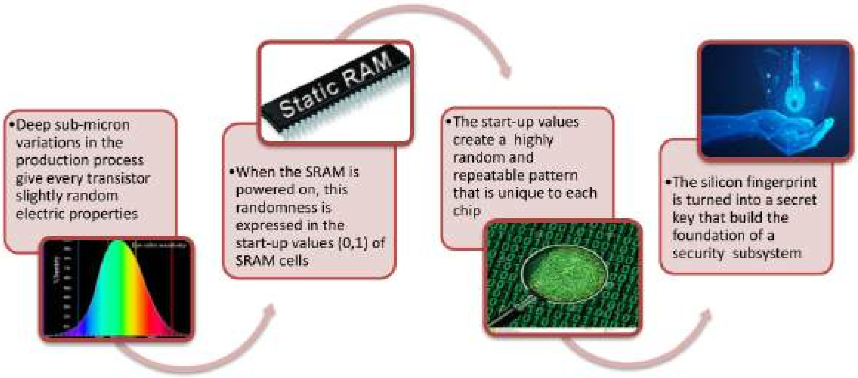


Figure 1.7: Ring Oscillator-based PUF [29].

process variation. An RO PUF consists of two identical ROs whose frequencies are measured by a pair of counters. Figure 1.7 shows how the output of these two counters is compared to obtain a 1-bit response. It provides fabrication simplicity over other PUF architectures because the RO hard macro can be instantiated several times [15, 29, 30]. This ensures that all ROs are equivalent in terms of routing and placement. Allowing ROs to oscillate for longer periods can increase the delay difference caused by process changes.

Memory-Based PUF

On the other hand, the memory-based PUFs are the designs that extract the inherent variations in bistable memory components. SRAM PUFs [22, 29], D flip-flop PUF [25], and butterfly memory-based examples are the PUF [26], SR-NOR latch PUF [27], and buskeeper PUF [28]. Figure 1.8 shows the functionality of memory based PUF.



- Deep sub-micron variations in the production process give every transistor slightly random electric properties

- When the SRAM is powered on, this randomness is expressed in the start-up values (0,1) of SRAM cells

- The start-up values create a highly random and repeatable pattern that is unique to each chip

- The silicon fingerprint is turned into a secret key that build the foundation of a security subsystem

Figure 1.8: Functional overview of SRAM PUF [31].

- **SRAM PUF** An SRAM cell is a sort of volatile memory that stores 1-bit data using two cross-coupled inverters and reads and writes the data with two access transistors.

  Figure 1.9 shows the schematic diagram of a 6T SRAM cell. Cross-coupled inverters have a positive feedback loop that strengthens their current state. An SRAM cell is bi-stable, with two stable and one unstable (metastable) state .Figure 1.10 shows that the power-on value of an SRAM cell first enters a metastable condition before settling into one of the stable states. The two inverters in the cell have a perfectly matching layout[31].

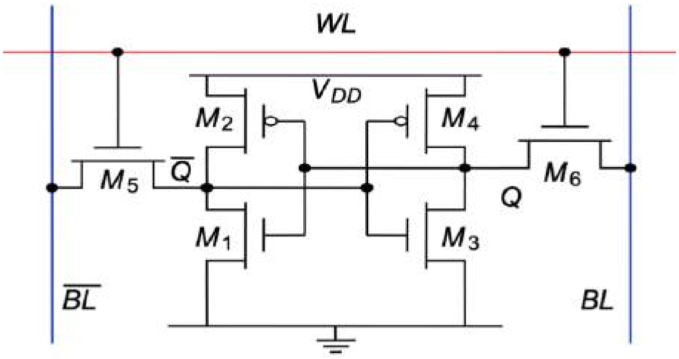


Figure 1.9: 6T SRAM cell.

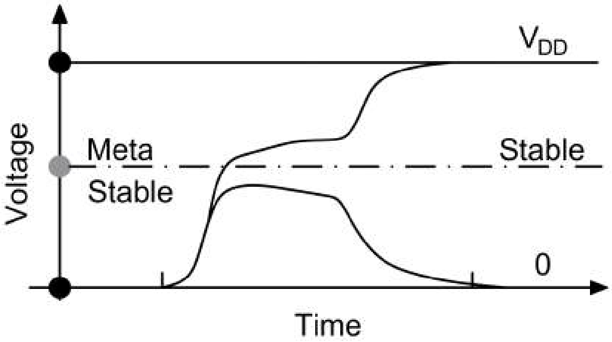


Figure 1.10: Metastable state [31].

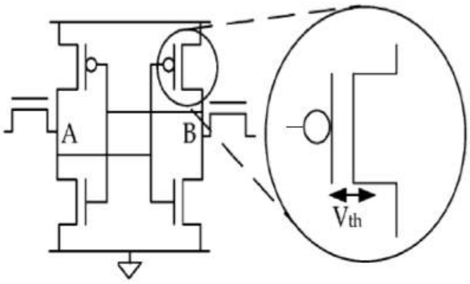


Figure 1.11: SRAM working as PUF [31].

However, the process variations make one of them slower. The settling state is decided by the mismatch between inverters [22]. As a result, the power-on value of an SRAM cell is random and dependent on the mismatch caused by process variation, which functions as a PUF and as shown in Figure 1.11. An SRAM memory array is composed of a large number of identical SRAM cells, where each cell is typically implemented using two cross-coupled inverters formed by complementary pMOS and nMOS transistors. When power is applied to an SRAM cell, its initial logical state is not explicitly defined but is instead determined by inherent process-induced device mismatches, particularly the threshold voltages of the transistors forming the inverters. During power-up, as the supply voltage (VDD) rises from zero, the transistor that begins conducting first establishes the initial state of the cell, forcing it into either a logical '0' or '1'. In practice, the power-up behavior is dominated by the mismatch in the threshold voltages of the two pMOS transistors (P1 and P2) in the cross-coupled inverters. For instance, if random manufacturing variations cause Vth, P1 to be slightly lower than Vth, P2, transistor P1 will turn on earlier during power ramp-up, driving node A high and suppressing the conduction of P2. Consequently, the cell settles into a preferred power-up state of A = 1. The greater the threshold voltage mismatch between P1 and P2, the stronger the cell's preference for a particular output state, resulting in improved stability and repeatability across multiple power cycles. Conversely, when Vth,P1 is equivalent to Vth, P2, the cell exhibits weak state bias, making it more susceptible to noise, voltage fluctuations, and environmental variations, thereby increasing the probability of bit flips. Such unstable cells introduce randomness and unreliability in SRAM-based physically unclonable function (PUF) responses and must be accounted for through reliability enhancement techniques. SRAMs are used as memory in many circuits, therefore as they are an essential component of the design, SRAM PUF is an intrinsic PUF. However, modern FPGAs initialize the SRAM to a known state, limiting the utility of SRAM PUF in FPGAs.

- **Latch PUF** An SR latch-based PUF is described in [27], in which two NOR gates form a cross-coupled SR latch, as shown in Figure 1.12 The settling state of the latch is used for IC identification, which is based on the mismatch in NOR gates caused by random process fluctuations.

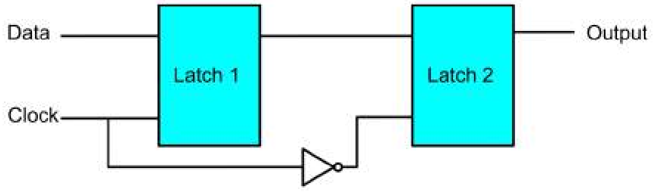


Figure 1.12: Latch-based PUF.

The latch is forced into an unstable state by applying logic '1' at the input, and when the input is removed, the latch returns to a stable state based on the internal mismatch.

- **D Flip-flop PUF** The majority of digital systems use state machines to control transitions. A D flip-flop is a major component of finite-state machines, and like SRAM, D flip-flops are integrated into the design, making them intrinsic PUFs. A D flip-flop consists of latches and is used to store a binary state as shown in Figure 1.13. The power-on state of a D flip-flop can be used as a PUF, similarly to the SRAM PUF [32].

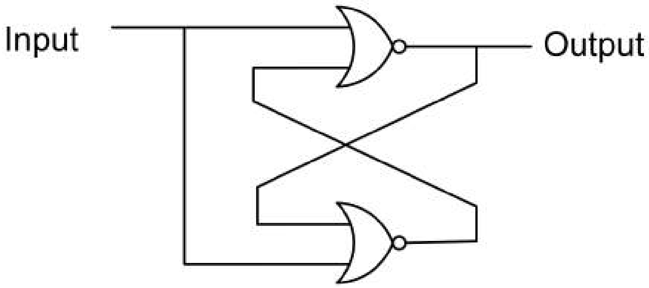


Figure 1.13: D Flip-flop PUF.

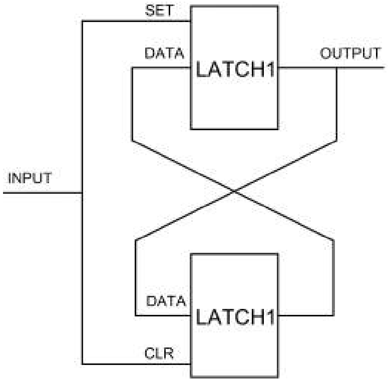


Figure 1.14: Butterfly PUF.

- **Butterfly PUF** SRAM PUF cannot be used on FPGAs as SRAM is automatically initialized to a known state upon power-on [26] a butterfly PUF is proposed to integrate the benefits of SRAM-based PUFs onto FPGA platforms. Figure 1.14 depicts the butterfly PUF, which consists of two cross-coupled latches. One latch is preset to clear the other latch.

- **Buskeeper PUF** A buskeeper is used to keep a bus from floating; it stores the last value driven on the bus. A buskeeper is a latch with cross-coupled inverters, as seen in Figure 1.15. A buskeepers power-on value varies based on random mismatches, resulting in a PUF.

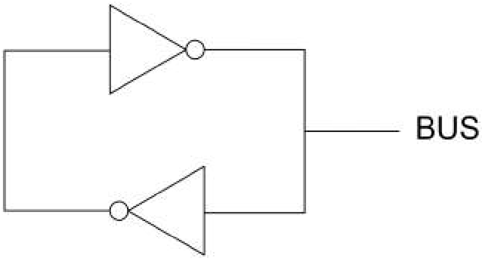


Figure 1.15: Buskeeper PUF.

1.2.5 PUF Application

Figure 1.16 shows the key security challenges with IoT devices that show the PUF requirement in edge devices. How a low-cost IoT device transmits sensor data to a cloud service, emphasizing the security challenges to be addressed. Although the first PUF was designed to obtain an identifier[11], a PUF can be used for a wide range of applications. Some of the applications are

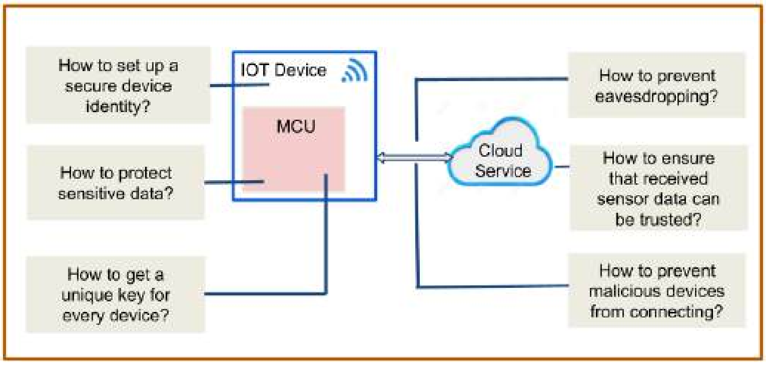
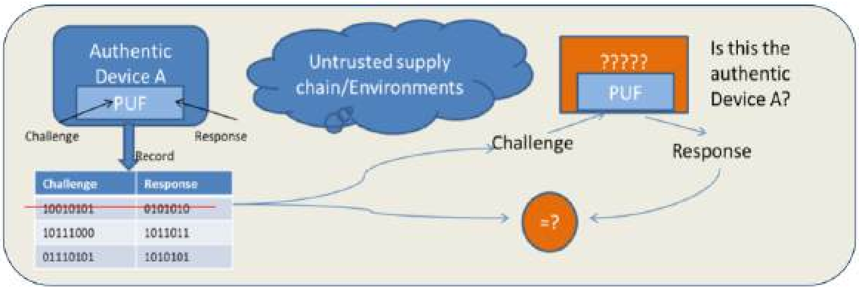

How to set up a secure device identity?
How to protect sensitive data?
How to get a unique key for every device?
IOT Device
MCU
Cloud Service
How to prevent eavesdropping?
How to ensure that received sensor data can be trusted?
How to prevent malicious devices from connecting?

Figure 1.16: Security challenges for an IoT device [1].

Device Authentication using PUF

A PUF can be used to establish a lightweight device authentication mechanism in resource-constrained applications, such as RFID, where cryptography implementation is too costly. A PUF responses to challenges in a unique and device-specific approach. In a secure environment, a challenge-response database can be built and saved for future authentication operations. Once the device is deployed in the field, the same challenge is issued to it, and the resulting response is compared to the database. To prevent man-in-the-middle attacks, challenges are never reused, as illustrated in Figure 1.17



Challenge	Response
~~10010101~~	~~0101010~~
10111000	1011011
01110101	1010101

Figure 1.17: Device Authentication using PUF.

Cryptographic Key Generation

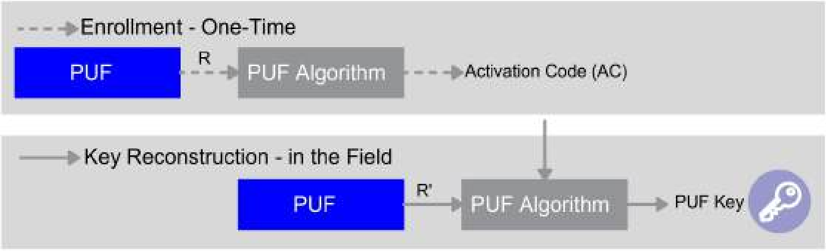


Figure 1.18: Cryptographic key generation with PUFs [1].

Many security applications require a key to encrypt sensitive data before sending it across an unsafe channel. Traditionally, these keys have been kept in non-volatile memory. The development of various hardware hacking methods, including as side-channel attacks and the use of machine learning algorithms, exposed the key stored in non-volatile memory to an attacker. A PUF could be an excellent choice for producing keys on demand instead of storing them in non-volatile memory. Unfortunately, due to noise, the output from the PUF circuits is not suitable for use as cryptographic keys.

IP Protection

Reverse engineering allows for cloning or modifying designs and selling them at a lesser price, as designing a chip needs significant research and development effort.

Reconfigurable designs developed in FPGA are particularly vulnerable to reverse engineering. FPGAs are configured using bit-files, which are typically stored in non-volatile memory. A bit-file can be quickly copied from non-volatile memory and used to build product copies [33]. A PUF can be used to extract the device-specific key, which can then be used to encrypt the bit-file, preventing such assaults and reverse engineering. The bit-file encryption makes it unique to FPGAs and cannot be used in other FPGAs [33].

1.3 Role of Memory in Modern and Edge Computing

Memory plays a critical role in modern and edge computing systems by enabling fast data access, low latency, and efficient processing of real-time applications. In edge devices, memory constraints directly impact performance, power consumption, and system responsiveness. Advanced memory technologies such as DRAM, Flash, and emerging non-volatile memories improve data handling capability in edge-based AI and IoT systems. In this work, we specifically focus on SRAM due to its high speed, low latency, and widespread use in cache and edge computing applications.

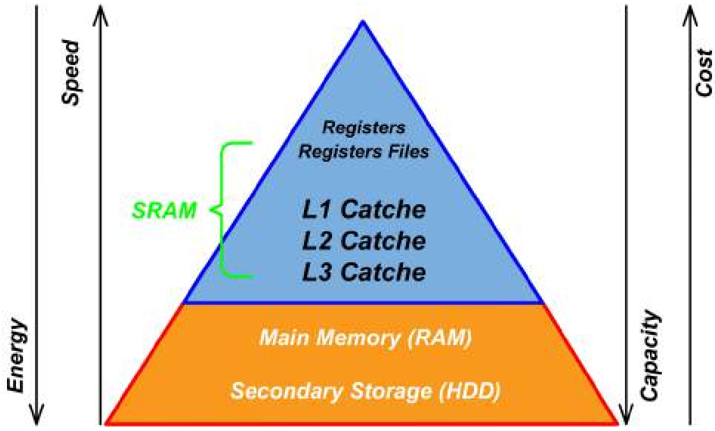


Figure 1.19: A typical memory hierarchy [34].

Figure 1.19 depicts the typical memory hierarchy, with increasing speed and decreasing energy of access as we move up the pyramid.As we travel down the hierarchy, however, production costs reduce and the density of stored bits increases. Consequently, frequently accessed data are stored in faster, more energy-efficient embedded memory (caches) near the processing engines[35, 36]. Data that is not easily accessible is stored in larger, slower memory such as DRAM and Flash. In this thesis, we primarily concentrate on embedded memories in the upper part of the hierarchy, specifically SRAM, which are typically used for on-chip caches in modern microprocessors

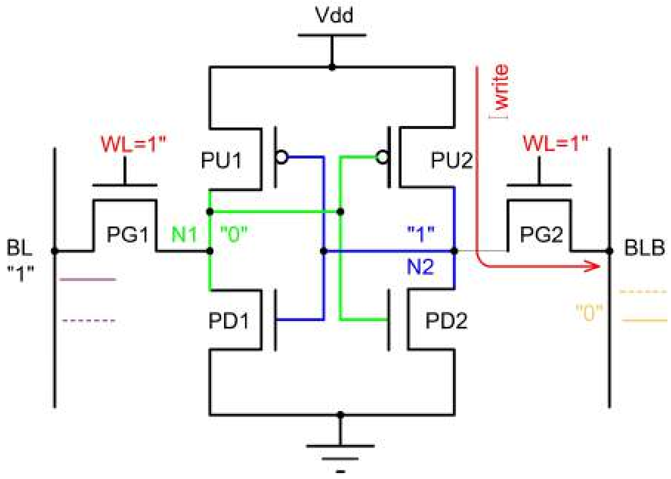


Figure 1.20: Write operations of 6T SRAM cell [34].

The 6T bit-cell during a write operation is seen in Figure 1.20. The bit lines are first driven to the data value that has to be written. The access transistors are thus activated when the WL is asserted. When writing data that differs from the previously recorded state , the potential of the high internal node decreases based on the drive strengths of the pull-up PMOS and access NMOS transistors. An essential factor in 6T SRAM design is the γ-ratio, which is the ratio of the driving strengths of the pull-up and access transistors. The transistors must be properly sized so that the γ-ratio is high enough to drop the high internal node's potential below the associated inverter's trip point. A low γ-ratio may lead to write failures.

The read operation starts with pre-charging the bit-line pairs (BL and BLB) to a supply voltage V_{DD}. The bit-lines are then kept floating, and the word-line WL is asserted. Depending on the data stored, one of the bit-lines (BL or BLB) starts discharging through the access and pull-down NMOS transistors, connected in series (Figure 1.21), depending on the data stored. A sense amplifier detects the bit-line differential voltage and outputs the data. On the side of the bit-cell that is storing a zero, the discharging current moves from the bit-line to the cell ground during the read operation. The potential of an internal node Q and the quantity of disturbance

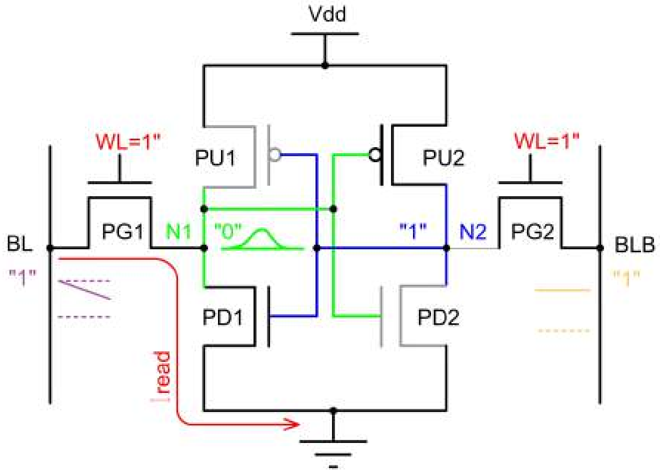


Figure 1.21: Read operations of 6T SRAM cell [34].

is determined by the driving strengths of access and pull-down NMOS transistors. The stored data is reversed if this elevated voltage exceeds the linked inverter's trip point. This phenomenon is referred to as "read disturb." To avoid this, the pull-down NMOS must be more powerful than the access NMOS. The β -ratio, a crucial SRAM design parameter, is the ratio of their driving strengths. Achieving the necessary β-ratio, which guarantees effective read operations (i.e., without any "read disturbs"), requires careful sizing of the NMOS transistors.

1.3.1 In/Near-Memory Computing Architectures

Although V_{DD} scaling can save energy in memory, current computer systems are limited by the von Neumann bottleneck, as previously discussed. Even with several cores, the system's throughput and energy are restricted by memory size and I/O bandwidth. The energy required for data transfer is more than a hundred times greater than that of an arithmetic operation. The idea of "in/near-memory" processing is one of the possible ways to get over this restriction, as shown in Figure 1.22 [37].

Assume that the necessary computation can be completed either inside the memory array or on its periphery, which is quite near to the array. In that scenario, the amount of data that needs to be carried over vast distances on the chip is greatly reduced. It is also possible to access several memory addresses that are involved in the computation at the same time. As a result, system throughput is increased be-

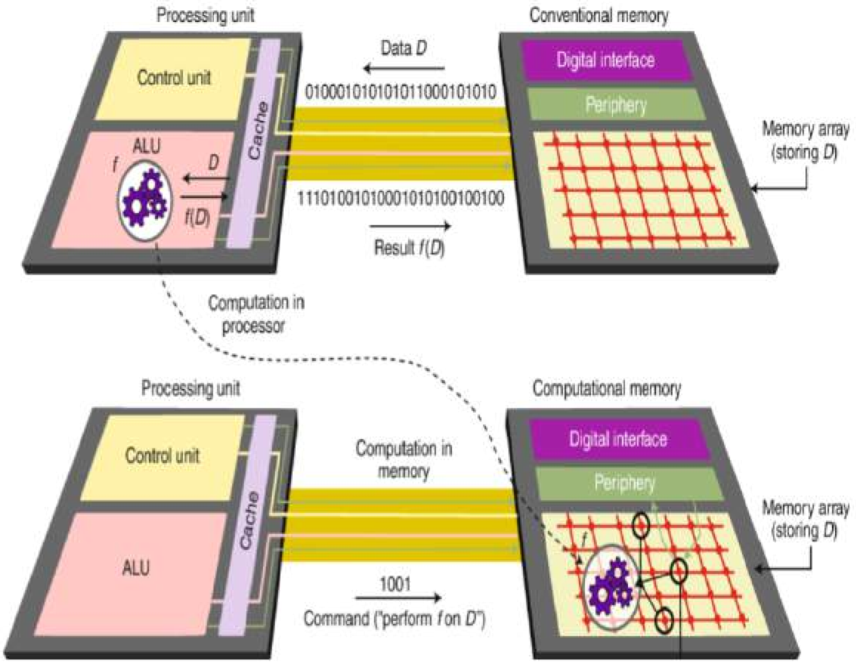


Figure 1.22: In-memory computing [37].

cause the effective amount of bits accessible from the memory is not constrained by its input/output. The memory and arithmetic processing components of Von Neumann's architecture are essential to computers. But data-driven applications like artificial intelligence and machine learning have revealed this architecture's shortcomings because of the Von Neumann bottleneck. Large data transfers between memory and the processor unit are the cause of this bottleneck. Researchers have used in-memory computing (IMC) to solve this. When compared to traditional computing, IMC dramatically lowers latency, improving performance for data-intensive applications.

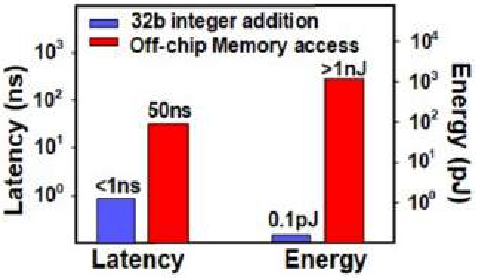


Figure 1.23: Latency and energy comparison for conventional computing v/s in-memory computing [38].

Figure 1.23 [38] shows the latency and energy comparison for data access and computation of 32-bit integer addition operation. A few recent studies have exam-

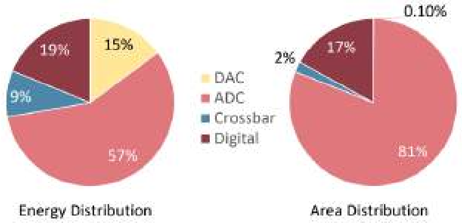


Figure 1.24: The energy and area overhead issue of ADC in analog IMC [39].

ined in/near-memory computing architectures since IMC shows promise as a solution for data-intensive applications. They can be broadly classified into two groups based on whether the information kept in memory is read explicitly and sequentially (referred to as "near-memory") or if it is implicitly, or "in-memory." Depending on whether the computation is carried out digitally (bit-precise) or in the analog domain, each can be further separated into two types. IMC is more energy-efficient for analog. It is more susceptible to PVT fluctuation, though. Additionally, an analog-to-digital converter, which uses more power and space than a memory crossbar, is needed for analog IMC. The energy and area distribution of various analog IMC blocks is displayed in Figure 1.24 [39]. Digital IMC, which also enables high throughput and can be readily scaled for greater memory sizes, is favored due to these limitations of analog IMC.

1.4 Thesis Contributions

Chapter 1 provides a comprehensive introduction to PUFs, highlighting their significance in hardware security. The chapter is also brief about the various designs of PUF, Both memory-based and delay-based PUFs are presented, along with a discussion of efficient architectural design strategies used in current research.

Chapter 2 introduces a Configurable Ring Oscillator (CRO) PUF architecture that offers advantages through an extensive Challenge-Response Pair (CRP) space and significant flexibility in selecting the RO direction within a single instance. The proposed design is implemented using standard 40 nm CMOS technology and operates at a supply voltage of 1.1 V. Functional verification is achieved by replicating the circuit on a Basys3 FPGA board. Furthermore, a comparative study of 3-stage, 5-stage, and 7-stage BRO PUF configurations demonstrates that performance gains saturate beyond a certain number of stages. Key metrics such as power dissipation, delay, and oscillation frequency across different BRO stage counts are characterized through detailed SPICE simulations.

Chapter 3 presents a novel gated logic-based 10T SRAM architecture designed for configurable ring oscillators. This chapter proposes a 10T SRAM cell, enhanced with gated logic, as an improvement over standard SRAM cells for implementing bi-directional ring oscillators (BROs). The gated logic approach offers notable advantages in reducing power consumption and minimizing area utilization. Performance comparisons of the GL-SRAM-RO with existing designs demonstrate its efficiency in terms of low power and compact area. The bi-directional operation and overall functionality are validated through post-layout simulation results, highlighting its suitability for security-critical applications.

Chapter 4 presents a proposed configurable SRAM-based RO PUF architecture featuring a reconfigurable 10T SRAM cell utilizing a tristate inverter. The design provides flexibility in reconfiguration to accommodate specific operational requirements. Compared to the conventional 6T SRAM cell, this approach enhances power efficiency, delay, and stability. Performance comparisons of the TL-SRAM-RO with prior art demonstrate low power consumption and area utilization, while its bi-directional operation is validated through post-layout simulation results, confirming its suitability for security-critical applications.

Chapter 5 presents a CIM-enabled MBRO-PUF architecture that integrates multistage ring oscillators and SRAM. This chapter focuses on the security features that demonstrate the effectiveness of the proposed design in achieving secure, low-power, and aging-resilient PUFs, implemented using a tristate inverter-based SRAM cell array. By combining ring oscillators, memory elements, and security primitives within the CIM framework, the design enables the generation of higher-quality PUF responses, resulting in a performance profile that is more unique, reliable, and robust. Functional verification is carried out through implementation on a Basys3 FPGA board.

Chapter 6 explores an SRAM-based PUF architecture enhanced by in-memory computing. This chapter proposes a 10T SRAM cell design that replaces the conventional inverter with an Aging Resilient Inverter (ARI) to improve reliability and security. The bitline discharge technique is employed with the proposed 10T bitcell to measure variations in the bitline discharge rate. To ensure proper operation and optimize performance of both the memory array and PUF implementation, extensive efforts were dedicated to designing, integrating, and simulating essential peripheral circuits, including the write driver, precharge circuit, and sense amplifier.

Chapter 7 concludes the thesis by summarizing its key contributions and reflecting on the insights gained from the proposed methodologies. The chapter also highlights potential directions for future research.

Chapter 2

Configurable Bidirectional RO based PUF Architecture

Protecting and securing a system for IoT applications involves hardware-based security primitives. For the purpose of cryptographic key generation and authentication, PUFs have emerged as the most widely used low-cost security primitives. This chapter introduces the bi-directional ring oscillator (BRO), featuring a configurable structure based on gated logic. Simulation results of the proposed BRO PUF, when compared to prior PUF designs, show better uniqueness. Notably, the proposed PUF design generates twice as many CRP in comparison with the conventional RO PUF. The proposed BRO PUF design is implemented on 40nm CMOS technology at a 1.1V supply. To validate the functionality, the proposed design is implemented on a Basys-3 FPGA board to calculate various PUF parameters.

2.1 Introduction

As discussed in the previous chapter, with the rapid expansion of the IoT, interconnected devices have become prevalent. Smart-connected devices have been deployed, and massive dataset obtained by these devices requires the integration of intelligent and dedicated machine-to-machine (M2M) interaction. Conventional cryptography, presumed to be secure on well-protected devices, is a traditional means by which the internet is safeguarded. Unfortunately, most IoT devices lack physical security, allowing hostile attackers to seize them quickly. Pappu, et al is credited with the initial conception of PUF [11]. The basic functionality of PUF is shown in Figure 2.1.

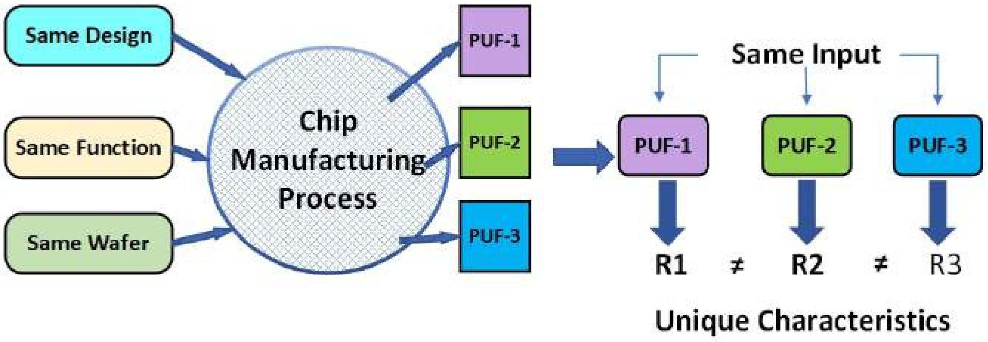


Figure 2.1: Functionality of PUF.

The challenges and issues found with various PUF topologies are crucial considerations when aiming to construct strong PUFs regarding CRP generation and the security of devices against attacks. BRO PUF provides an advantage in terms of large CRP generation. Based on current understanding, a configurable ring oscillator PUF employing a BRO-based approach is noticeably absent from the existing literature, capable of generating double CRPs. Such an approach offers significant flexibility in selecting the direction of the RO within a single instance. From a security perspective, this approach significantly complicates an attacker's ability to predict the response.

2.2 Bidirectional Ring Oscillator(BRO) PUF Framework

2.2.1 Design of BRO PUF

Figure 2.2 depicts the overall design of the proposed BRO PUF. The proposed PUF replaces n-RO with n-BRO in conventional design. In the proposed architecture, a total of 256 BRO instances are implemented, of which two are selected at a time based on the applied challenge through a multiplexer network. Two multiplexers of size 128×1 are employed for instance selection, where BRO_1 to BRO_{128} are connected to MUX-1 and BRO_{129} to BRO_{256} are connected to MUX-2. Each multiplexer produces a single output, and the selected BRO pair is propagated to

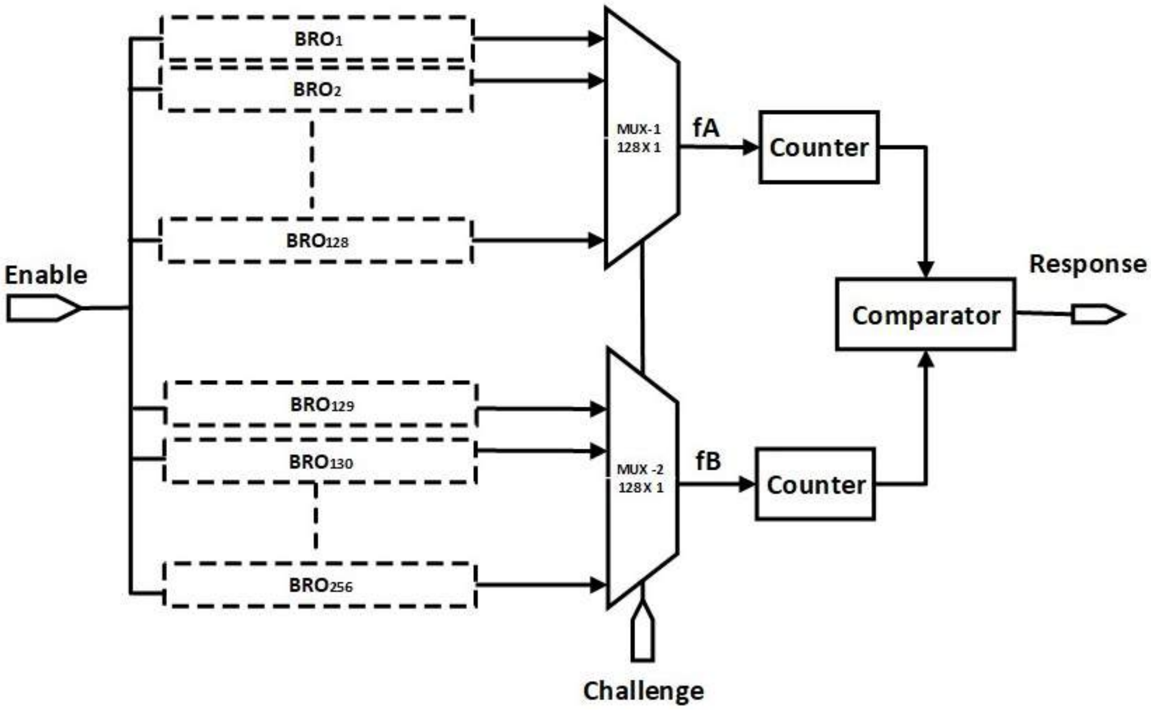


Figure 2.2: Bi-directional Ring Oscillator-based PUF [40].

two independent counters to measure their oscillation frequencies. A comparator then evaluates the counter values and produces the final one-bit response depending on which signal arrives faster. The BRO structure is realized by combining two ring oscillators using gated NOT and gated NAND logic, resulting in a flexible and efficient design. The frequency difference between the selected oscillators is thus exploited to generate a stable and unique PUF response bit. Using this topology, the susceptibility of the device to side-channel attacks is significantly reduced by appropriately selecting the control signal values as follows:

(a) The set of CRPs in the BRO-PUF architecture is directly changed by choosing different ring oscillators because the signal propagation direction alternates between the left and right routes.

(a) In addition, the suggested BRO-PUF architecture includes a halt-state mechanism in both directional modes that, when activated, disables response generation. This feature facilitates operational controllability and adds an additional layer of security by restricting unauthorized CRP extraction.

The complexity of RO-based PUF rises as the number of stages, corresponding to the quantity of linked ROs in the ring configuration, increases. With an increase in complexity, the PUF generates more unique and reliable responses. However, increasing the number of stages beyond a certain point can lead to performance saturation, where adding more stages does not provide significant improvements in the performance of the PUF. n-stage BRO [41] as shown in Figure 2.3.

Considering the gated NOT logic, a static inverter comprises charging and discharging paths regulated by two series-connected pMOS transistors and two series-connected nMOS transistors, respectively, to which the control inputs are applied as shown in Figure 2.3. nMOS is in the cutoff state if.

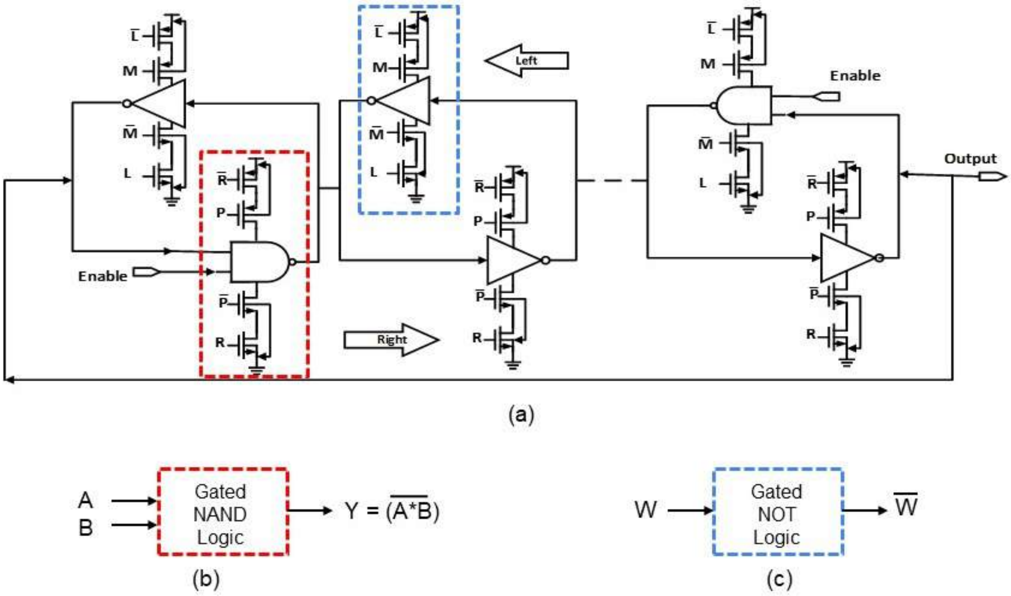


Figure 2.3: (a) The Structure of an n-Stage Bi-directional Ring Oscillator. Upper-gated logic is responsible for the leftward direction, and lower-gated logic is responsible for the rightward direction (b) Generalized diagram of gated NAND logic and (c) Generalized diagram of gated NOT logic [40].

$$V_{gsn} < V_{thn} \tag{2.1}$$

and it is in the ON state if

$$V_{gsn} \geq V_{thn} \tag{2.2}$$

Similarly, pMOS is in the cutoff state if

$$V_{gsp} > V_{thp} \tag{2.3}$$

and it is ON state if

$$V_{gsp} \leq V_{thp} \tag{2.4}$$

We consider the different values of the control signal and input signal operation

Table 2.1: Operation of Gated NOT logic.

Input Signal	**Control Signals**		**Output**
W	L	M	$\overline{W}$
X	0	0	Z
1	0	1	Z
0	0	1	1
1	1	0	0
0	1	0	Z
X	1	1	Z

X = Don't Care, Z = Floating Condition, 0 = GND, 1 = V_{DD}

Table 2.2: Right and left shift operation of BRO structure based on the control signal.

Enable Signal	**Control Signals**				**Output Oscillation**
	P	R	L	M	
0	X	X	X	X	No Oscillations
1	1	0	1	0	Propagate Rightward
1	1	0	0	1	Halt Rightward Propagation
1	0	1	0	1	Propagate Rightward
1	0	1	1	0	Halt Leftward Propagation

of gated NOT logic as shown in Table 2.1.

Case-I: If L = 0, and M = 0 and if input W = 0 or V_{DD},

One pMOS is in the ON state and one in the cutoff state similarly for the nMOS transistor so there is no path V_{DD} to GND and the output is in a floating condition. whatever the value is at input.

Case-II: If L = 0, and M = V_{DD} and if input W = 0,

output W' = V_{DD}, both pMOS are in ON state and both nMOS in the cutoff state, there is charging path from V_{DD} to output.

but if W= V_{DD} then both pMOS are in the ON state and both nMOS in the cutoff state, but inverter pMOS is in the cutoff state and output is floating.

Case-III: If L =V_{DD}, and M = 0 and if input W = V_{DD},

output W' = 0, both nMOS are in ON state, and both pMOS in the cutoff state, there is a path from output to GND to discharge the output.

But if W = 0, both nMOS are in the ON state and both pMOS in the cutoff state, but inverter nMOS is in the cutoff state so there is no path from output to GND and output is floating.

Case-IV: If L $=V_{DD}$, and M $=V_{DD}$ and if input W = 0 or V_{DD}

Here, one pMOS is in ON state and other is in cutoff state similarly for nMOS transistor so there is no path from V_{DD} to GND and output is floating.

Similarly, the operation of the gated NAND logic is performed. In the gated NAND logic structure when R= 0 & P= V_{DD} Both gated pMOS and nMOS transistors are in ON state, and output is generated. When the gating signal L or P arrives, the oscillator begins to oscillate. The RO's output will move to the right if L=1 and cease propagation if M=1. In the same way, it will move leftward if R=1 and stop propagation when P=1. Oscillation stops when M=1 in the rightward direction and R=1 in the leftward direction, as shown in Table 2.2.

2.2.2 Implementation Methodology

The proposed PUF design was implemented using a 40 nm technology node at a temperature of 25°C and a supply voltage (V_{DD}) of 1.1 V. To evaluate the impact of process variations, 100 Monte Carlo simulation iterations were performed at various stages, as illustrated in Figure 2.4.

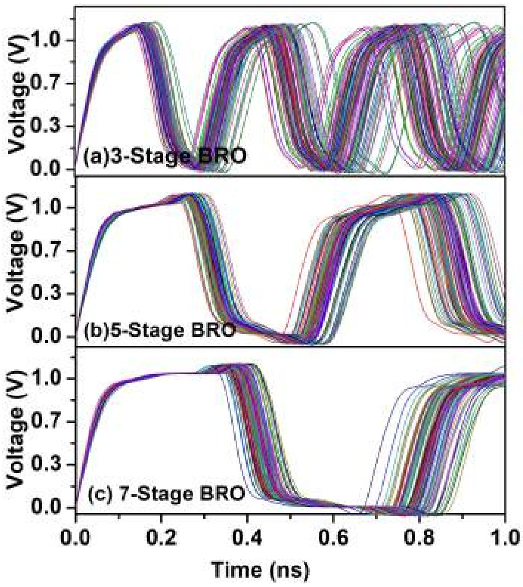


Figure 2.4: Monte Carlo simulation result for 3-stage, 5-stage, and 7-stage BRO [40].

Process variation and transistor mismatch were considered to account for intra-chip and inter-chip variations, respectively. For accurate identification of distinct chips, a Hamming Distance (HD) close to n/2 and a uniqueness (U) value of 50%.

In this study, 128 arbitrary challenges were applied to each of the m = 100 instances. So, 100 × 99/2 = 4950 comparisons were used to calculate inter-chip HD. A transistor-level Monte Carlo simulation methodology, widely adopted in prior PUF research (e.g., [42, 43, 45]), was employed for the experimental evaluation. Using 256 instances, 128-bit CRPs were generated simultaneously in the leftward direction and an additional 128-bit CRPs in the rightward direction. Figure 2.5 illustrates the distribution of zeros and ones. A total of 1000 samples of the architecture were analyzed, and the count of ones and zeros for each sample was recorded. It was observed that the counts of ones and zeros are nearly balanced for the 3-stage BRO-PUF, with the distributions centered around the mean values of 60.31 for the leftward direction and 62.15 for the rightward direction, exhibiting symmetrical distribution for both logic states.

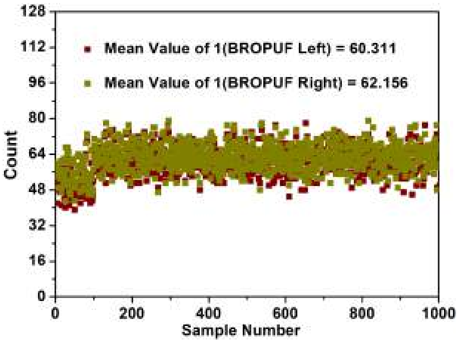


Figure 2.5: Allocation of one and zero in ASIC implementation for 3-stage BROPUF [40].

2.3 Functional Verification Using FPGA

A logically equivalent circuit corresponding to the proposed BRO-PUF architecture has been developed to validate its functionality. The bistable ring operation was verified using an XOR latch configuration, as shown in Figure 2.6. A total of 256 instances were implemented in the design. Two control signals, A and B, are employed to enable bidirectional operation by alternately switching their values to control the direction of signal propagation.

The implementation was carried out on three Basys3 FPGA boards using the Xilinx Vivado design suite. A MicroBlaze soft processor core was instantiated and integrated with the proposed PUF architecture to enable the generation, storage,

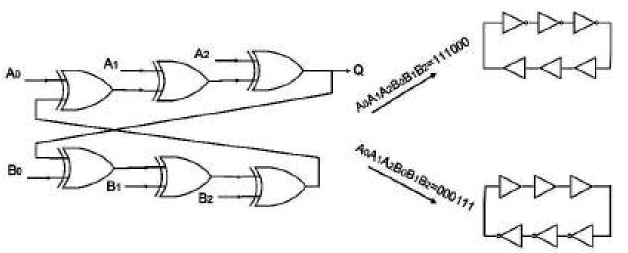


Figure 2.6: X-OR latch circuit (a) A=1, B=0 The upper inverter works for rightward operation (b) A=0, A=0, A=0, B=1 lower inverter works for leftward operation [40],[46].

and retrieval of CRPs. The MicroBlaze application was developed in the C programming language within the Xilinx SDK environment, as illustrated in Figure 2.7.

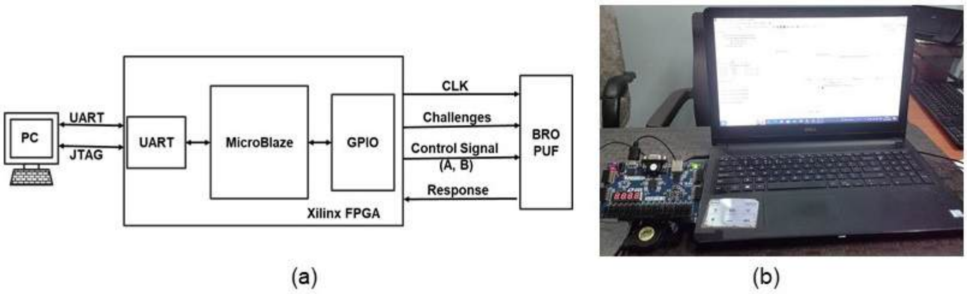


Figure 2.7: (a) Functional block diagram (b) Setup for CRP generation using Basys3 board [40].

Table 2.3: Resource utilization of 128-bit 3-stage BROPUF.

Component	No. of LUTs	No. of MUXs	No. of Registers
BRO (256-instances)	1792	0	0
Multiplexer	68	50	0
Counter	15	1	16
Comparator	0	0	1

The design and implementation were based on Verilog (HDL) for FPGA. TCL scripts were employed in vivado and plan to implement placement constraints as part of the methodology. Resource utilization of the BROPUF is as shown in Table 2.3. Figure 2.8 a comparison for the allocation of one and zero. 240 samples has been taken and based on each sample, the number of zeros and ones are shown in individual 128-bit responses. It is observed that although the scattered distribution, zeros, and ones are randomly distributed and centered around the mean value.

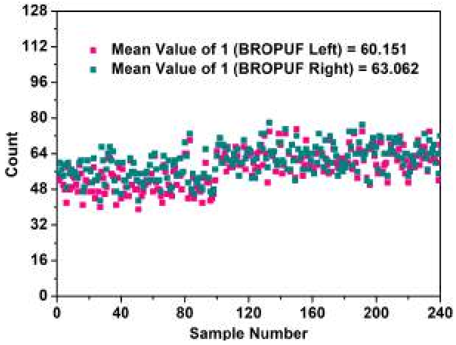


Figure 2.8: FPGA implemented the allocation of one and zero for the 3-stage BROPUF [40].

2.4 Performance Analysis

2.4.1 Comparative performance analysis of BRO stages

The post-layout performance of the proposed 3-stage BRO is compared with previously reported works, as summarized in Table 2.4. The layout of the 3-stage BRO, illustrated in Figure 2.9, was implemented with transistor widths of $W_{pMOS} = 240$nm and $W_{nMOS} = 120$nm. It is noted that the primary design objective of this work is to enhance security through dual CRP generation rather than to achieve aggressive area optimization.

To analyze the impact of performance metrics such as power consumption, delay, uniqueness, and reliability on the behavior of BRO-PUFs, this study focuses on the security implications of increasing the number of stages in the proposed architecture. Specifically, 3-stage, 5-stage, and 7-stage BRO configurations were evaluated

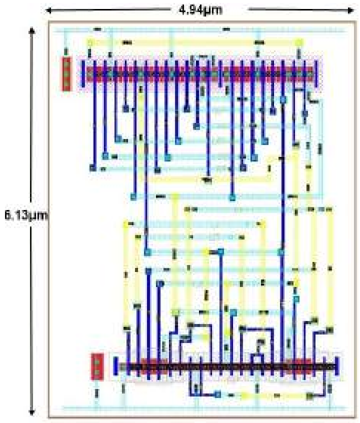


Figure 2.9: Layout of 3-stage BRO with W_{pMOS}=240nm and W_{nMOS}=120nm [40].

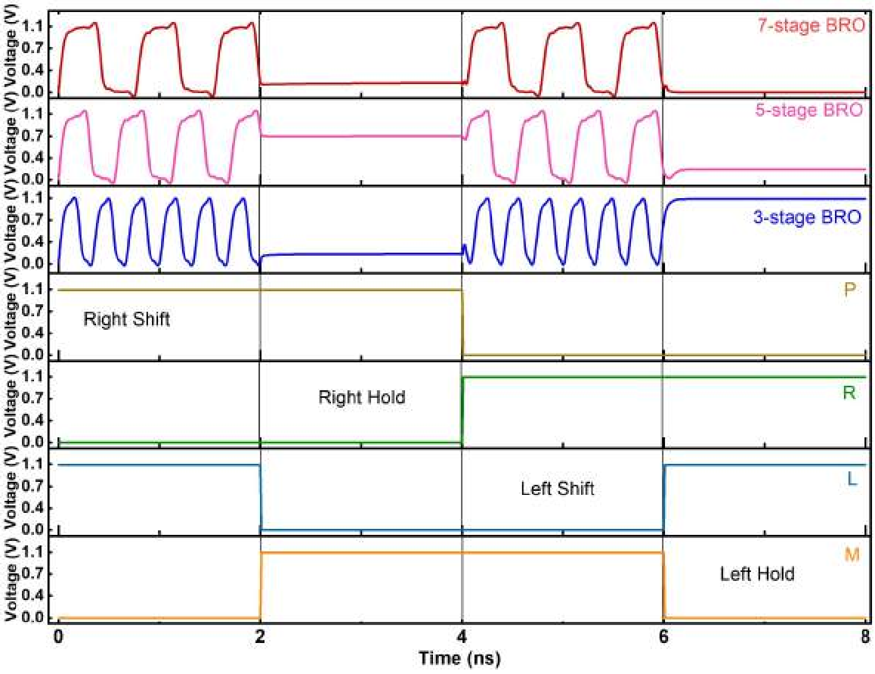


Figure 2.10: Signal propagation in BRO: output of bi-directional ring oscillators, control signal. P and R: Gating signals in right shift; L and M: Gating signals in left shift[40].

for both leftward and rightward operating modes. The frequency of oscillation, propagation delay, and power consumption were systematically measured for each configuration. These parameters are affected by design variables including transistor dimensions, biasing conditions, supply voltage, and operating temperature. Although variations in these parameters influence absolute performance values, the reported results are based on the fixed circuit configuration employed in this study. It is observed that the oscillation frequency is highest in the 3-stage BRO configuration compared to the 5-stage and 7-stage implementations. The signal propagation behavior of the BRO is illustrated in Figure 2.10.

The delay of a BRO is directly proportional to the gate capacitance and the resistance of the transistor, and inversely proportional to the bias current. Therefore,

Table 2.4: Performance comparison of ROs

Metric	**This Work**	**ICCEEE'19** [47]	**ICEE'20** [48]	**TCAS-II'09** [49]	**TCAS-II'13** [50]
Technology (nm)	**40**	40	40	40	40
RO inverter stages (N)	**3**	3	3	3	3
Average power (nW)	**50.8**	10,000	32,700	90	112
Frequency (MHz)	**1793**	12.3	10.5	3.7	500
Supply voltage (V)	**1.1**	1.8	1.2	1.8	0.6

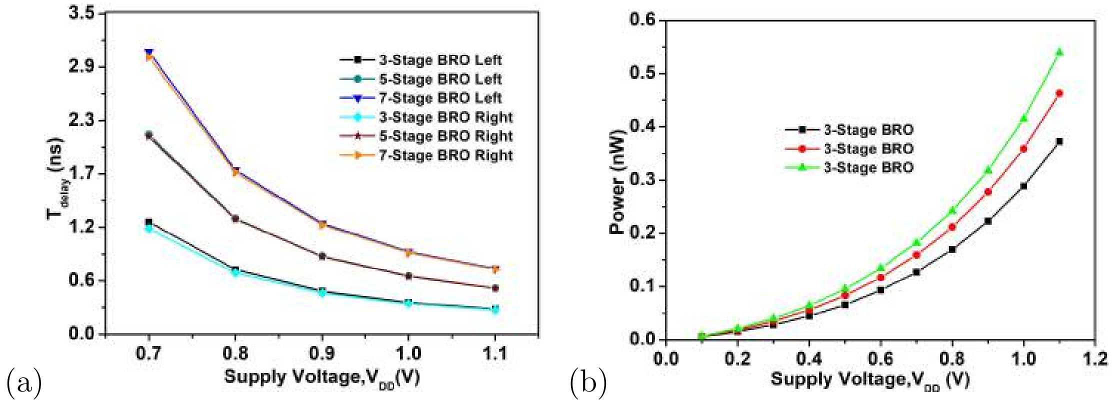


Figure 2.11: (a) Delay (b) Power comparison of 3-stage, 5-stage, and 7-stage BRO in both left and right directions [40].

increasing the number of stages will increase the delay due to the larger number of transistors in the signal path. As the number of stages in the BRO increases, the delay through the circuit will also increase. Figure 2.11a shows the delay concerning the supply voltage curve. For a ring oscillator with N stages to achieve self-sustained oscillation, it is necessary to maintain a phase shift of 2Π with unity gain at the oscillation frequency, the oscillator uses N stages, each providing a phase shift of Π/N. The remaining Π phase shift is accomplished through DC inversion. As a result, for a total phase shift of 2Π, the oscillating signal passes through each N inverter stage twice. The time for one full cycle is $2NT_{delay}$. The equation gives the oscillation frequency:

$$f = \frac{1}{2NT_{delay}} \tag{2.5}$$

Where f is the frequency of oscillation, N is the number of stages, and T_{delay} is the propagation delay of each stage. The frequency of the BRO is determined by both the number of stages in the loop and the delay per stage. A higher total delay in the loop results in a lower frequency, so a larger delay per stage leads to a lower frequency. The power dissipation of the BRO depends on the transistor sizes and their biasing conditions. The 7-stage BRO will consume more power compared to the 5-stage BRO, and the 5-stage BRO will consume more power compared to the 3-stage BRO. Figure 2.11b shows power dissipation at different stages. While operating it is found that leftward and rightward generate different delays. We observed that the delay of 3-stage, < 5-stage, and < 7-stage BRO and the delay of the rightward is lower than the leftward for all the stages. Similarly, the frequency of 3-stage, > 5-stage, and > 7-stage BRO. Based on delay and power consumption performance, 3-stage BRO is better than 5- and 7-stage BRO PUF.

2.4.2 Performance as a BRO PUF

The PUF response is generated by propagating a signal through multiple stages and the output is determined by the cumulative effect of the variations in each stage. The performance of BRO-based PUFs is affected by the quality of the RO stages, rather than the quantity [51]. The trade-off between these two factors depends on the number of stages in the RO circuit and the quality of the oscillator design [32].

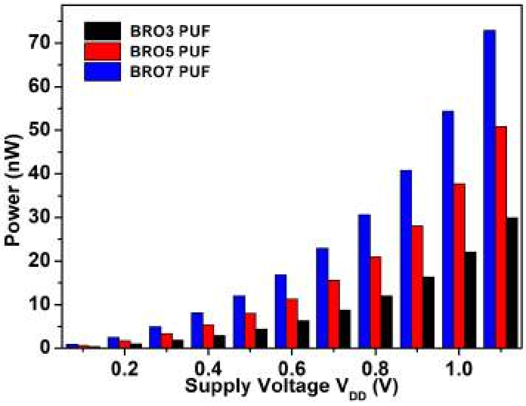


Figure 2.12: Power Dissipation of 3-Stage, 5-Stage, and 7-Stage BRO-Based PUF [40].

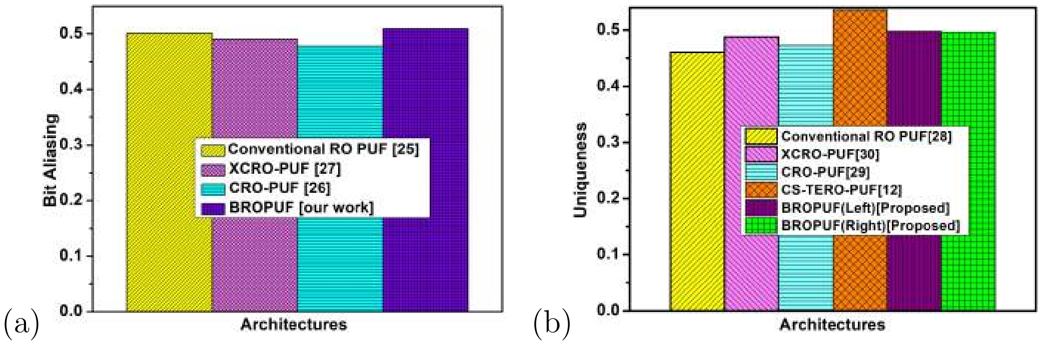


Figure 2.13: (a) Bit aliasing (b) Uniqueness comparison of various RO-PUFs [40].

The number of stages in the oscillator circuit impacts the reliability of the PUF. A PUF must have low power consumption to be employed in any resource-constrained application because each application has its power budget, which cannot be compromised. From Figure 2.12 it has been found that 7-stage BRO PUF consumes 2.43× higher than 3-stage BRO PUF and 1.7× higher than 5-stage BRO PUF.

Bit-aliasing: It determines the bias of a bit in the responses generated from different devices against the same challenge. That is, it estimates the biasing of 0 or 1 for the same bit in responses of multiple devices. Ideally, bit-aliasing should reach 0.5. Our proposed design has approached it very well with a value of 0.509 as depicted in Figure 2.13(a) shows a comparison for conventional RO PUF [29], CRO-PUF [52] and XCRO-PUF [53] architectures. The responses are biased equally because of the design of the RO in the PUF design.

Uniqueness: It is assessed by measuring the inter-chip Hamming distance of different PUFs' responses. Let's suppose that, about challenge R_a and R_b represent two n-bit response outputs from arbitrarily taken chips a and b out of m available chips. The uniqueness (U) can be quantified as:

$$U = \frac{2}{m(m-1))} \sum_{a=1}^{m-1} \sum_{b=a+1}^{m} \frac{HD(R_a, R_b)}{n} * 100\% \tag{2.6}$$

uniqueness, which assesses how well one PUF can be distinguished from others by calculating the average HD among PUFs in distinct chips (aiming for an inter-chip HD near 50% for sufficient uniqueness)[42, 45]. Figure 2.13(b) illustrates the unique values associated with various architectures. The outcome indicates that the suggested framework exhibits the utmost uniqueness, approaching closely to the ideal value of 0.5. and considering different stages of BROPUF it has been found that for BRO PUF uniqueness of the 3-stage BRO PUF is highest and that of 7-stage BRO PUF is lowest in both directions at nominal values 1.1V and 25°C. BRO PUF in rightward performs better than the leftward for all the stages. The histogram for uniqueness is shown in Figure 2.14. The percentage of Inter-chip HD is shown in Table 2.5.

Reliability: For an ideal PUF, the response variation at different environmental conditions should be zero. Temperature changes and voltage fluctuations primarily affect circuit delay, which can cause instability in the PUF response. To calculate reliability, the two responses obtained at different time instances under varying environmental conditions

Table 2.5: Inter-chip Hamming Distance percentage comparison at different temperatures.

Operating Condition	3-stage PUF	5-stage PUF	7-stage PUF
25°C	49.8	49.8	48.0
50°C	48.2	49.3	46.5
75°C	47.7	47.6	45.9

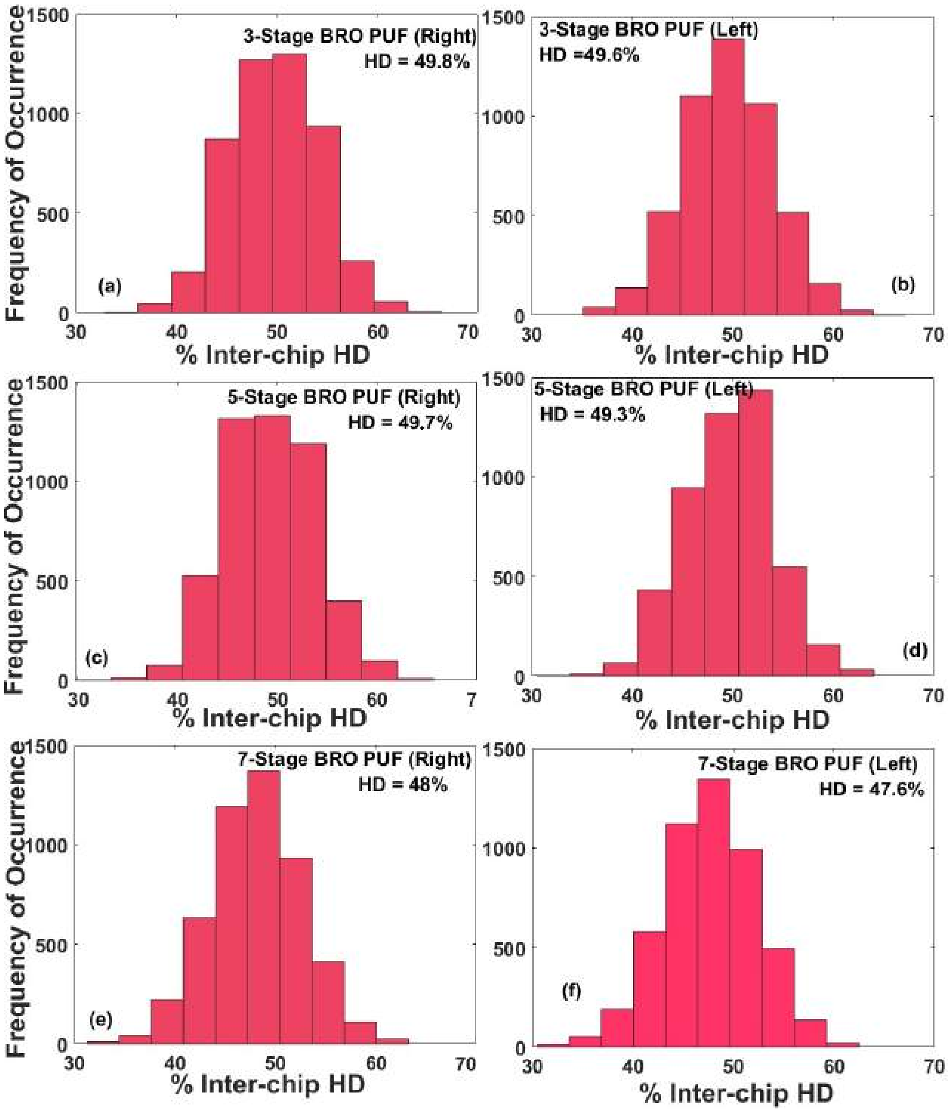


Figure 2.14: The representation of the inter-chip hamming distance of proposed BRO-PUF (a) 3-stage BRO-PUF Right (b) 3-stage BRO PUF Left (c) 5-stage BRO PUF Right (d) 5-stage BRO PUF Left (e) 7-stage BRO PUF Right (f) 7-stage BRO PUF Left[40].

are compared. The reliability R can be measured by:

$$R = 1 - \frac{1}{k}\sum_{m=1}^{k}\frac{HD(R_n, R_n^{'})}{n} * 100\% \tag{2.7}$$

Here, k represents sample count, n represents bits count generated, and $HD(R_n, R_n^{'})$ indicates the Hamming Distance between R_n and $R_n^{'}$. Different approaches like Bit-Flip Rate (BFR) and CRP analysis offer additional insights but may not capture overall uniqueness, and assessing reliability with intra-die Hamming Distance is important for evaluating response consistency within a single PUF instance in a chip, enhancing security. Figure 2.15 shows the reliability of the proposed PUF under various operating voltages. The

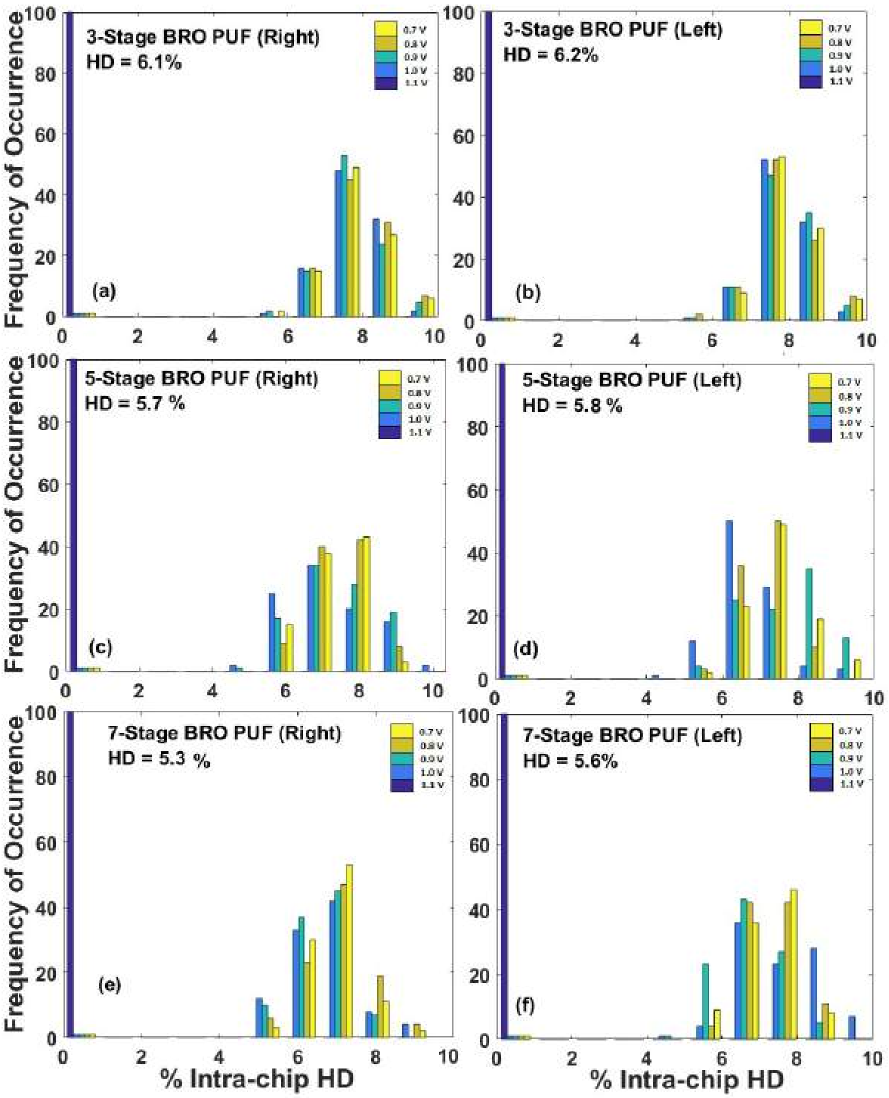


Figure 2.15: The intra-chip hamming distance for the proposed PUF (a) 3-stage BRO-PUF Right (b) 3-stage BRO-PUF Left (c) 5-stage BRO-PUF Right (d) 5-stage BRO-PUF Left (e) 7-stage BRO-PUF Right (f) 7-stage BRO-PUF left [40].

reliability of 3-stage BRO PUF is degraded by 6.56% and 13.11% as compared to 5-stage and 7-stage BRO PUF rightward and the reliability of 3-stage BRO PUF is degraded by 6.45% and 9.68% as compared to 5-stage and 7-stage BRO PUF in leftward. It is found that if the temperature increases then uniqueness is better however in the case of Intra HD variation when the temperature increases then reliability is degraded. The percentage of Intra-chip HD for different temperatures is shown in Table 2.6. With increasing temperature uniqueness is good but reliability is degraded. A comparative study with other work is shown in Table 2.7. We found that the CRPs of the proposed BRO PUF are the highest. we found that the uniqueness of the 3-stage BRO PUF with rightward is highest and in all stages rightward performs better than the leftward. Reliability is calculated

Table 2.6: Intra-chip Hamming Distance percentage comparison at different temperatures.

Operating Condition	**3-stage PUF**	**5-stage PUF**	**7-stage PUF**
50℃	3.34	3.56	2.78
75℃	3.43	3.72	3.19
100℃	3.70	3.72	3.44

Table 2.7: Performance Comparison of PUFs

Metric	**This Work**	**JSSC'19** [54]	**JSSC'19** [55]	**ISCAS'21** [56]	**ISSCC'15** [57]	**IEEE Access'19** [58]	**TCAS-I'25** [59]
Technology (nm)	**40**	40	40	40	40	40	45
Architecture used	**BRO**	Soft BD	Static Mono	RRAM	RO	Inv. based Array	SRAM
Response size (bit)	**256**	128	128	–	256	128	64
Supply voltage (V)	**1.1±10%**	0.9∼1.5	0.8∼1.0	1∼1.2	0.7∼1.2	1.1	0.6∼1.2
Uniqueness (%)	**49.8, 49.6**	49.6	49.0	48.6	50.07	49.99	49.37–49.89
Power consumption (μW)	**0.30**	–	151	–	28.4	0.32	–

using intra-die HD for BRO PUF it is found that 7-stage performs better than 5-stage and 5-stage performs better than 3-stage BRO PUF. The increased number of BRO PUFs enhances their effectiveness in these areas by providing more randomness and uniqueness in the generated keys or device identifiers.

2.5 Summary

This chapter presents a unique bidirectional ring oscillator-based PUF architecture designed specifically for IoT security applications, allowing challenge-response pair production in both operational directions under control signal guidance. The bidirectional nature greatly increases response variety and system robustness. A comprehensive examination of several oscillator stages demonstrates the importance of stage layout in balancing key design criteria like as uniqueness, reliability, area, and power consumption. Our findings show that careful selection of RO stages is critical for achieving optimal performance under specific application conditions. The expanded CRP space increases the system's entropy and unpredictability, making it more resilient against modeling and cloning attacks. These findings help to design more secure and efficient PUF-based authentication systems in resource-constrained IoT contexts.

Chapter 3

A Novel Gated Logic-based 10T-SRAM for Configurable RO

3.1 Introduction

This chapter explores an SRAM-based ring oscillator design based on gate logic. An SRAM cell is proposed using a gated-logic-based inverter, and a ring oscillator architecture is subsequently developed using the proposed cell. Pre-layout and post-layout simulations are performed to validate the functionality of the design using a 40 nm technology node at a supply voltage of 1.1 V and an operating temperature of 25°C. The gating logic not only ensures stable operation but also provides flexibility in managing the activation and deactivation of the oscillator, thereby reducing power consumption during idle periods. Furthermore, the impact of aging, temperature variations, and supply voltage V_{DD} on the oscillation frequency is analyzed to evaluate the robustness and reliability of the proposed ring oscillator. The simulation results demonstrate bidirectional operation, indicating that the architecture is well suited for security-driven and power-efficient applications, particularly in resource-constrained and embedded system environments.

The goal of this study is to overcome the limitations of traditional 6T SRAM cells in creating memory architectures that merge ring oscillator capabilities. Multiple 6T SRAM cells can be used to achieve RO behavior[60]. However, these methods lack directionality control and integration efficiency. This work improves the design of intelligent memory-integrated circuits by proposing a unique 10T gated-logic SRAM-based ring oscillator with bi-directional behavior, allowing for in-memory oscillation with better control and density. The PMOS recovery time is much higher for GLI as compared to other topologies. T-

SRAM is designed here with clocked power sources that reduce power consumption in the macro [61]. A bi-directional gated ring oscillator (BDGRO) is employed for time-based signal processing, utilizing gated logic-based inverters for time integration [41]. An Embedded SRAM Ring Oscillator (ESRO) structure is implemented to measure the degradation of 6T SRAM cell transistors caused by BTI effects and evaluate frequency degradation [60].

3.2 Gated logic based SRAM Ring Oscillator

3.2.1 Gated Logic

The logical behavior of the gated logic as an inverter or high-impedance state (Z) depends on the enable signals EN/ENB and input IN and corresponding output OUT as shown in Figure 3.1. The operating condition of the gated logic is listed in Table 3.1 for different conditions of enable and input signals. When $EN = 0$ and $IN = 0/1$, the circuit behaves as an inverter, it corresponds $OUT = 1/0$ as shown in Figure 3.1(a). Similarly, when $EN = 1$ and $IN = 0/1$, the circuit entered into the high-impedance state ($OUT = Z$) as shown in Figure 3.1(b). A latch arrangement by connecting two gated logic back to back is designed and the operating conditions are decided by the enable signals as shown in Figure 3.1(c). The threshold voltages of the PMOS and NMOS are the same so that the logic can act as a perfect switch. To study the relationship between time and voltage in a delay stage, we have considered the process described in Figure 3.1(c). If $\mathrm{V_c} < \mathrm{V_{Th}}$, the PMOS transistor is in saturation region whereas if the $\mathrm{V_{Th}} < \mathrm{V_c} < 0.5\mathrm{V_{DD}}$, the PMOS transistor is in triode region. Here $0.5\mathrm{V_{DD}}$ is the circuit threshold voltage. The transistor offers a resistance $\mathrm{r_{on}}$ in the triode region and a constant current $\mathrm{I_{sat}}$ in the saturation region.

Table 3.1: Operating Condition of Gated Logic (GL).

IN	EN	ENB	OUT	Gated Logic
0	0	1	1	Inverter
1	0	1	0	Inverter
0	1	0	Z	Open Circuit
1	1	0	Z	Open Circuit

Z = Floating Condition, 0 = GND, 1 = $\mathrm{V_{DD}}$

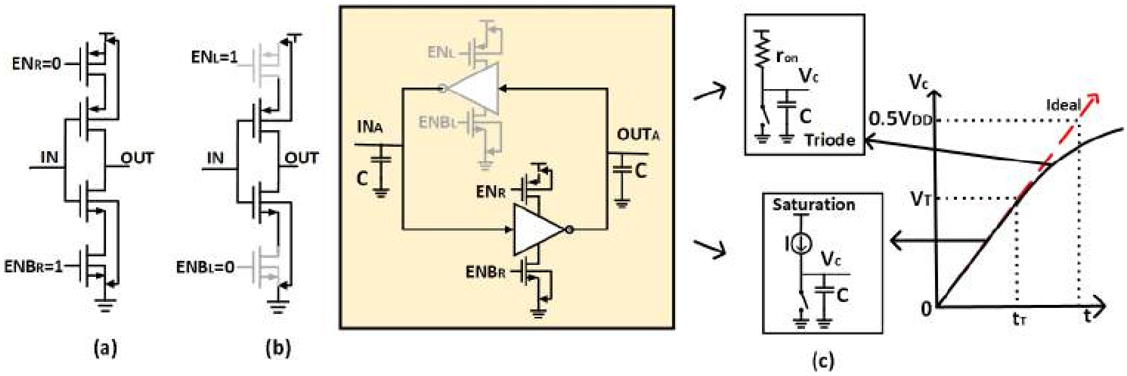


Figure 3.1: Operation of the gated logic (a) when $EN = 0$, (b) when $EN = 1$, (c) charging steps of gated delay in the right shift [62].

3.2.2 Proposed Gated Logic-based SRAM cell (GL-SRAM)

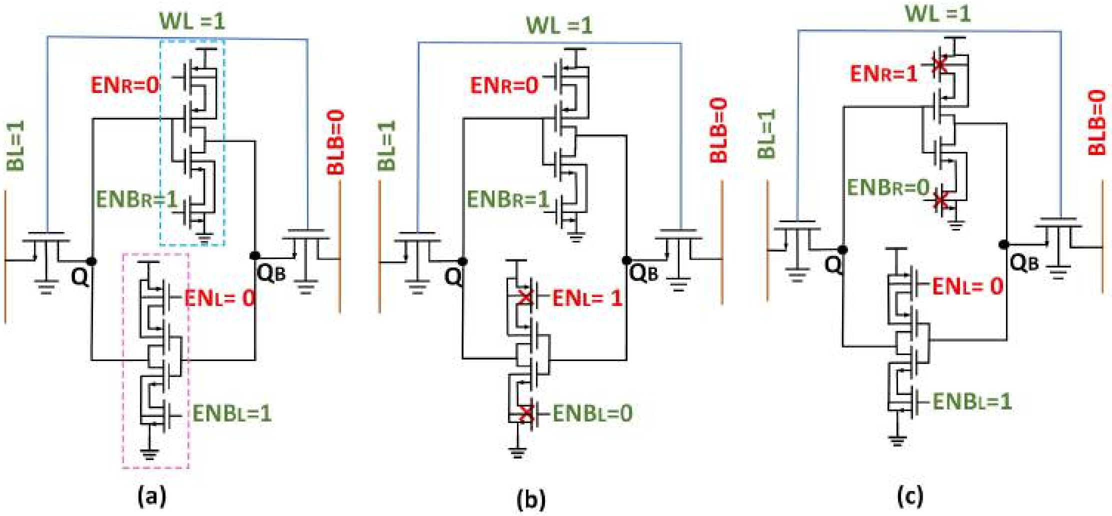


Figure 3.2: Proposed gated logic-based SRAM cell behavior as (a) Storage cell (b) GL-1 as inverter and GL-2 as an open circuit, and (c) GL-1 as an open circuit and GL-2 as an inverter [62].

Gated logic is also used to construct the proposed 10T SRAM cell as shown in Figure 3.2(a). Table 3.2 presents the working state of the proposed cell for different operating modes. The storage cell requires two gated logic and two access transistors for reading/writing the information into the SRAM cell. The circuit behaves as a storage cell, left shift and right shift based on the status of the gated logic enable signals.

If wordline $WL = 1$, bitlines are precharged to V_{DD}, $EN_R = EN_L = 0$ and $ENB_R = ENB_L = 1$ then both the gated logics (GL-1 and GL-2) are ON and the circuit act as an SRAM cell as shown in Figure 3.2(a). Now to perform the various SRAM operations, the status of WL, BL, and BLB changes. If $EN_R = 0$, $ENB_R = 1$, $EN_L = 1$ and $ENB_L = 0$,

Table 3.2: Status of the control signals of Gated Logic (GL) based SRAM Cell

Bitline (BL/BLB)	Wordline (WL)	$\mathbf{EN_R/ENB_R}$ (GL-1)	$\mathbf{EN_L/ENB_L}$ (GL-2)	GL (Inverter)
1/0 (↑)	1	0/1	1/0	Upper
1/0 (↑)	1	1/0	0/1	Lower
1/0 (↑)	1	0/1	0/1	Both

(↑) = Precharge

then GL-1 and GL-2 act as a high impedance Z and the backward inverter, respectively as shown in Figure 3.2(b). Similarly, if $EN_R = 1$, $ENB_R = 0$, $EN_L = 0$ and $ENB_L = 1$, then GL-1 and GL-2 behaves as a forward inverter and high impedance Z, respectively as shown in Figure 3.2(c).

To implement the ring oscillator WL = 0 and enabling the forward inverters is considered. The SRAM-based ring oscillator as discussed in the next section.

3.2.3 Proposed SRAM-Based Ring Oscillators

GL-SRAM allows selective control for the direction of the SRAM ring oscillator is active at a given time. Figure 3.3 shows the proposed n-stage gated logic SRAM-based ring oscillator (GL-SRAM-RO). It is designed to produce periodic oscillations with an odd number of SRAMs which can be used to design the PUFs. We executed the RO behavior in a GL-SRAM-RO during the SRAM read operation by connecting five SRAM cells horizontally. QB output of the SRAM cell is connected to the Q of the next cell to form the loop. For the proper functionality of the proposed RO, we have enabled word line (WL) and bit lines (BL/BLB) to be precharged. Pass transistors can be utilized to provide connectivity between cells, as they behave as non-ideal switches. The rightward oscillator is built using the upper inverter of the SRAM cells and the ring oscillator works in a clockwise direction. This direction is determined by the control signals EN_R/ENB_R and EN_L/ENB_L, which allow the signal to flow through the ring in a specific manner as discussed in the previous subsection.

Ring oscillator with N stages to achieve self-sustained oscillation, it is necessary to maintain a phase shift 2π with unity gain at the oscillation frequency. The oscillator used N stages, each providing a phase shift of π/N. The remaining π phase shift is accomplished through DC inversion. As a result, for a total phase shift of 2π, the oscillating signal passes through each N GL-SRAM-based inverter stage twice. The time for one full cycle is $2\mathrm{NT}_{\mathrm{delay}}$ and the oscillation frequency is given by:

$$\mathrm{f} = \frac{1}{2\mathrm{NT}_{\mathrm{delay}}} \tag{3.1}$$

Where f is the frequency of oscillation, N is the number of stages, and T_{delay} is the propagation delay of each stage. The frequency of the GL-SRAM-RO is determined by both the number of stages in the loop and the delay per stage. A higher total delay in the loop results in a lower frequency. To achieve the higher frequency it is important to optimize and improve the delay of each GL-SRAM cell. The latency of the EN/ENB transition is limited to only a few gate delays, which is negligible compared to the overall oscillation period. The circuit consumes the same power in both directions of oscillation and the latency remains same because as the forward and reverse inverters are both identical.

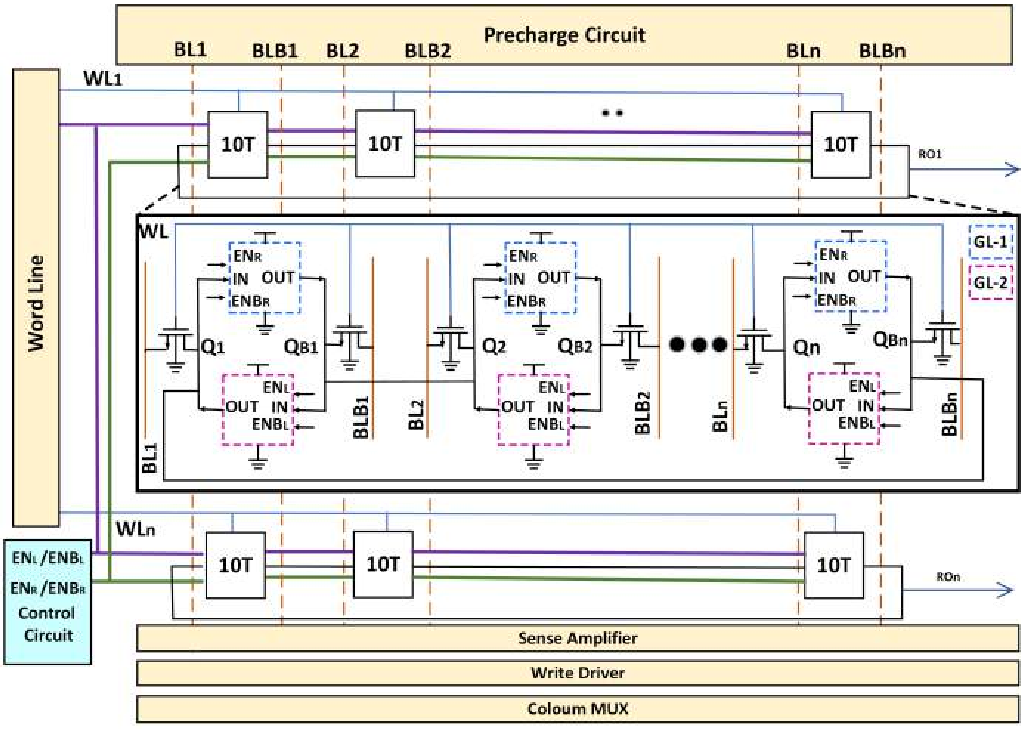


Figure 3.3: Proposed SRAM architecture with n-stage GL-SRAM-based ring oscillator [62].

3.3 ASIC Implementation and Simulation Results

The pre and post-layout simulation of all the considered circuits were conducted using the Cadence Spectre environment, and reliability analysis was carried out using the RelXpert design simulator using UMC 40nm process technology. For all the simulations, we have

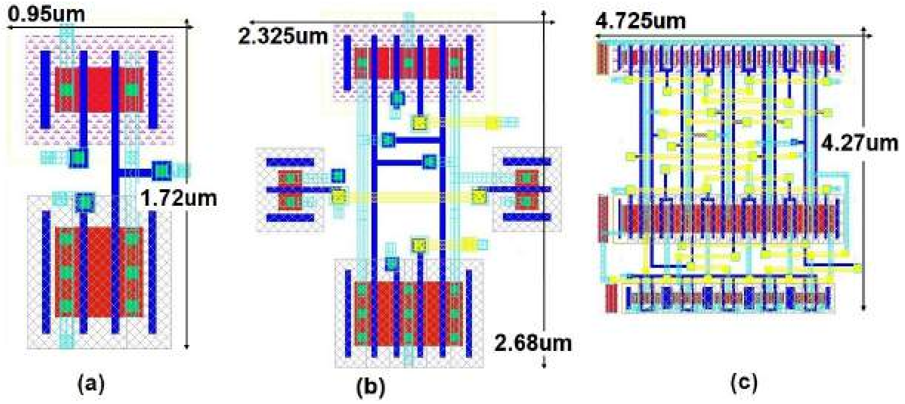


Figure 3.4: Layout of (a) Gated inverter (b) Gated inverter based SRAM cell, and (c) a 5-stage GL-based SRAM ring oscillator [62]

considered 1.1V supply voltage, 27°C operating temperature unless specified. The layout of the gated-logic-based inverter, GL-based SRAM, and GL-SRAM-based RO is shown in Figure 3.4.

3.3.1 Inverter Configurations

Table 3.3: PDAP Comparison across Process Corners for Different Inverter Topologies with different capacitance

Corner	2T-INV	GL-INV	AICSP'23 [63]	TED'20 [64]
1pF (SS)	11.83	4.42	15.45	15.7
1pF (TT)	15.26	5.99	16.78	17.2
1pF (FF)	18.57	7.62	19.05	19.1
100pF (SS)	13.02	4.78	16.97	18.21
100pF (TT)	17.11	6.67	17.63	19.35
100pF (FF)	21.23	8.70	19.05	21.49

To evaluate the effectiveness of the gated logic circuit we have computed different parameters for all the inverter circuits. Results indicate that the power dissipation of a GL-based inverter is approximately the same as a conventional GL-INV dissipating more power 1.10×, 1.42× and 2.29× more power than the ARI, TG-ARI, and 2T-INV inverters. We also analyzed the delay of all the considered inverters. The results show that the gated logic-based inverter offers less delay as compared to the other considered inverters. GL-INV offers 2.22×, 5.94×, and 4.94× smaller delay as compared to the 2T, ARI, and TG-ARI inverters respectively. The PDAP variation is shown in Table 3.3 and Table 3.4

Table 3.4: PDAP Comparison across Process Corners for Different Inverter Topologies at different supply voltage

Corner	2T-INV	GL-INV	AICSP'23 [63]	TED'20 [64]
1.1V(SS)	11.83	4.42	15.45	15.7
1.1V(TT)	15.26	5.99	16.78	17.2
1.1V(FF)	18.57	7.62	19.05	19.1
1V (SS)	13.02	4.78	15.97	12.3
1V (TT)	17.11	6.67	17.63	15.6
1V (FF)	21.23	8.70	20.05	16.7
0.9V (SS)	13.02	4.2	13.97	9.57
0.9V (TT)	17.11	4.47	16.3	14.6
0.9V (FF)	21.23	6.2	18.1	16.4

In addition, we also calculated the area requirement for all inverter circuits considered.The results show that the area of GL-INV offers 3.08 ×, 1.14× higher and 1.06× smaller as compared to the 2T-INV, ARI and TG-ARI respectively. For the combined effect of power, delay, and area, we also calculated the power delay area product (PDAP) for all the considered inverter circuits. From the results, we observe that the GL-based inverter has the lowest PDAP as compared to the ARI and TG-ARI inverter circuits. From the above discussion, we conclude that the GL-based inverter is the better choice considering power, delay, and area. Considering the reliability of the circuit, we have analyzed the effect on threshold voltage with different stress time as well as temperature and supply voltage as shown in Figure 3.5(a),(b)and (c). Results indicate that the change in threshold voltage is less for the GL-based inverter with other inverter configurations.

3.3.2 SRAM Cell Structure

We have designed and analyzed 6T SRAM and GL-SRAM cells at typical process corners considering 1.1V supply voltage and 27°C. We performed detailed simulations and analyzed various parameters for all the considered SRAM cells.

Stability Analysis

Static Noise Margin (SNM) of the SRAM is a crucial metric used to evaluate the stability and robustness of memory cells during read, write, and hold operations [61][65]. Write SNM measures the ability of the SRAM cell to switch its state during a write operation successfully. If the Write SNM is too low, the cell may resist state changes, leading to write failures. A higher Write SNM indicates more robustness during write operations.

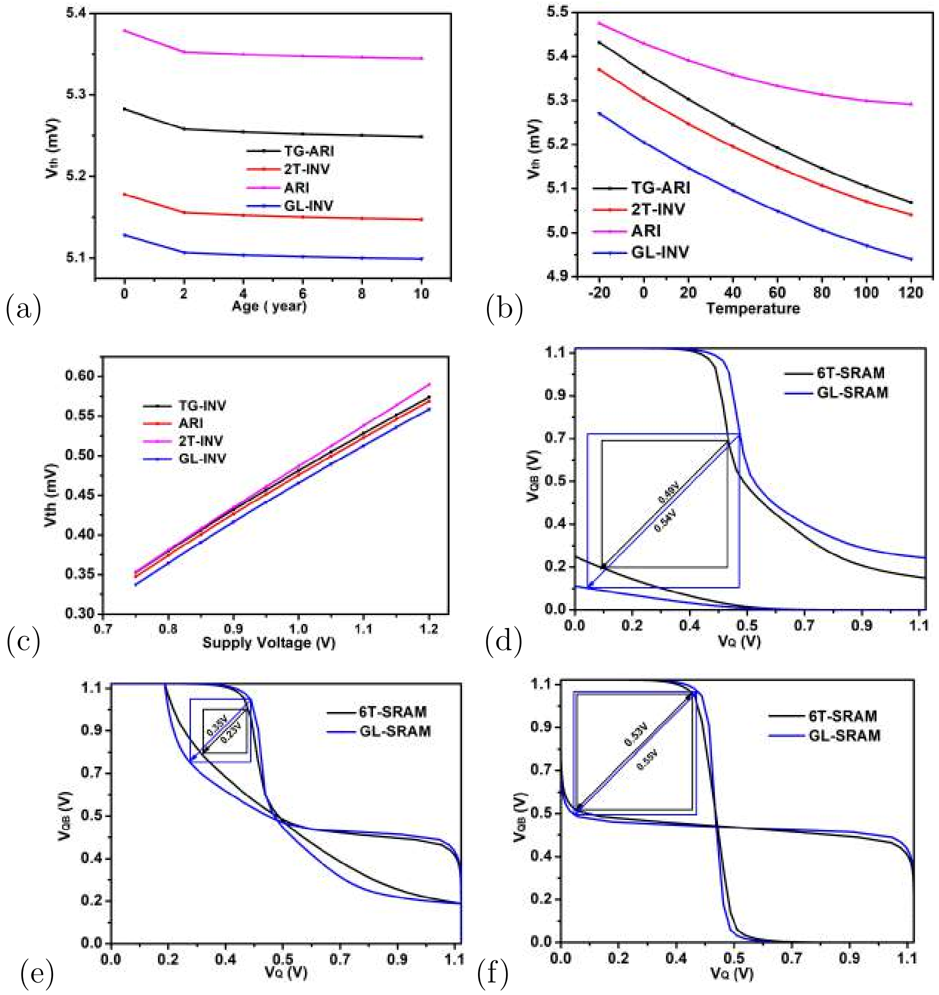


Figure 3.5: Stability analysis of SRAM cells (a) Change in threshold voltage with age (b) Change in threshold voltage with temperature (c) Change in threshold voltage with supply voltage for Inverters (d) Write SNM (e) Read SNM and (f) Hold SNM [62].

Similarly, the read SNM refers to the stability of the stored data in the SRAM cell during a read operation. When reading data, the access transistors are turned on, allowing the stored data to be sensed by external circuitry. This process can disturb the internal state, potentially causing it to flip and lose data. A higher Read SNM indicates more stability during read operations. whereas a lower one can lead to read disturb issues, where the content in the cell might change unintentionally during a read operation. The butterfly curve method was used in cadence virtuoso to examine the SRAM cell's Read, Write, and Hold SNMs. The word line was kept low in Hold SNM, while the bit lines were left floating to isolate the cell. To assess stability under read conditions, the word line was triggered and the bit lines were precharged to VDD. For write SNM, one bit line was set low and the other set high, with the word line enabled to test the cell's ability to flip its stored state. Figure 3.5(d) (e)and (f) show the write, read and hold noise margin for all the considered SRAM cells. 1.11× higher write SNM and 1.16× higher lower Read SNM than 6T SRAM. Results indicate that the read and write stability of the GL-SRAM cell is better as compared to the 6T SRAM cell and for the SVNM of the GL-SRAM cell is 1.005× higher than the 6T-SRAM. Similarly, the SINM represents the current-based noise margin of the SRAM cell indicating stability in terms of current variations. GL-SRAM has the higher SINM which is 1.038% higher than 6T-SRAM.

Delay Analysis

Results indicate that the 6T offers minimum delay as compared to the other SRAM cells. The read delay of the 6T-SRAM is 1.38× than the GL SRAM , respectively. Similarly, the write delay of the GL-SRAM is 1.30× less than 6T-SRAM cells, respectively.

Power and Area Analysis

We have also calculated the power dissipation of the various SRAM cells during read and write operations. The read power dissipation for the GL-SRAM has 1.17× lower power than the conventional 6T SRAM cell. Similarly, the write power dissipation for the GL-SRAM cell is 1.02× lower than 6T SRAM cell, respectively. Further, 6T-SRAM has the smallest cell area requirements and is 1.23× less than the GL-SRAM. GL-SRAM is thus preferred for embedded applications with limited power, such as edge devices of the IoT, biomedical devices, and security devices, where power savings are more important than area efficiency. The Read and Write Power Delay Product (PDP) and Power–Delay–Area Product (PDAP), where

$$PDAP = PDP * Area$$

to effectively mark the energy efficiency and power efficiency of the design, and the Normalized Figure of Merit (FOM)[66], which is found to be 0.34 for the proposed GL SRAM.

3.3.3 SRAM-based Ring Oscillator

We examine the GL-SRAM-RO output during the schematic and post-layout phases. The GL-SRAM-RO oscillates in the two directions according to the gating signals as shown in Figure 3.6(a). Figure 3.6(b) shows the comparison of schematic and post-layout simulation results for frequency variation with temperature at different process corners. The parasitic extraction was carried out in cadence virtuoso with calibre tool, which includes both

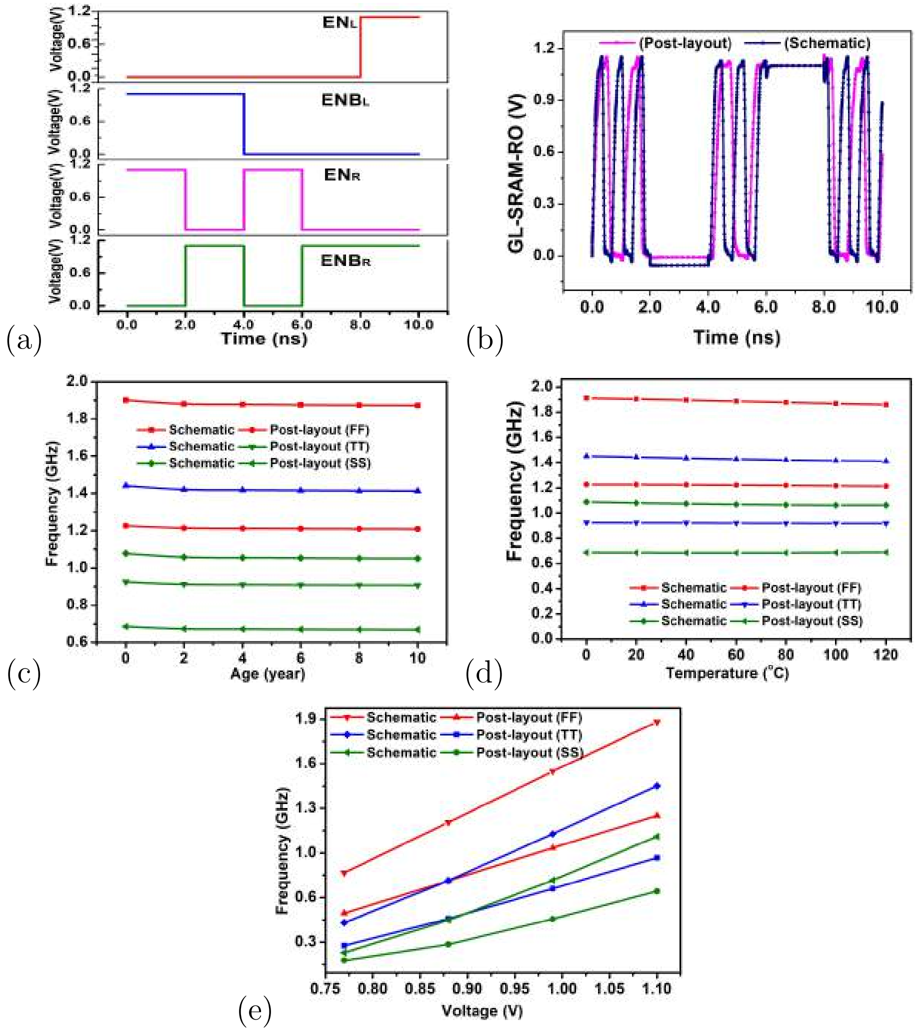


Figure 3.6: Comparison (a),(b) Gating signals and the output of GL-SRAM-RO in schematic and that in post-layout. The frequency of GL-SRAM-RO is 1.54GHz in the schematic and 1.24GHz in post-layout, (c) Frequency with NBTI aging for pre and post-layout simulations, (d) Frequency with temperature for pre and post-layout simulations, (e) Frequency with supply voltage for pre and post-layout simulations [62].

resistive and capacitive parasitics. The extracted netlist was then back-annotated into the SPICE environment for transient simulations under the same biasing conditions as the pre-layout case. For layout optimization, we minimized parasitics by adopting symmetry-aware placement. Despite these optimizations, some degradation is inevitable due to RC parasitics. The reported frequency drop therefore reflects a realistic scenario under post-layout conditions. From the results it is observed that the frequency in post-layout simulation results is low compared with schematic simulation and frequency decreases with temperature.

The parasitic capacitance and resistances generated by the transistors, load MOS

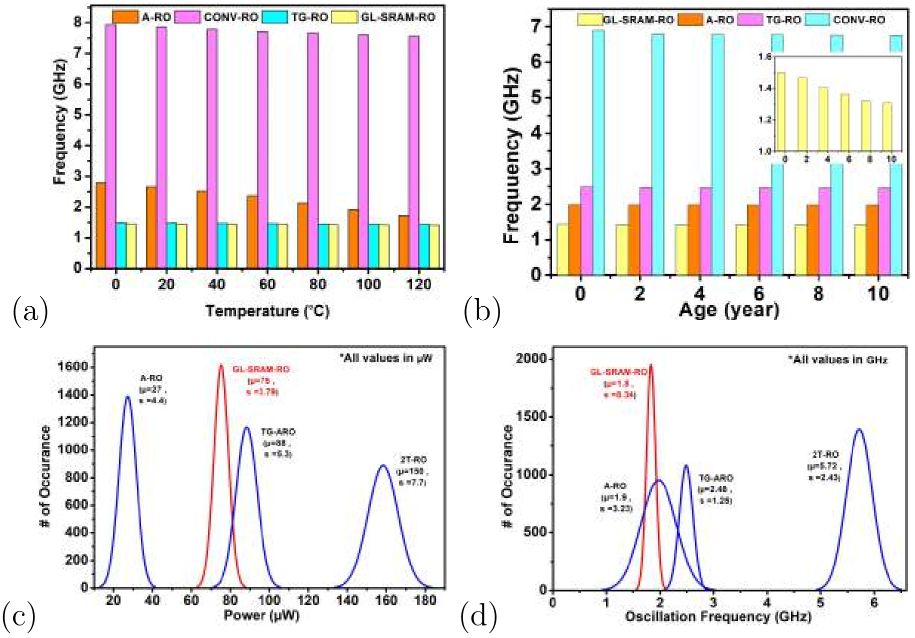


Figure 3.7: Comparison: (a) Temperature variation effect on the oscillation frequency of different RO circuits, (b) Frequency variation with aging (c) and (d) 2000 Monte Carlo analysis of Power and frequency of different RO circuits[62].

Table 3.5: Performance analysis of various RO structures

Parameters	Conv-RO	A-RO [67]	BDGRO [41]	SRAM-RO [60]	4TXOR-RO [68]	TG-RO [63]	Proposed RO
Technology (nm)	40	40	130	55	40	40	40
Supply Voltage (V)	1.1±10%	1.1±10%	1.2	1.0	1.1±10%	1.1	1.1
Area (μm^2)	29.33	59.67	26.9	38.5	53.84	-	20.17
Frequency (MHz)	1810	402.9	284	14.5	669.3	2490	1540
Mode of operation	Unidirectional	Unidirectional	Bidirectional	Unidirectional	Unidirectional	Unidirectional	Bidirectional
Power (μW)	40	27.1	27.9	-	32	37	12.2

capacitors, buffers, and interconnects are responsible for the larger time in the post-layout. Further, we also analyzed the oscillation frequency at different process corners for different stress time as shown in Figure 3.6(c). Figure 3.6(d) shows the oscillation frequency of all the considered ring oscillators with varying temperatures and with varing voltage ranges as shown in Figure 3.6(e).The frequency variation at different reliability parameters is quite low for all the corners which verifies the reliability of the GL-SRAM-RO. It is observed that the oscillation frequency of the proposed GL-SRAM-RO remains the same with the change in operating temperature, as discuss in Figure 3.7(a). Further, we also calculated the oscillation frequency of different ROs with stress time as shown in Figure 3.7(b). Results indicate that the oscillation frequency of most of the ROs is affected by stress time. For the process variations analysis on the GL-SRAM-RO, we have performed 2000 Monte Carlo simulations for the power dissipation and oscillation frequency as shown in Figure 3.7(c) and (d). From the results, it is noticed that the proposed GL-SRAM-RO shows less process variations. Table 3.5 illustrates the comparison of various performance parameters of different ring oscillator circuits. Results indicate that the GL-SRAM-RO dissipates minimum power as compared to the other RO structures.

3.4 Summary

In this chapter, we present an SRAM cell with gated logic, which is further utilized for the implementation of an SRAM-based ring oscillator, whose bidirectional behavior enables the design of a configurable oscillator. The use of gated logic design offers significant benefits in reducing power consumption and low area utilization. GL-SRAM-RO performance comparison with previous art to ensure low power (12.2 μW), area utilization (20.17 μm^2), and bidirectional behavior validated through post-layout simulation results.

Chapter 4

Tri-state Logic SRAM Array: Reconfigurable design as SRAM Array and Bidirectional RO

4.1 Introduction

As discussed in Chapter 1, the in-memory computation framework forms the basis for integrating memory structures with computational logic. Unlike conventional architectures, which shuttle data between separate processing and storage units, CIM performs computations directly where the data reside, offering two key advantages: a substantial reduction in intermediate data transfers and improved parallel computing efficiency with respect to both energy consumption and area overhead [69] as shown in Figure 4.1. The configurable ring oscillators were also introduced in that chapter, implemented with SRAM Array.

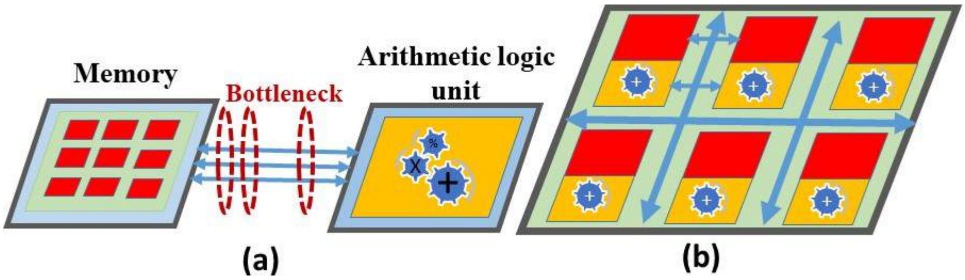


Figure 4.1: Comparison between (a) traditional von Neumann architechture and (b) CIM arhitecture.

In Chapter 2, a gated-logic-based approach using a 10T SRAM cell as the memory element was presented, where a bidirectional ring oscillator architecture was implemented and evaluated against existing designs. In this chapter, a tristate-inverter-based SRAM ring oscillator is proposed, and its functionality is validated across multiple oscillator stages through simulation and performance analysis to enhance control, flexibility, and robustness of operation. Pre-layout and post-layout simulations are carried out to validate the functional correctness of the proposed design using a 40nm technology node at a supply voltage of 1.1 V and an operating temperature of 25°C. In addition, a comprehensive performance evaluation is conducted by analyzing oscillation frequency variations with respect to aging effects, temperature changes, and supply voltage. The results demonstrate that the tristate SRAM-based ring oscillator provides improved control capabilities and reliable operation, making it a suitable candidate for secure and low-power applications in resource-constrained and embedded systems.

4.2 Tristate Logic based SRAM Ring Oscillator

4.2.1 Tristate Logic based Inverter

Different inverter topologies are used for configurable RO as shown in Figure 4.2 (a) conventional aging resilient inverter (ARI)[65] (b) transmission gate-based aging resilient inverter (TG-ARI)[63] (c) conventional inverter (2T-INV) (d) Tristate inverter (TL-INV) exhibits lower deterioration compared to conventional inverters. Table 4.1 shows the working behavior of TL-INV with enable signal.

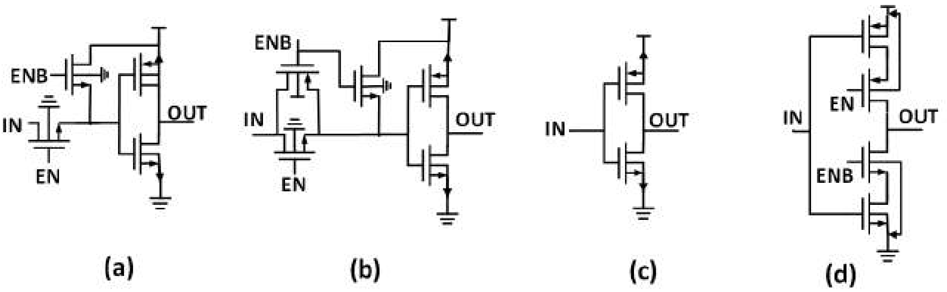


Figure 4.2: Different Inverter Topologies: (a) Conventional aging resilient inverter (ARI), (b) Aging resilient transmission gate-based inverter (TG-ARI) (c) Conventional inverter (2T-INV) (d) Tri-state inverter (TL-INV).

Considering a tristate inverter here again, the degradation is less compared to conventional inverters, ARI, and TG-ARI. The recovery time for PMOS is much longer than in other topologies.

Figure 4.3a displays the operation of tristate logic with input *IN* and output *OUT*

Table 4.1: Operating Condition of Tristate Logic (TL) with input (IN) and control signal (EN) corresponding to Figure 4.2d.

IN	EN	ENB	OUT	Gated Logic
0	0	1	Z	Open Circuit
1	0	1	Z	Open Circuit
0	1	0	1	Inverter
1	1	0	0	Inverter

Z = Floating Condition, 0 = GND, 1 = V_{DD}

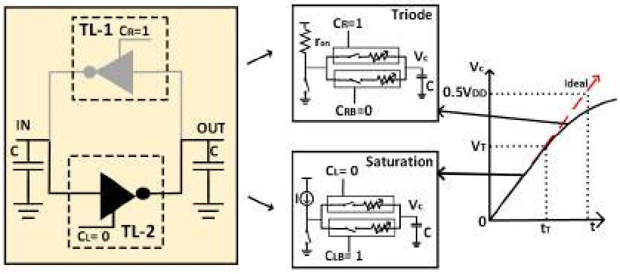


Figure 4.3: (a) Operation of tristate logic connected back-to-back and (b) charging steps of gated delay in right shift.

connected to C_L and C_R as control signals. Figure 4.3b describes the transmission gate in the tristate inverter is bilateral. This bilateral operation is used as a control circuit because, as a result of this behavior, the inverter can move into a high-impedance state while behaving as an inverter. The value of the logic level OUT is $IN \times C_L$. To simplify the study, assume that nMOS and pMOS transistors have an equal threshold voltage V_T. A transmission gate serves as a perfect switch. Since the pMOS transistor will operate in saturation if $v_c < V_T$ and triode if $V_T < v_c < 0.5V_{DD}$. $0.5V_{DD}$ is the threshold voltage of the inverter, the transistor is expressed as a resistor of resistance r_{on} in triode and a current source of constant current I in saturation [70]. The capacitor voltage is given by

$$C\frac{dv_c}{dt} = I, (0 \leq t \leq t_1)(Sat.) \tag{4.1}$$

in saturation region

$$C\frac{dv_c}{dt} = g_{on}(V_{dd} - \ v_c) + CV_T\delta(t), (0 \leq t \leq t_2)(Tri.) \tag{4.2}$$

in the triode. here $g_{on} = \frac{1}{r_{on}}, t_1 = t_T, t_2 = t - \ t_T$.

4.2.2 Tristate logic based SRAM cell

Figure 4.4 shows that the proposed cell is implemented using tristate inverter instead of conventional inverter and its working based on control signals and inputs are shown in Table 4.2. Its behavior makes it suitable for a variety of operations.

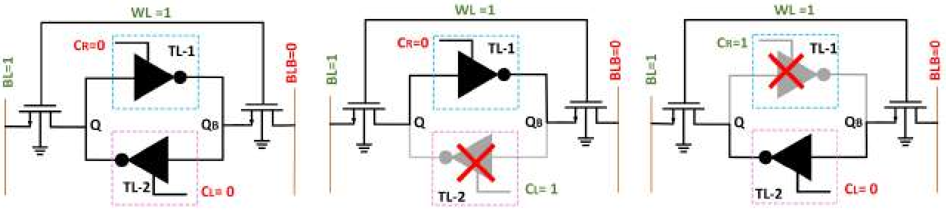


Figure 4.4: Proposed Tristate logic-based SRAM cell behavior as (a) Storage element (b) (TL-1) Inverter TL-2 Open Circuit (c) (TL-1) Open Circuit (TL-2) Inverter.

Table 4.2: Status of the control signals of Tristate Logic (TL) based SRAM Cell

Bitline (BL/BLB)	**Wordline (WL)**	**$\mathrm{C_R}$ (TL-1)**	**$\mathrm{C_L}$ (TL-2)**	**Tristate Logic (Active Path)**
1/0 (↑)	1	1	0	Upper
1/0 (↑)	1	0	1	Lower
1/0 (↑)	1	1	1	Both

(↑) = Precharge, 0 = GND, 1 = $\mathrm{V_{DD}}$

Case I: If word line $WL = 1$ and Bit lines to be precharged to V_{DD}, $BL = 1$ and $BLB = 1$. If $C_R = 0$ and $C_L = 0$, TL-1 and TL-2 are ON, TL-SRAM act as storage elements Figure 4.4a.

Case II: If word line $WL = 1$ and Bit lines to be precharged to V_{DD}. $BL = 1$ and $BLB = 1$. If $C_R = 0$ and $C_L = 1$, TL-2 (lower logic) at high impedance Z and TL-1 (upper logic) behaves as an inverter, as shown in Figure 4.4b.

Case III: If word line $WL = 1$ and Bit lines to be precharged to V_{DD}. $BL = 1$ and $BLB = 1$.If $C_R = 1$ $C_L = 0$, TL-2 (lower logic) behaves as an inverter and TL-1 (upper logic) is at high impedance Z as shown in Figure 4.4c.

4.2.3 Proposed SRAM-Based Ring Oscillators

The Proposed TL-SRAM cell further utilize for CRO implementation, allowing for selective control over which direction the SRAM ring oscillator is active at any given time. We connected five SRAM cells horizontally to form a ring. To complete the loop, the output of the SRAM cell Q_B is connected to the Q of the next cell through five transmission

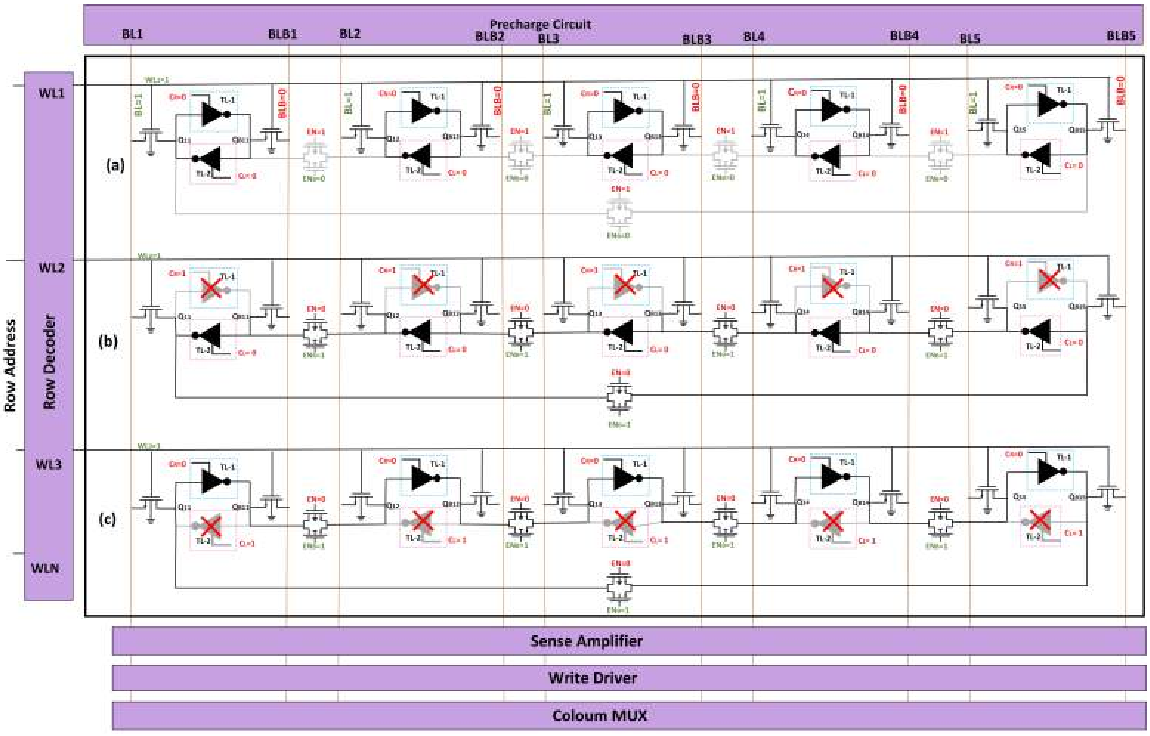


Figure 4.5: Proposed TL-SRAM-Array (a) Behave as 8-bit Storage cells (b) TL-2 Behave as Inverter and responsible for building Leftward RO (c) TL-1 Behave as Inverter and responsible for building Rightward RO.

gates responsible for propagating the outputs with signals from EN and EN_B as shown in Figure 4.5. EN and EN_B are the input and output of inverter.

Storage cell: If word line $WL = 1$ and Bit lines BL_1/BLB_1 to BL_5/BLB_5 to be precharged to V_{DD}. The control signals $C_R = 0$ and $C_L = 0$ corresponding to TL-2 and TL-1 make them behave as an inverter and $EN = 1$ and $EN_B = 0$ corresponding to all transmission gates build high impedance state as shown in Figure 4.5a.

Leftward RO: If word line $WL = 1$ and Bit lines BL_1/BLB_1 to BL_5/BLB_5 to be precharged to V_{DD}. The control signals $C_R = 1$ and $C_L = 0$, TL-1 (upper logic) at high impedance Z and TL-2 (lower logic) behaves as an inverter. $EN = 0$ and $EN_B = 1$ corresponding to all transmission gates.TL-2 is used to generate leftward oscillations. The ring oscillator functions in an anticlockwise direction, as shown Figure 4.5b.

Rightward RO: If word line $WL = 1$ and Bit lines BL_1/BLB_1 to BL_5/BLB_5 to be precharged to V_{DD}. The control signals $C_R = 0$ and $C_L = 1$, TL-2 (lower logic) are at high impedance Z and TL-1 (upper logic) behaves as an inverter.$EN = 0$ and $EN_B = 1$ corresponding to all transmission gates. TL-1 used to generate rightward oscillations. The ring oscillator operates clockwise as shown in Figure 4.5c. The transmission gate controls the direction in which the signal travels through the ring.

To achieve self-sustaining oscillation, maintain a phase shift of 2π with unity gain at the oscillation frequency. The oscillator had N stages, each with a phase shift of $2\pi/N$. DC inversion completes the remaining π phase shift. For a total phase shift of 2π, the oscillating signal goes through each N inverter step twice. A single full cycle takes $2NT_{delay}$. The equation gives the oscillation frequency:

$$f = \frac{1}{2NT_{delay}} \tag{4.3}$$

Where f is the frequency of oscillation, N is the number of stages, and T_{delay} is the propagation delay of each stage. The TL-SRAM-RO frequency is determined by the number of stages in the loop and the delay per stage. A higher total delay in the loop results in a lower frequency, so a larger delay per stage leads to a lower frequency.

4.3 ASIC Implementation and Simulation Results

The Cadence Spectre simulation platform was used for pre- and post-layout simulations, showing comparable results. For reliability testing, we used the Cadence RelXpert design simulator and UMC 40nm manufacturing technology. All simulations were carried out at 1.1V supply voltage and 27°C temperature. Figure 4.6 shows the layout of the TL-based SRAM and the tristate logic-based SRAM-based RO. Figure 4.7a shows the relation between the switching voltage of different inverter topologies with aging, indicating that TL-INV shows better performance than previous works.

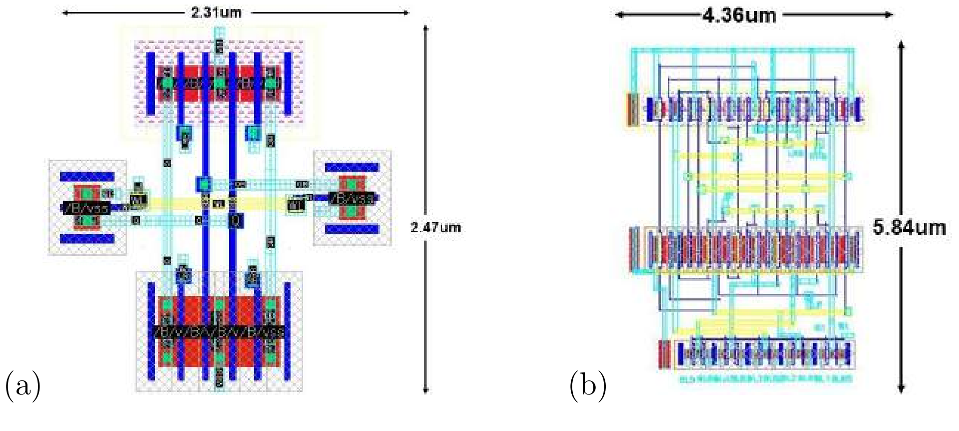


Figure 4.6: Layout of (a) TL-based SRAM cell and (b) TL-based SRAM RO.

4.3.1 SRAM Cell Structure

We have designed and analyzed 6T SRAM and T-SRAM cells at typical process corners with a 1.1V supply voltage and 27 °C. Table 6.2 summarizes our extensive simulations and analysis of the characteristics of SRAM cells.

Stability Analysis

The static noise margin (SNM) of SRAM is critical for evaluating the stability and robustness of memory cells during read, write, and hold operations [71]. Write SNM is critical for guaranteeing that an SRAM cell may flip states consistently during a write operation. When the Write SNM is set too low, the probability of write failure increases because the cell may reject essential state changes. A greater Write SNM indicates improved write resilience, which is critical for memory system dependability.

Table 4.3: Comparison of Parameters for Different SRAM Cell Structures

Parameters	**6T-SRAM**	**TL-SRAM**
Read Power (pW)	7.63	6.8
Write Power (uW)	163	158.7
Area (μm^2)	0.303	6.28
Write Delay (ps)	16.96	12.97
Read Delay (ps)	5.94	4.6
SVNM (mV)	492.04	474.35
SINM (uA)	113.25	101.19

In contrast, read SNM is critical for preserving the integrity of stored data during a read operation. When data is accessed, the access transistors are activated, allowing the external circuitry to perceive the stored information. However, this procedure may disrupt the internal state of the cell, posing a risk of data flips and loss. As a result, understanding and improving write and read SNM is crucial to ensure consistent SRAM performance. A greater read SNM implies that the SRAM cell is more stable during read operations, making it less sensitive to disturbances caused by external sources like voltage fluctuations or noise. In contrast, a smaller read SNM increases the probability of random changes to the cell's content during read operations. Figure 4.7 shows that the read, write, and hold SNM of TL- SRAM is 20.77 %,18.93 %, and 6.25% higher than the conventional 6T SRAM cell. The proposed SRAM cell is utilized for the implementation of a ring oscillator using the SRAM array.

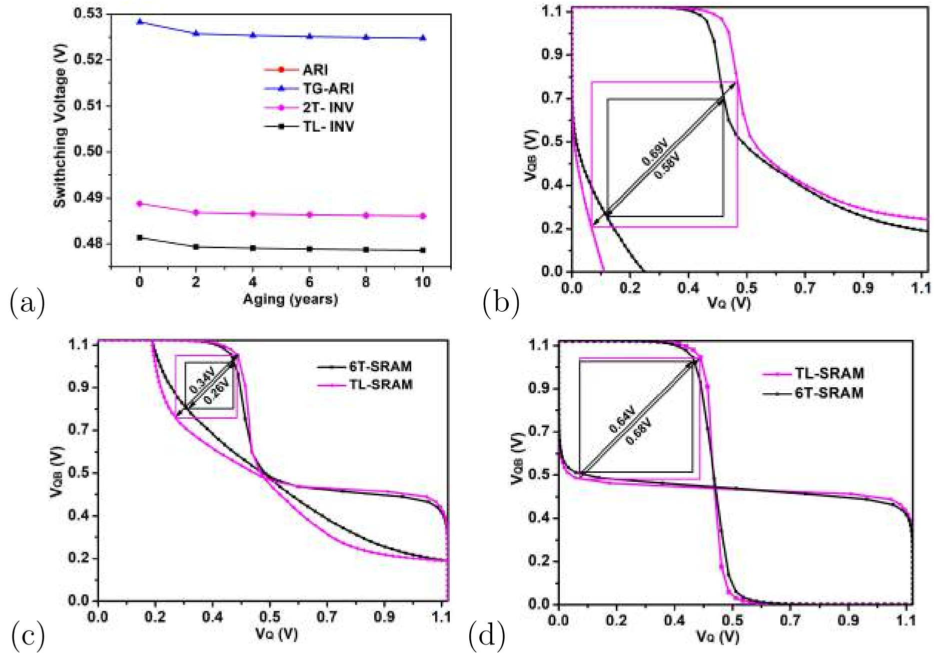


Figure 4.7: Switching voltages vs Aging and SRAM reliability analysis: (a) Switching voltages vs Aging for different inverter topologies, (b) Write SNM, (c) Read SNM, (d) Hold SNM for 6T-SRAM and TL-SRAM.

Power Analysis

We have performed the power dissipation for 6T-SRAM and TL SRAM cells. The read power improves by 10.88%, while the write power increases by 2.61%. TL-SRAM provides a significantly higher power efficiency than 6T-SRAM, particularly for write operations.

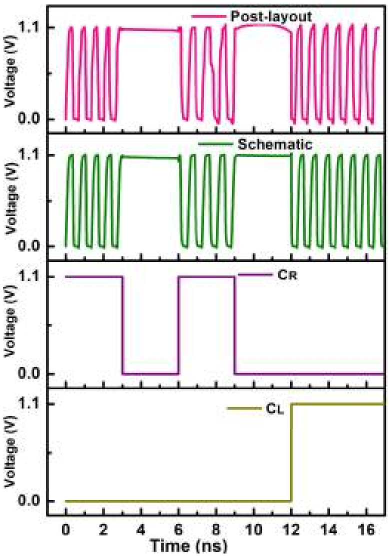


Figure 4.8: Comparison between schematic and post-layout simulations with Control signals C_R and C_L of TL-SRAM-RO .

Delay Analysis

We have calculated the for 6T-SRAM and TL SRAM cell. The lower values of delay indicate faster performance. write delay and read delay of TL-SRAM are 23.5% and 22.5% lower than conventional 6T-SRAM cells. Further, we measure that 6T-SRAM takes up less cell area compared to TL-SRAM.

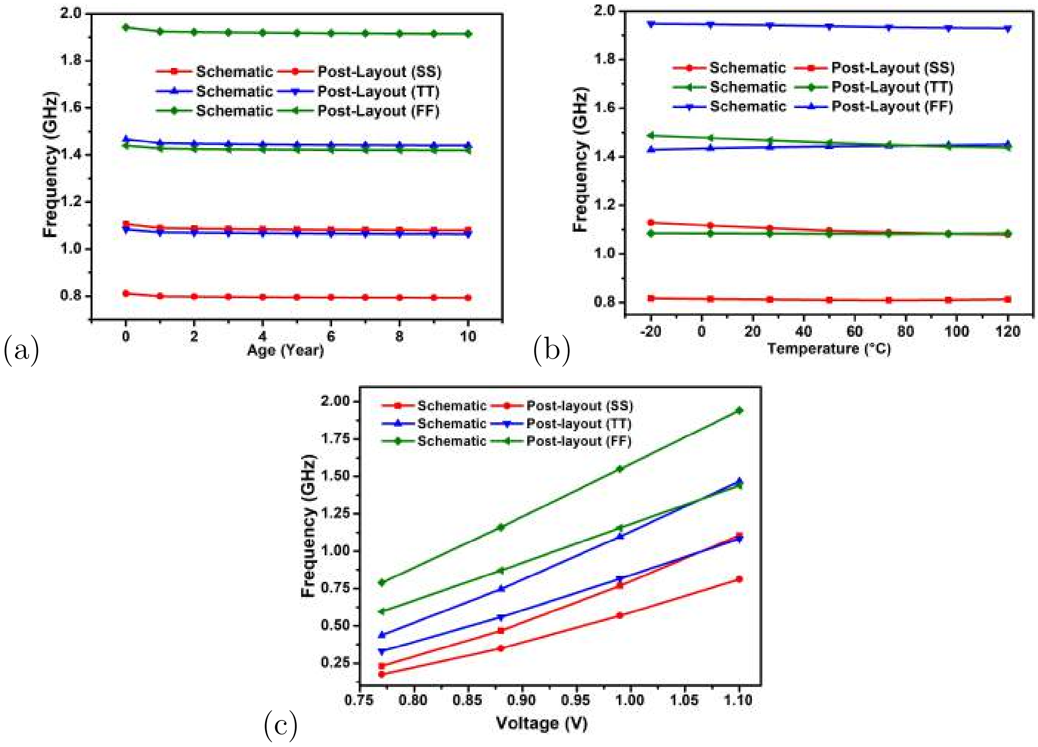


Figure 4.9: Comparison of frequency variation under different operating conditions between schematic and post-layout simulations.

4.3.2 SRAM-based Ring Oscillator

Figure 4.8 shows the control signal, and correspondingly, the TL-SRAM-RO output is examined in both the schematic and post-layout stages. The control signals in the post-layout cause the TL-SRAM-RO to oscillate in both directions. The TL-SRAM-RO duration is significantly longer in post-layout than the schematic response due to parasitic capacitance and resistances produced by the interconnects, buffers, load MOS capacitors, and transistors. The TL-SRAM-RO in the schematic completes two cycles for the same control signals, however, the post-layout only completes about 1.5 cycles. Figure 4.9a show the frequency variation with aging at different corners and we have found that frequency increases 33% from SS(slow-slow) corner to TT (typical-typical) and 32.4% TT to FF (fast-fast) corner and frequency decreases 1.85% from zero years to ten years at typical corner and frequency decreases 35% between pre and post layout results. Figure 4.9b shows the frequency variation with the temperature at different corners and we have found that frequency increases 32. 7% from the SS corner to TT and 30. 9% TT to the FF corner and frequency decreases 0.1% from zero year to ten years at TT and frequency decreases 37. 2% between pre- and post-layout results. Figure 4.9c show that the frequency variation with supply voltage at TT from pre-layout to post-layout frequency decreases to 26% and the frequency increases from TT to the FF corner.

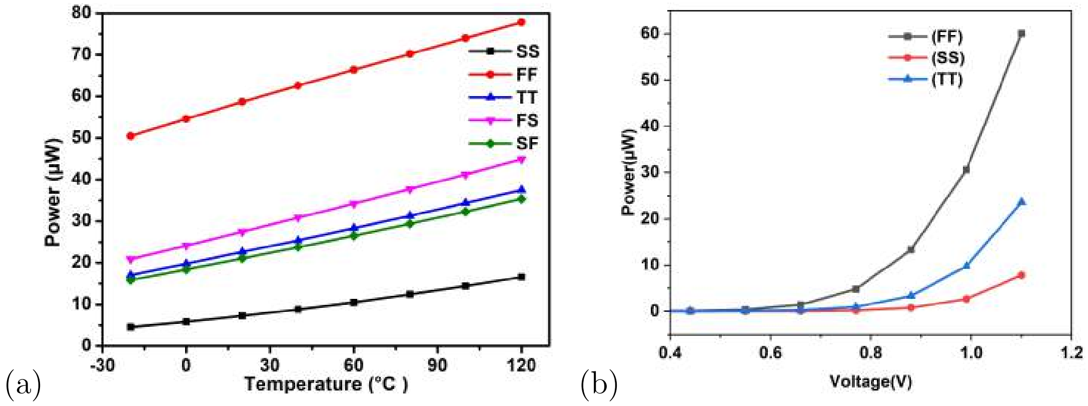


Figure 4.10: Power consumption in TL-SRAM RO (a) temperature at different process corners.(b) supply voltage.

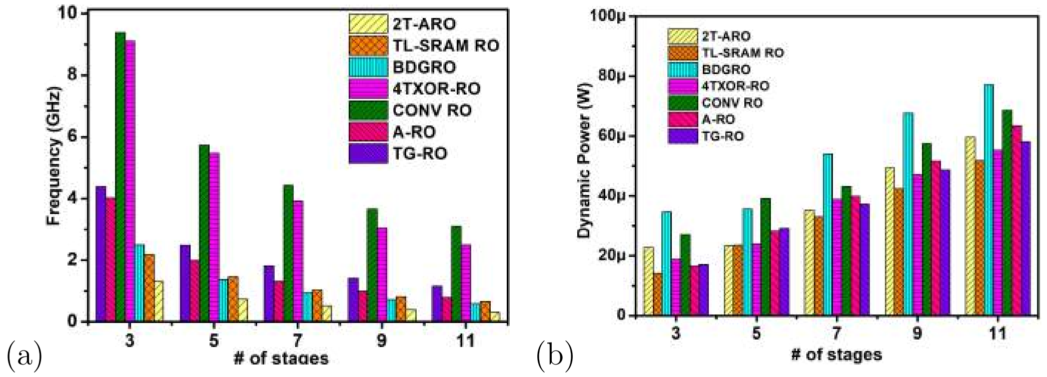


Figure 4.11: Comparison (a) oscillation frequency at various RO with respect to the number of inverter stages (b) dynamic power at various RO with respect to the number of inverter stages.

Figure 4.10a shows increases in power consumption for temperature at different corners and Figure 4.10b shows increases in power consumption as supply voltage increases from 0.6V to 1.1V. Figure 4.11 shows that when the number of RO stages increases, the frequency of 2T-ARO decreases more quickly than that of TL-SRAM RO. Figure 4.11 shows that the dynamic power of 2T-ARO increases rapidly as the number of stages, but at the third stage, the dynamic power consumed by TL-SRAM RO is 19.76% less than that of 2T-ARO.

Table 4.4: Performance Analysis of Various RO Structures

Parameters	**ConvRO**	**BDGRO [70]**	**A-RO [65]**	**4TXOR-RO [67]**	**TG-RO [63]**	**Proposed RO**
Technology (nm)	40	130	40	40	40	40
Supply Voltage (V)	1.1±10%	1.2	1.1±10%	1.1±10%	1.1	1.1
Area (μm^2)	29.33	26.9	59.67	53.84	-	25.4
Frequency (MHz)	1810	284	402.9	669.3	2490	1084
Mode of Operation	Unidirectional	Bidirectional	Unidirectional	Unidirectional	Unidirectional	Bidirectional
Power (μW)	40	27.9	27.1	32	37	24.1

Table 4.4 shows the power consumption and area utilization are low with the bidirectional behavior of the proposed TL-SRAM-RO with 1.08 GHz frequency compared with the previous work.

4.4 Summary

This chapter describes an SRAM cell employing tristate logic, which permits the building of an SRAM-based ring oscillator architecture that exhibits bidirectional behavior and is based on a projected 10T SRAM cell. The architecture successfully makes use of the 10T configuration for greater control and stability to produce dependable oscillation with increased power efficiency. With an oscillation frequency of 1084 MHz and a low power consumption of 21.4 µW compared with state of art, the design is suitable for low-power and high-speed applications. Furthermore, its small 25.4 µm² area footprint emphasizes its potential for integration in systems with limited space, especially in contemporary SoC and low-power embedded designs.

Chapter 5

CIM-Enabled MBRO-PUF: Integrating Multistage RO and SRAM

In chapter 4, the BRO-PUF architecture was discussed as a method to enhance CRP quality. In addition, configurable SRAM-based ring oscillators using gated logic and tristate-inverter-based approaches were presented to reduce latency and minimize area overhead by integrating the oscillator within the memory array. In this chapter, a multi-stage bidirectional ring oscillator based on SRAM is proposed and further utilized for the implementation of RO PUF.

In the implementation of the MBRO architecture, the proposed TL SRAM cell presented in the previous chapter is utilized as the fundamental building block. For the realization of multi-stage operation in the ring oscillator, transmission gates are employed as switching elements to establish programmable connectivity between adjacent cells within the array. Three independent challenge parameters are incorporated in the design:

- Direction control, implemented through the control inputs of the tristate inverters.
- Stage control, achieved by enabling or disabling selected transmission gates to vary the effective number of RO stages.
- RO selection through multiplexing.

Based on these three challenge dimensions, a large number of ROs are generated, and a specific RO pair is selected through a multiplexer-based RO PUF architecture. This enables dynamic selection among n available ROs, thereby significantly increasing the

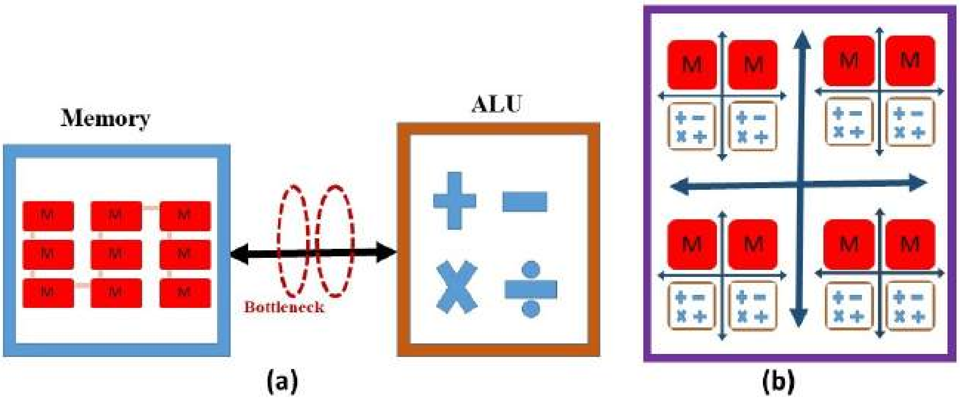


Figure 5.1: Comparison between (a) Traditional von Neumann architecture and (b) CIM architecture [72].

number of valid CRPs. Such configurability enhances resistance against modeling and side-channel attacks. Compared to conventional RO PUF designs, the proposed architecture offers a substantially larger CRP space due to its multi-dimensional reconfigurability. By combining:

The proposed design can be characterized as a multi-stage, multi-challenge, and multi-directional RO PUF architecture. This structure improves unpredictability, security, and robustness against adversarial attempts to clone or model the PUF behavior. Further, simulations of the proposed MBRO architecture are performed across different process corners to evaluate frequency variation with respect to aging, temperature, and supply voltage. Based on these variations, the uniqueness metric of the PUF implementation is extracted and analyzed to assess inter-chip variation and reliability under practical operating conditions.

5.1 State-of-the-art

Previous work shows the use of tunable ring oscillators to characterize the stability of dynamic SRAM cells during read and write operations, allowing quick performance measurements without altering the SRAM array[60]. Existing work on time integrators addresses challenges such as nonlinearity, skew, supply noise, device noise, and metastability, but often lacks the comprehensive integration and robustness demonstrated by the bidirectional gated ring oscillator approach [70] . Prior work on RO PUFs has explored various architectures, with recent designs like the BRO PUF using gated logic to enhance uniqueness and significantly increase the number of challenge-response pairs [40]. A 4T XOR-based RO PUF achieved ultra-low power, aging resilience, high CRP, and stable performance, addressing the limitations of conventional RO PUFs for IoT security [45]. An SRAM-based architecture integrates TRNG (True Random Number Generator) and multi-bit PUF generation using bitline discharge dynamics, offering low-cost, energy-efficient, and attack-resilient entropy extraction within standard memory arrays[70]. Several authors have proposed SRAM architectures or cell designs to enable SRAM-based CIM [73]. The motivation behind this research lies in overcoming the limitations of traditional 6T-SRAM cells, which restrict the implementation of ring oscillators within memory architectures. Previous works demonstrated RO integration using multiple 6T-SRAM cells [60], however, they lack compactness and directional control.

Characterization of SRAM stability using tunable ring oscillators: tunable ring oscillators to characterize dynamic cell stability during write and read operations without the need to modify the SRAM array [74]. Time-domain CIM core that implement 8T SRAM cell's XNOR-and-accumulate (XAC) XNOR network. This method creates periodic waves using an inverter-based ring oscillator, the period of which is the accumulation result of the input XNOR values[75]. Unlike conventional architectures as shown in Figure 5.1(a) which shuttle data between separate processing and storage units, CIM shown in Figure 5.1(b) performs computations directly where the data reside, offering two key advantages: a substantial reduction in intermediate data transfers and improved parallel computing efficiency with respect to both energy consumption and area overhead [69]. CIM has been widely used to offer energy-efficient computation in approaches for machine learning, sparse distributed memory architectures and IoT applications [76],[77].

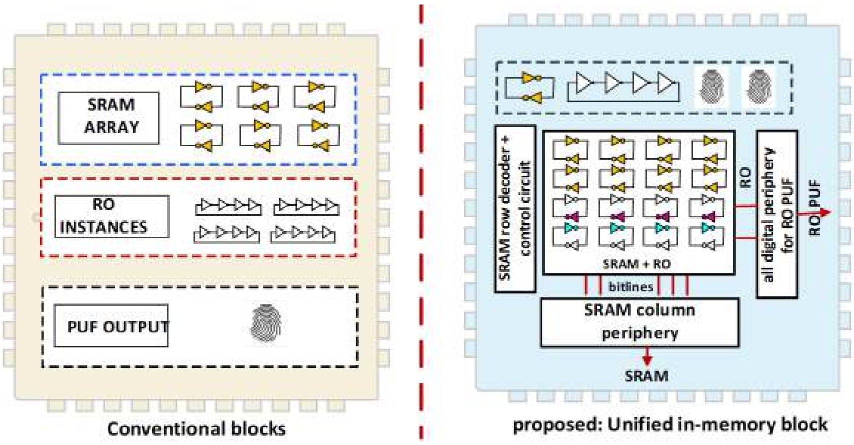


Figure 5.2: Functional overview of the proposed computing-in-memory-based PUF design [72].

To address such constraints, the proposed design combines ring oscillators, memory elements, and security primitives into CIM framework as shown in Figure 5.2. Data travel is greatly reduced by this proposed design, allowing for effective in-memory processing. Consequently, the system shows significant gains in speed, area efficiency, latency, and delay, making it ideal for real-time secure hardware applications with limited resources. The design of memory-integrated ring oscillator structures for hardware security applications takes advantage of both the frequency discrimination properties of ROs and the intrinsic randomness of SRAM. This synergy allows for the development of higher-quality PUF responses, resulting in a performance matrix that is more unique, reliable, and robust. The chapter highlights primary contributions as follows:

- **Novel approach for a reconfigurable SRAM-based ring oscillator through memory:** A novel methodology is presented to transform a SRAM cell array into a functional ring oscillator. This enables multistage and bidirectional oscillation, laying the foundation for in-memory physical unclonable function generation within the same hardware substrate.

- **Design of a configurable RO PUF:** The proposed architecture introduces a highly configurable PUF based on ring oscillators that improves both security and adaptability. The configuration capability allows for dynamic tuning suitable for diverse hardware security applications.

- **Comprehensive simulation and reliability evaluation:** Extensive simulation results demonstrate the robustness of the proposed PUF under various operating conditions, including supply voltage variations, temperature changes, and aging effects. Key performance metrics such as uniqueness, reliability, and BER are thoroughly evaluated.

- **Overhead reduction through in-memory integration:** By integrating ring oscillators and PUF generation mechanisms within the memory array, the design significantly reduces hardware overhead. This multifunctional approach improves system efficiency by optimizing area usage, enhancing scalability, and minimizing data movement.

5.2 Multistage bidirectional SRAM-based Ring Oscillator

The implementation of a ring oscillator with bidirectional operation using a conventional SRAM cell is extremely challenging and, in most cases not feasible. This limitation arises because conventional 6T SRAM cells are optimized purely for data storage and lack the configurability required to control oscillation paths. In contrast, our configurable SRAM cell overcomes this limitation by enabling bidirectional and multistage oscillation within the same memory structure.

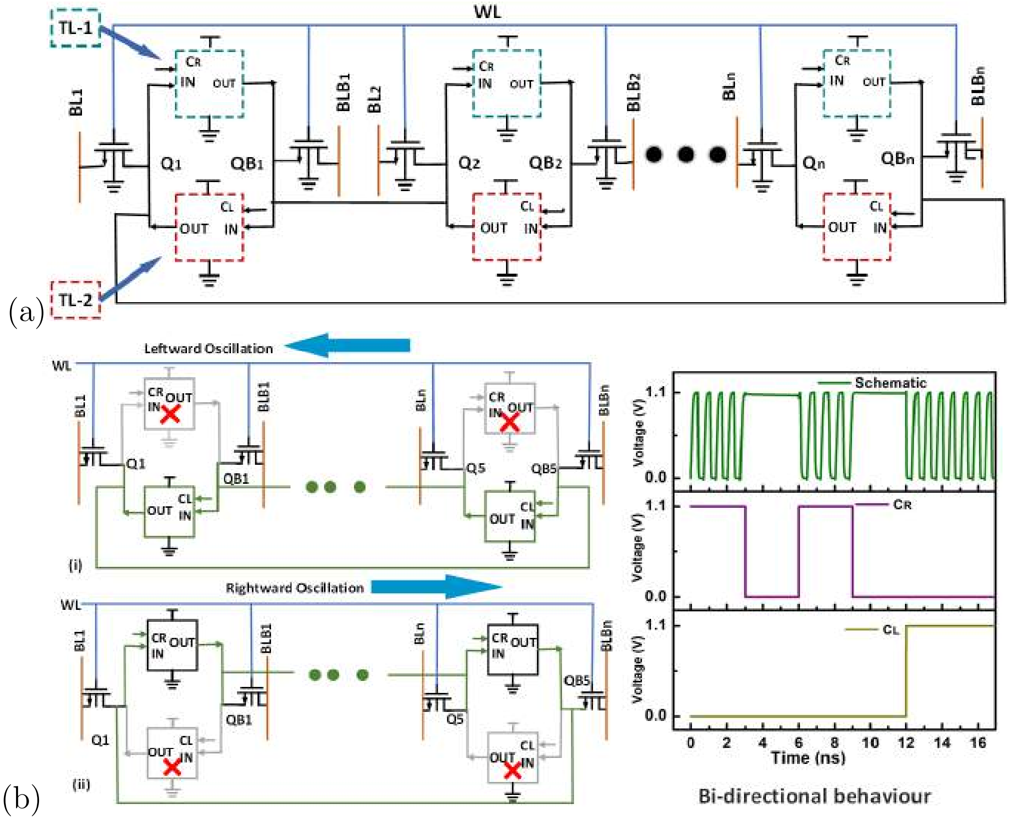


Figure 5.3: (a) n-stage ring oscillator structural representation (b) Behavioral representation (i) Leftward oscillation (ii) Rightward oscillation[72].

Figure 5.3(a) illustrates the structure of the proposed n-stage ring oscillator. The activation of the RO is controlled through the wordline (WL), while the bitlines are precharged to V_{DD} to initialize the circuit. Figure 5.3(b) demonstrates the bidirectional operation of the ring oscillator, where leftward and rightward oscillations are selectively enabled. In each SRAM cell, only one inverter participates in the oscillation loop at a time, while the complementary inverter is placed in the high-impedance state. This arrangement ensures controlled signal propagation and enables dynamic reconfiguration of the oscillator direc-

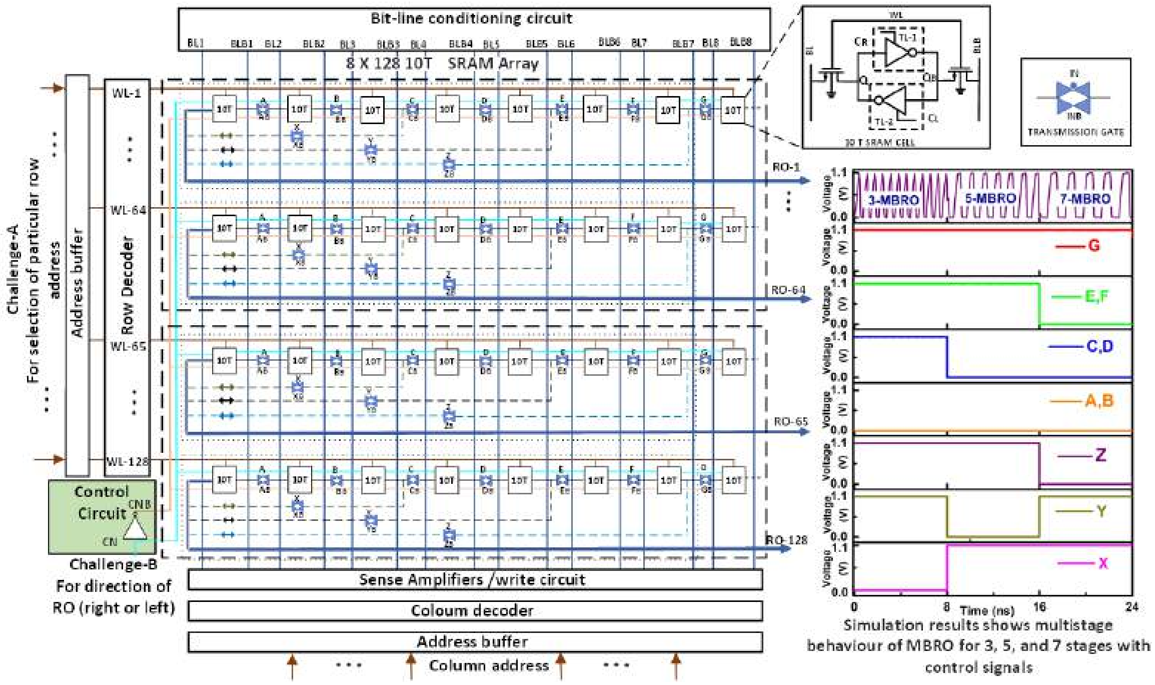

Bit-line conditioning circuit
BL1 BLB1 BL2 BLB2 BL3 BLB3 BL4 BLB4 BL5 BLB5 BL6 BLB6 BL7 BLB7 BL8 BLB8
8 X 128 10T SRAM Array
WL-1
WL-64
WL-65
WL-128
Challenge-A
For selection of particular row address
Address buffer
Row Decoder
Control Circuit
CNB
CN
Challenge-B
For direction of RO (right or left)
10T
RO-1
RO-64
RO-65
RO-128
Sense Amplifiers /write circuit
Coloum decoder
Address buffer
Column address
WL
CR
TL-1
TL-2
CL
Q
QB
BL
BLB
10 T SRAM CELL
IN
INB
TRANSMISSION GATE
3-MBRO
5-MBRO
7-MBRO
G
E,F
C,D
A,B
Z
Y
X
Voltage (V)
1.1
0.0
0
8
16
24
Time (ns)
Simulation results shows multistage behaviour of MBRO for 3, 5, and 7 stages with control signals

Figure 5.4: Proposed 8 x 128-bit SRAM architecture is utilized for the implementation of the multistage bidirectional ring oscillator along with transient behavior in multistage mode [72].

tion. The proposed architecture for the SRAM array consists of an 8 X 128 10T SRAM cell, ten transmission gates used to provide connectivity between the cell, and a control circuit made up of an inverter with input CN and the generated output is CNB both behave as the control signal to the 10T SRAM cell determines the direction of oscillation this control signal is connected inside the SRAM cell with C_R and C_L. A MBRO is designed to produce periodic oscillations, which can be used for the application of PUFs. Depending on the control signals CN and CNB, the oscillator can be configured to oscillate in a clockwise (rightward) or counterclockwise (leftward) direction or as storage cell and behave as challenge-B for the proposed PUF as shown in Figure 5.4. Table 5.1 shows the operating condition for the MBRO. During the read operation, the SRAM cell array

Table 5.1: Status of the control signals to form Ring Oscillator Bitlines $BL/BL_B = 1/0$ (↑) and Wordline $WL = 1$

C$_R$/CB$_R$ (TL-1)	**C$_L$/CB$_L$ (TL-2)**	**A/A$_B$, B/B$_B$ (TG-1),(TG-2)**	**C/C$_B$, D/D$_B$ (TG-3),(TG-4)**	**E/E$_B$, F/F$_B$ (TG-5),(TG-6)**	**W/W$_B$ (TG-7)**	**X/X$_B$ (TG-8)**	**Y/Y$_B$ (TG-9)**	**Behavior**
0/1	1/0	0/1	1/0	1/0	0/1	1/0	1/0	**3 stage RO(L)**
1/0	0/1	0/1	1/0	1/0	0/1	1/0	1/0	**3 stage RO(R)**
0/1	1/0	0/1	0/1	1/0	1/0	0/1	1/0	**5 stage RO(L)**
1/0	0/1	0/1	0/1	1/0	1/0	0/1	1/0	**5 stage RO(R)**
0/1	1/0	0/1	0/1	0/1	1/0	1/0	0/1	**7 stage RO(L)**
1/0	0/1	0/1	0/1	0/1	1/0	1/0	0/1	**7 stage RO(R)**
0/1	0/1	1/0	1/0	1/0	1/0	1/0	1/0	**Memory Array**

(↑) = Precharge, (L) = Left, (R) = Right can behave as a multistage ring oscillator, e.g., five SRAM cells connected horizontally. QB the output of the SRAM cell is connected to the Q of the next cell to form the loop. wordline WL can be used to enable RO and bit lines BL/BLB are precharged with V_{DD} and GND value. The TL-SRAM can isolate parts of the oscillator based on the control input, ensuring that only the required elements are active.

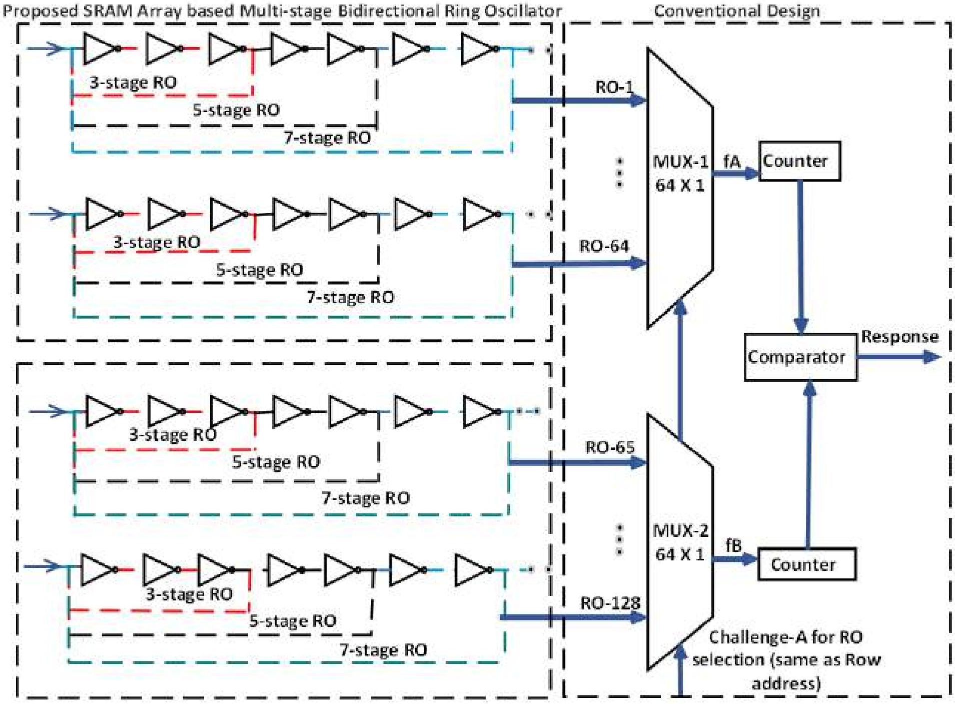


Figure 5.5: Proposed MBRO PUF architecture [72].

5.3 Proposed MBRO PUF Architecture

We have implemented the proposed PUF by replacing the conventional RO with the proposed MBRO architecture. The proposed PUF design is shown in Figure 5.5. We have designed 256 MBRO instances, and we have enabled 256 wordlines WL and precharged BL_1/ BLB_1 to BL_5/ BLB_5 with V_{DD}.Two MBRO are selected at a time through challenge-A, available at both the MUX, and same challenge-A is the row address for MBRO selection in SRAM array. To select MBRO instances, two (64 X 1) MUX can be used. MBRO_1 to MBRO_{64} instances are input to MUX-1 and MBRO_{65} to MBRO_{128} instances are input to MUX-2 then a further single output is generated from MUX, which is fed into the counters. The counter output is further given to the comparator that compares and generates the final response. By using this multi-challenge topology and choosing the control signal values from the tristate logic present in the SRAM cell, we can lessen side-

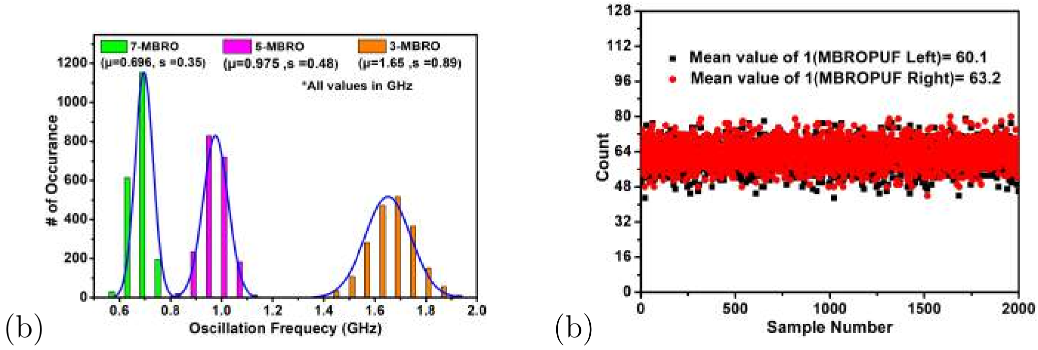


Figure 5.6: (a) Monte Carlo analysis and (b) ASIC-level implementation insights for the proposed MBRO PUF [72].

Table 5.2: Resource utilization comparison between combined SRAM–RO Design and the proposed SRAM-Based MBRO design.

Designs	Transistor Utilization	
	Conventional Design	Proposed Design
8-bit SRAM Array	8*6 = 48	8*10 + two extra transistor = 82
3 stage RO *2	(2 INV + 1 NAND) = 16	(3 SRAM + 3 Transmission Gate) = 36
5 stage RO *2	(4 INV + 1 NAND) = 24	(5 SRAM + 5 Transmission Gate) = 60
7 stage RO *2	(6 INV + 1 NAND) = 32	(7 SRAM + 7 Transmission Gate) = 84
Total Transistor Count*	**120**	**(8 SRAM + 10 Transmission Gate) = 100**
64*8-bit SRAM Array	64*8*6 = 3072	(64*8*10 = 5120) + (Control circuit) 2 = 5122
64 (3 stage RO)	512*2 RO = 1024	64 (3 stage MBRO) = 2304
64 (5 stage RO)	768*2 RO = 1536	64 (5 stage MBRO) = 3840
64 (7 stage RO)	1024*2 RO = 2048	64 (7 stage MBRO) = 5376
64 (3,5,7 stage RO) + 64*8-bit SRAM Array	**4608 + 3072 = 7680**	**5632 + 768 = 6400**

*RO = Ring Oscillator, MBRO = Memory-Based Ring Oscillator

channel attacks on the devices. The CRPs of the PUF directly change with the direction of SRAM RO is altered. Table 5.2 shows that the transistor count decreases compared to the conventional design. Proposed design uses approximately 16.67 % fewer transistors than the conventional design. To analyze the effect of process variation, we have performed the 100 rounds of Monte carlo simulation for oscillation frequency at different stage as shown in Figure 5.6a. We have taken 2000 samples of the architecture, and corresponding to individual samples, we have analyzed the ones and zeros count. Figure 5.6b shows the allocation of zero and one. It is observed that the count of ones and zeros are nearly equal for the MBRO PUF and are centered near the mean value of 60.1 for MBRO PUF left and 63.2 for MBRO PUF right and has symmetric distributions for both ones and zeros.

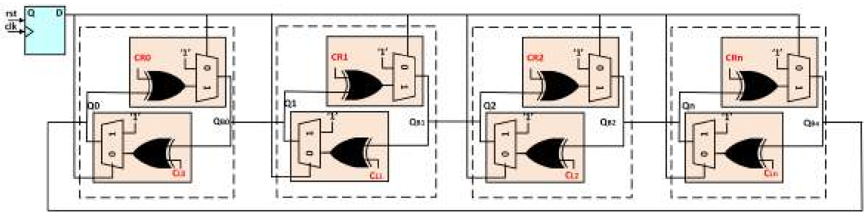


Figure 5.7: Equivalent circuit of proposed RO [72].

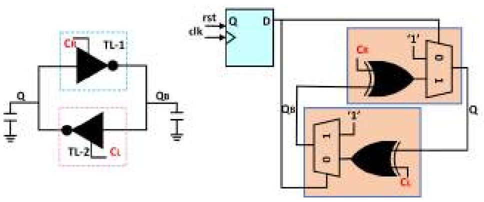


Figure 5.8: Logical and conceptual design of bitcell [72].

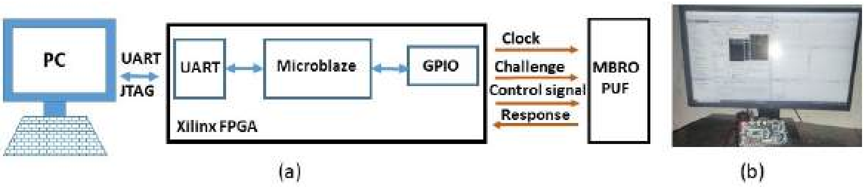


Figure 5.9: Functional block design [72].

Table 5.3: Resource utilization comparison of various RO-PUF designs

PUF Design	Resource Utilization					
	LUT		FF		IO	
	#	%	#	%	#	%
Conventional RO-PUF [29]	2500	12.02	64	0.15	41	38.67
CRO-PUF [52]	4557	21.90	64	0.15	41	38.67
RRO-PUF [42]	4987	23.97	64	0.15	41	38.67
Proposed MBRO PUF	**4054**	**19.49**	**67**	**0.16**	**17**	**16.04**

5.4 Functional Verification Using FPGA

To validate the functionality of the proposed MBRO PUF we have implemented the 256 instances of the logically equivalent circuit as shown in Figure 5.7. A memory-based PUF design that uses a compact cell, where the single-bit output becomes known only after it stabilizes following a reset. For example, in Figure 5.8, If both inputs C_R and C_L are initially enabled, the capacitors at Q and Q_B will be charged. At time $t = 0$, the switches are opened, and the circuit settles into a stable state determined by the inverter delay, interconnect delays, and the switching threshold of the logic. If the upper route has the shorter delay, it will stay in logic 1 and drive Q_B to logic 0. Conversely, if the lower route is faster, it will hold logic 1 and cause Q to go to logic 0. Q and Q_B will always have opposite values, but which value holds is determined by the physical characteristics of the hardware. Here, we have considered the XOR logic to work with one inverter at a time to implement ring oscillator. Xilinx Vivado tool is used for the implementation on the three Basys3 FPGA (Field Programmable Gate Array) boards. A Microblaze soft processor

Table 5.4: Uniqueness, uniformity, and bit-aliasing comparison of various RO-PUF designs

Type of RO-PUF	Uniqueness	Uniformity	Bit-Aliasing
Conventional RO-PUF [29]	0.464	0.478	0.501
CRO-PUF [52]	0.472	0.480	0.478
RRO-PUF [42]	0.498	0.491	0.488
Proposed 3-MBRO PUF	**0.496**	**0.483**	**0.513**
Proposed 5-MBRO PUF	**0.494**	**0.480**	**0.492**
Proposed 7-MBRO PUF	**0.480**	**0.477**	**0.486**

core has been integrated with the architectural design of PUF to facilitate the writing and reading of challenge-response pairs. The MicroBlaze application involved the utilization of C programming within the ARM SDK (Software Development Kit) environment, as shown in Figure 5.9. The design and implementation were based on Verilog Hardware Description Language for FPGA. TCL scripts were used in vivado and the plan is to implement placement constraints as part of the methodology [78]. The utilization of the 7 stage MBRO PUF resources and the comparison with the other considered is shown in Table 5.3. From Table 5.4, We observed that the proposed MBRO PUF architectures achieve competitive performance compared to conventional RO PUF variants. The 3 stage MBRO PUF shows the highest uniqueness, close to the ideal 0.5, though at the cost of slightly higher bit-aliasing. The 5 stage MBRO PUF achieves balanced performance in all three metrics, which is better than conventional and CRO-PUF designs. Meanwhile, the 7 stage MBRO PUF offers the lowest bit-aliasing , enhancing stability, though with a slight reduction in uniqueness. In general, the proposed designs demonstrate improved trade-offs between uniqueness, uniformity, and bit-aliasing.

5.5 Performance Analysis

Simulations were performed using the Cadence Spectre simulation platform, while reliability analysis was performed with the Cadence RelXpert design simulator, based on the UMC 40nm process technology. Unless otherwise specified, all simulations assumed a supply voltage of 1.1V and an operating temperature of 27°C. We have implemented the layout as shown in Figure 5.10 that show the 64 X 128 bit SRAM cell array, and we use an 8 X 128 array to build RO PUF.

Table 5.5: Performance Analysis of Various RO Structures [72].

Parameter	**Conv-RO**	**E-SRAM RO** [40]	**BDGRO** [41]	**A-RO** [65]	**4T XOR-RO** [45]	**TG-RO** [79]	**MBRO** **Proposed (3,5,7-stage)**
Technology (nm)	40	55	130	40	40	40	40
Supply Voltage (V)	1.1±10%	1.0	1.2	1.1±10%	1.1±10%	1.1	1.1
Area (μm^2)	29.33	38.5	26.9	59.67	53.84	-	89.4
Transistor count (7 stage)	14	84	84	28	32	40	84 (Multistage)
Frequency (MHz)	1810	14.5	284	402.9	669.3	2490	1530, 942.9, 652.5
Mode of operation	Unidirectional	Unidirectional	Bidirectional	Unidirectional	Unidirectional	Unidirectional	Multi-stage / Bidirectional
Power (μW)	30	-	27.9	27.1	32	37	32

Table 5.6: Inter-chip Hamming Distance percentage comparison at different temperature.

Operating Condition	**3-stage PUF**	**5-stage PUF**	**7-stage PUF**
25°C	49.6	49.4	48.0
50°C	48.0	49.1	46.6
75°C	47.1	46.2	45.0

5.5.1 Multistage-Bidirectional Ring Oscillator

Figure 5.5 shows the control signal and, correspondingly, the response of the proposed MBRO in stages 3, 5, and 7. The control signal with MBRO oscillates in both directions. The complexity of RO-based PUF increases as the number of stages, or the number of linked ROs in the ring arrangement, grows. As complexity increases, the PUF produces more unique and trustworthy replies. However, increasing the number of stages beyond a certain point can result in performance saturation, when the number of RO stages increases, more inverters and interconnects are added, resulting in a longer propagation delay and parasitic capacitance. These factors cause nonlinearity in the delay and lower the oscillation frequency. Beyond a certain stage count, the parasitic impact becomes

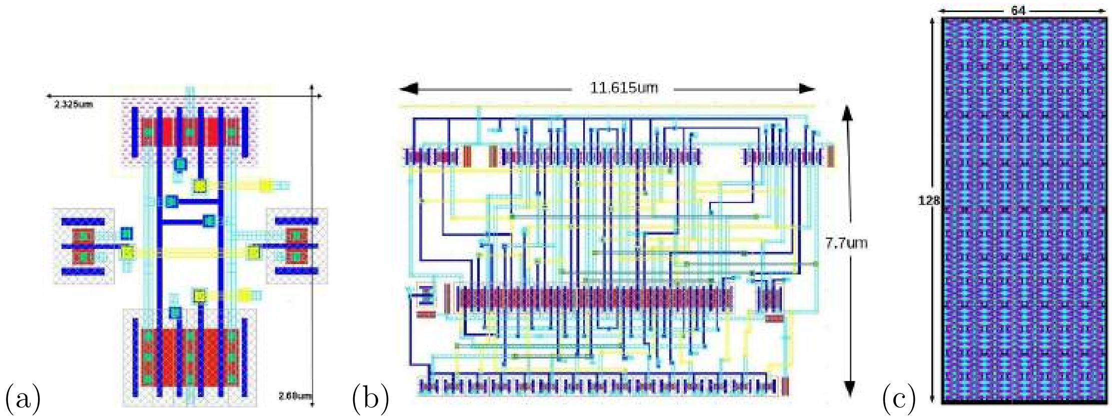
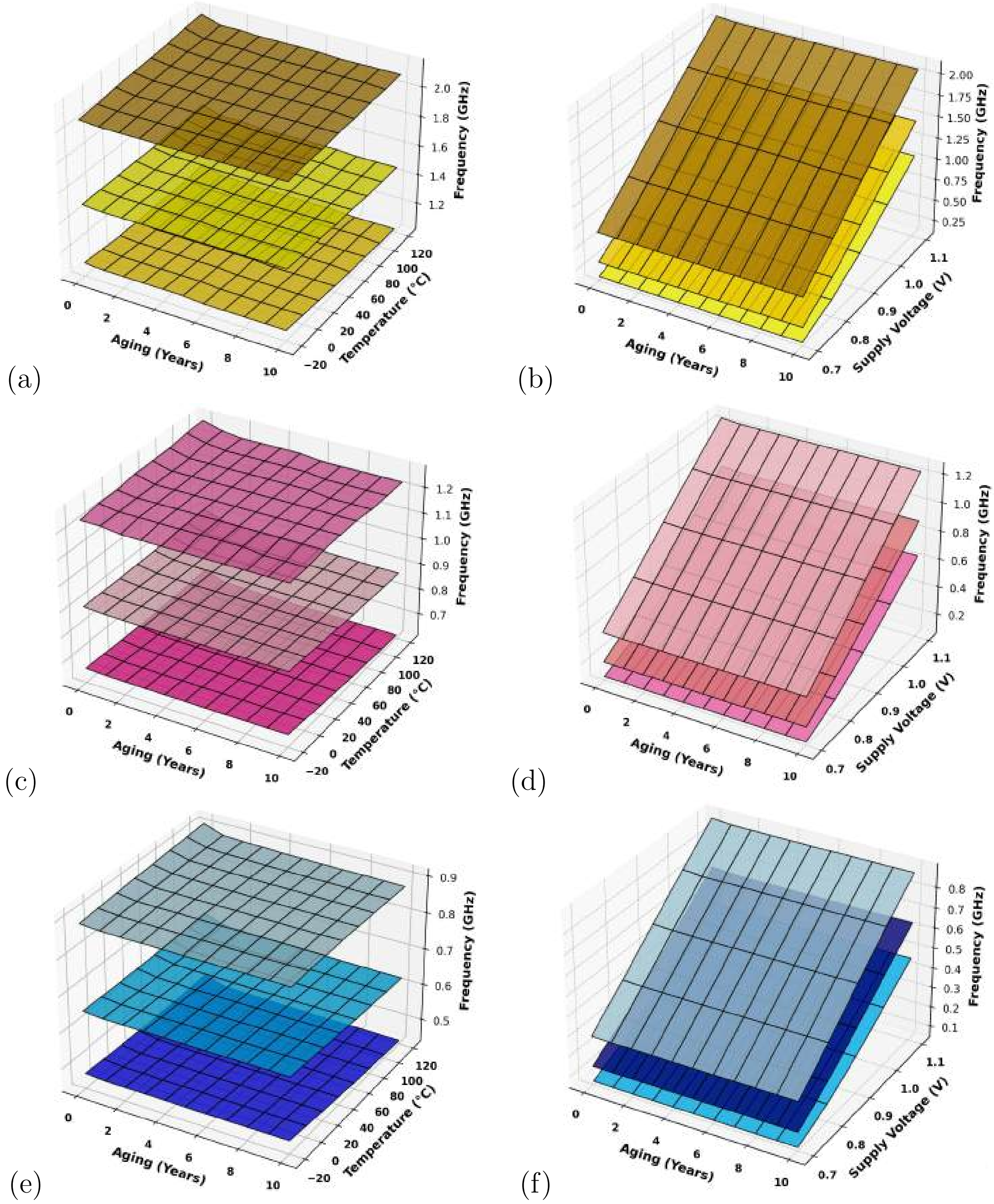


Figure 5.10: Layout of (a) a tristate inverter-based SRAM cell, (b) MBRO, and (c) a 64 X 128 SRAM array [72].



(a) (b)

(c) (d)

(e) (f)

Figure 5.11: Frequency variation with respect to aging and temperature for (a) 3-stage MBRO, (c) 5-stage MBRO (e) 7-stage MBRO. frequency variation under varying temperature and supply voltage (V_{DD}) conditions (b) 3-stage MBRO (d), 5-stage MBRO (f) 7-stage MBRO under different Process the upper layer represents the fast–fast (FF) corner, the middle layer represents the typical–typical (TT) corner, and the lower layer represents the slow–slow (SS) corner [72].

dominant, leading to performance saturation as further stage additions yield minimal improvement in frequency response and affects its latency, power consumption, and entropy quality. The oscillation frequency is inversely proportional to the number of stages, with shorter configurations (e.g., 3-stage) generating higher frequencies and longer ones (e.g., 7-stage) producing lower frequencies due to increasing propagation delay in the feedback loop. As the number of stages increases, additional delay routes are included, which not only extend the overall delay but also improve sensitivity to process variations by enhancing the entropy of the generated response. Furthermore, considering reliability in terms of aging, temperature, and supply voltage, Figure 5.11 (a), (c), and (e) shows the impact on frequency on aging and temperature for 3, 5 and 7-stage MBRO. It is observed from the result that 3-stage MBRO have largest variation between process corners and 7-stage MBRO has the lowest, and 5 stage MBRO lies between the two. Figure 5.11 (b), (d), and (f) highlights the impact on frequency over aging and supply voltage variation for 3, 5 and 7-stage MBRO. It is also observed that 3-stage MBRO have largest variation from 250 MHz to 2.1 GHz between process corners and 7-stage MBRO have lowest from 250 MHz to 870 MHz and 5-stage MBRO lies between the two ranging from 250 MHz to 1.24 GHz. The frequency variation of 7-stage < 5-stage < 3-stage MBRO is observed. Further based on the performance of MBRO, can be utilized for the implementation of ring oscillator based PUF. The power dissipation of the MBRO depends on the transistor sizing and their biasing conditions. The 7-stage > 5-stage > 3-stage MBRO power consumption. While operating it is found that leftward and rightward generate different delays. We observed that the delay of 3-stage < 5-stage < 7-stage MBRO and the delay of the rightward is lower than the leftward for all the stages. Similarly, the frequency of 3-stage > 5-stage > 7-stage MBRO. Based on delay and power consumption performance of 3-stage BRO is better than 5 and 7-stage MBRO PUF. We have compared the proposed MBRO with previous work as mentioned in Table 5.5. A comparison of 3-stage, 5-stage, and 7-stage BRO PUFs shows that performance saturation occurs after a particular stage count. The study recommends selecting the best configuration based on priorities: a 7-stage PUF for high security and power, a 5-stage PUF for balance, and a 3-stage PUF for reduced power usage. In light of the comparison and design, MBRO may be a viable option for PUF implementation.

5.5.2 Performance as a MBRO PUF

The capability of MBRO PUFs is influenced by the quality of the RO stages, not numbers [45]. The trade-off between these two aspects is determined by the number of stages and the quality of the oscillator design [32],[80]. Stages in the oscillator circuit affect the reliability of the PUF. Every application has a power budget that cannot be compromised, hence a PUF must have low power consumption in order to be used in any resource-

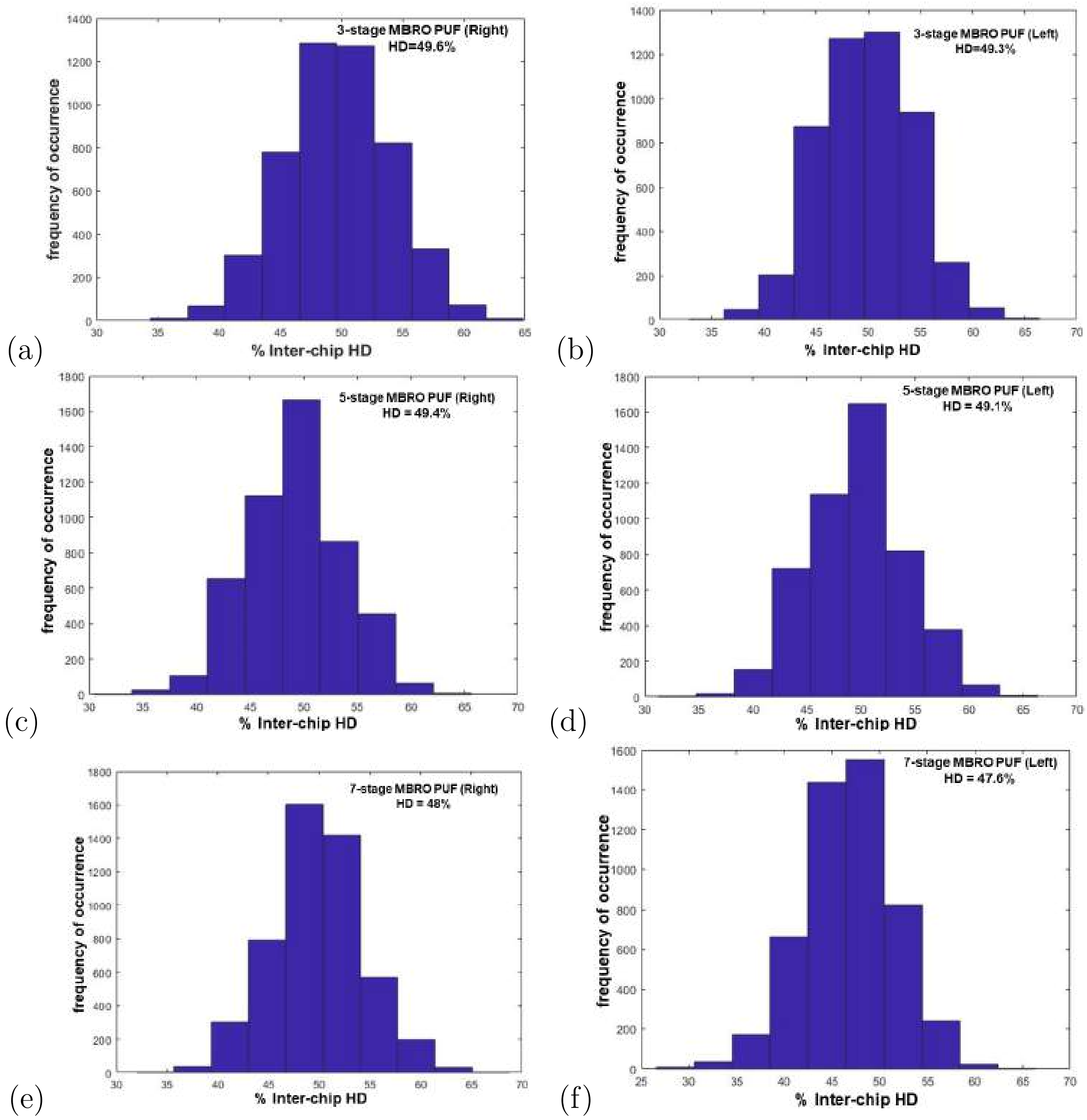


Figure 5.12: The representation of the inter-chip hamming distance of proposed MBRO PUF (a) 3-stage MBRO PUF Right (b) 3-stage MBRO PUF Left (c) 5-stage MBRO PUF Right (d) 5-stage MBRO PUF Left (e) 7-stage MBRO PUF Right (f) 7-stage MBRO PUF Left [72].

constrained application. In light of this, we are focusing on MBRO PUF that facilitate in-memory security.

Bit-aliasing: It calculates the bias of a bit in replies provided by different devices to the same challenge. it calculates the bias of 0 or 1 for the same bit in replies from many devices. Bit-aliasing should ideally be 0.5. We have obtained bit aliasing for all stages equivalent to 0.48, 0.49 and 0.51, respectively, for 7-, 5-,and 3-stage RO PUF.

Uniqueness: It is assessed by measuring the inter-chip Hamming distance of different PUF responses. Let us suppose that about challenge R_a and R_b represent two n-bit response outputs from arbitrarily taken chips a and b out of m available chips. Uniqueness

(U) can be quantified as :

$$U = \frac{2}{m(m-1)} \sum_{a=1}^{m-1} \sum_{b=a+1}^{m} \frac{HD(R_a, R_b)}{n} * 100\% \tag{5.1}$$

uniqueness, which assesses how well one PUF can be distinguished from others by calculating the average HD among PUFs in distinct chips (aiming for an inter-chip HD near 50% for sufficient uniqueness)[45]. The uniqueness histogram is shown in Fig. 6.9 (c). The study indicates the proposed MBRO PUF exhibits the utmost uniqueness, approaching closely to the ideal value of 0.5, and considering different stages of PUF it has been found that for the proposed PUF uniqueness of the 3 stage > 5 stage > 7 stage at nominal values 1.1V and 25°C.

Table 5.7: Intra-chip Hamming Distance percentage comparison at different temperatures.

Operating Condition	**3-stage PUF**	**5-stage PUF**	**7-stage PUF**
50°C	3.34	3.56	2.78
75°C	3.43	3.72	3.19
100°C	3.70	3.72	3.44

Reliability: The response variation under various environmental circumstances should be zero for ideal PUF. Circuit delay is affected by temperature and voltage variations, which can lead to instability in the PUF response. To calculate reliability, the two responses obtained at different time instances under varying environmental conditions are compared. Reliability R can be measured by:

$$R = 1 - \frac{1}{k} \sum_{m=1}^{k} \frac{HD(R_n, R_n^{'})}{n} * 100\% \tag{5.2}$$

Here, k represents sample count, n represents bits count generated, and $HD(R_n, R_n^{'})$ indicates the Hamming Distance between R_n and $R_n^{'}$. In order to improve security, reliability calculation with intra-die hamming distance is important for measuring response consistency within a single PUF instance in a chip. It has been found that if the temperature increases, then uniqueness is better; however, in the case of intra-HD variation, the temperature increase degrades the reliability. We have checked the reliability at nominal values of 1.1V at 25°C. The % change in intra-HD with temperature is shown in Table 5.7. Further comparison with previous work is shown in Table 5.8. The proposed

MBRO PUF demonstrates improved performance with significantly reduced area (11,447 µm^2) and power consumption (30 µW) compared to prior works. It achieves near-ideal inter-chip hamming distances (0.496, 0.494, 0.48), ensuring high uniqueness and stability. Additionally, its compact cell design (6.23 µm^2) offers efficient integration without compromising reliability.

Table 5.8: Performance Comparison of PUFs

Metric	**ISSCC'15** [57]	**JSSC'18** [55]	**JSSC'19** [81]	**JSSC'21** [82]	**ISSCC'21** [83]	**ISCAS'21** [80]	**TCAS-I'25** [59]	**MBRO PUF** **Proposed (3,5,7-stage)**
Technology (nm)	40	40	40	40	40	40	45	**40**
Architecture used	RO	Static monostable	Soft BD	SRAM bitcell read current	Hybrid RO	RRAM	MBM	**MBRO**
Response size (bit)	256	128	128	128	128	–	64	**256 (128 in each direction)**
Supply voltage (V)	0.7∼1.2	0.8∼1.0	0.9∼1.5	0.7∼1.2	0.7–1.4	1∼1.2	1.0	**1.1±10%**
Power consumption (μW)	28.4	151	–	–	–	–	–	**30**
Inter-chip HD (%)	0.5007	0.49	0.496	0.503	0.496	0.486	0.4937–0.4989	**0.496, 0.494, 0.48**
PUF cell area (μm^2)	–	5.83	–	3	–	3	9.4	**6.23**
PUF area (μm^2)	845	–	–	15,400	21,675	–	1,400	**11,447**

5.6 Summary

We explore the security aspects that demonstrate the effectiveness of this approach in creating secure, low-power, and aging-resilient PUFs. The proposed MBRO PUF demonstrates improved inter-chip hamming distance (0.496–0.48) and reduced power consumption ($30uW$) compared to prior designs. It also offers a compact PUF cell area ($6.23\mu m^2$) and scalable architecture supporting multi-stage operation. By integrating memory and oscillator functionality within the same hardware substrate, the proposed design supports both in-memory PUF generation and CIM operations.

Chapter 6

SRAM-Based PUF Enhanced by In-Memory Computing

The rapid rise of edge devices requires security measures that are portable, energy-efficient, and resistant to attacks. Because they sometimes require a significant computing cost, conventional encryption methods are inappropriate for edge devices with limited resources. Using the intrinsic properties of 10T SRAM cells and the bitline discharge technique, this chapter investigates a secure and reliable in-memory computing architecture to construct PUF as shown in Figure 6.1. The main objective of this work is to develop and assess a complete 10T SRAM-based system that can manage secure key generation based on PUF with little overhead. The work begins with the construction and characterization of a single 10T SRAM cell before moving on to a 64x32 array architecture. Significant efforts were made to design, integrate, and simulate essential peripheral circuits such as the write

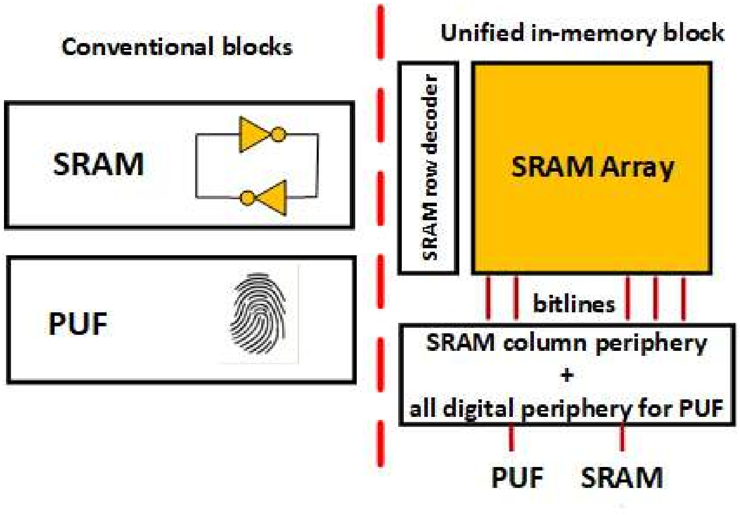


Figure 6.1: Functional overview of the computing-in-memory-based PUF design.

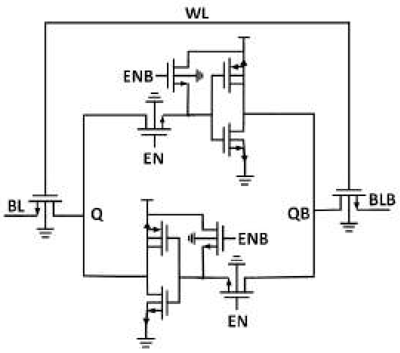


Figure 6.2: Proposed 10-T SRAM cell

driver, precharge circuit, and sense amplifier in order to guarantee correct functioning. The study included extensive pre- and post-layout simulations as a critical component for PUF implementation. The PUF operation, including delay and power consumption metrics, was obtained at both stages in order to examine the effects of parasitic components introduced during layout synthesis. Comparative analysis was used to highlight the performance differences between schematic-level and extracted-level findings.

6.1 In-Memory PUF Architecture

6.1.1 10T SRAM with Aging-Resilient Inverter (ARI)

The proposed 10T SRAM cell is designed to replace the conventional inverter with the aging resilient inverter (ARI) [79] as it exhibits lower deterioration compared to the conventional design. To improve the functionality of the SRAM cell, we introduce one NMOS pass transistor at the input of the inverter with gate terminal connected to EN and one nmos with the source terminal connected to VDD and the gate connected to ENB as shown in Figure 6.2. The working of the proposed SRAM cell is discussed below:

Write Operation for* 1*: Initially Bit lines $BL = 1$ and $BLB = 0$ by using write driver circuit then after we enable the word line $WL = 1$.

Write Operation for* 0*: Initially Bit lines $BL = 0$ and $BLB = 1$ using the write driver circuit, then after we enable the word line $WL = 1$.

Read Operation : Initially Bit lines are precharged to $BL = 1$ and $BLB = 1$ then we enable the word line $WL = 1$ we observe the output using a sense amplifier.

For the proposed 10T-SRAM we have calculated the SNM with the transistor sizing shown in Table 6.1 and compared with the 6T SRAM and it shows the better results.

Table 6.1: Transistor Sizing for SRAM Cell Components

Transistor Type	**Size (nm)**
Inverter PMOS (INV PMOS)	120
Inverter NMOS (INV NMOS)	520
Outer NMOS	480
Pass Transistor (SRAM)	200

Table 6.2: Comparison of Parameters for Different SRAM Cell Structures

Parameters	**6T-SRAM**	**10T-SRAM**
Read Power, (**pW**)	8.5	9.2
Write Power, (**uW**)	174	169
Area, ($\mu\mathbf{m^2}$)	3.1	4.5
Write Delay, (**ps**)	18.5	15.8
Read Delay, (**ps**)	9.4	8.2

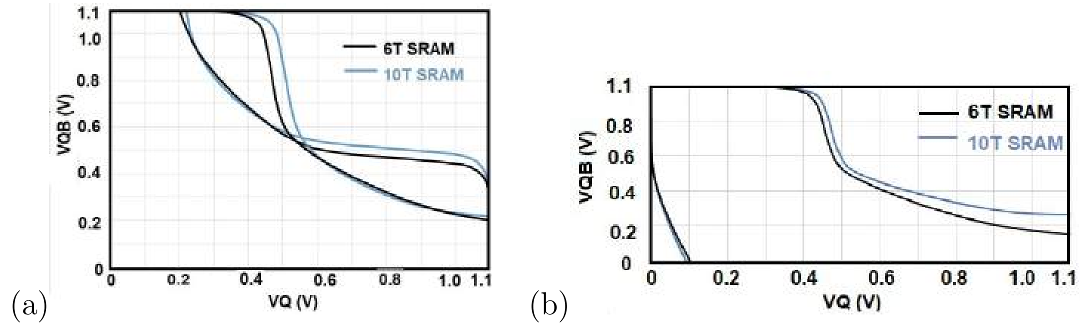


Figure 6.3: Static Noise Margins of standard 6T-SRAM and proposed 10T-SRAM (a) read SNM (b) write SNM.

6.1.2 Peripherals of Memory Array

Peripheral circuits play a vital role in enabling reliable read and write operations in memory systems, especially in SRAM-based arrays used for PUF applications. Key peripherals include the write driver, precharge circuit, and sense amplifier. While the core memory cell (such as a 6T or 8T SRAM cell) is responsible for data storage, the peripheral circuits ensure correct operation, high speed, and power efficiency during memory access. Moreover, the accuracy and timing of these circuits directly influence the stability and quality of the generated output bits in entropy-based applications such as PUFs.

- **Write Driver Circuit:** During a write operation, the write driver controls the voltages on the bitlines (BL and BLB) to store data in the SRAM cell. Once the write word line is activated, the access transistors connect the internal storage nodes of the cell to the bitlines. The write driver then applies complementary voltage levels to BL and BLB according to the input data, forcing one node high and the other

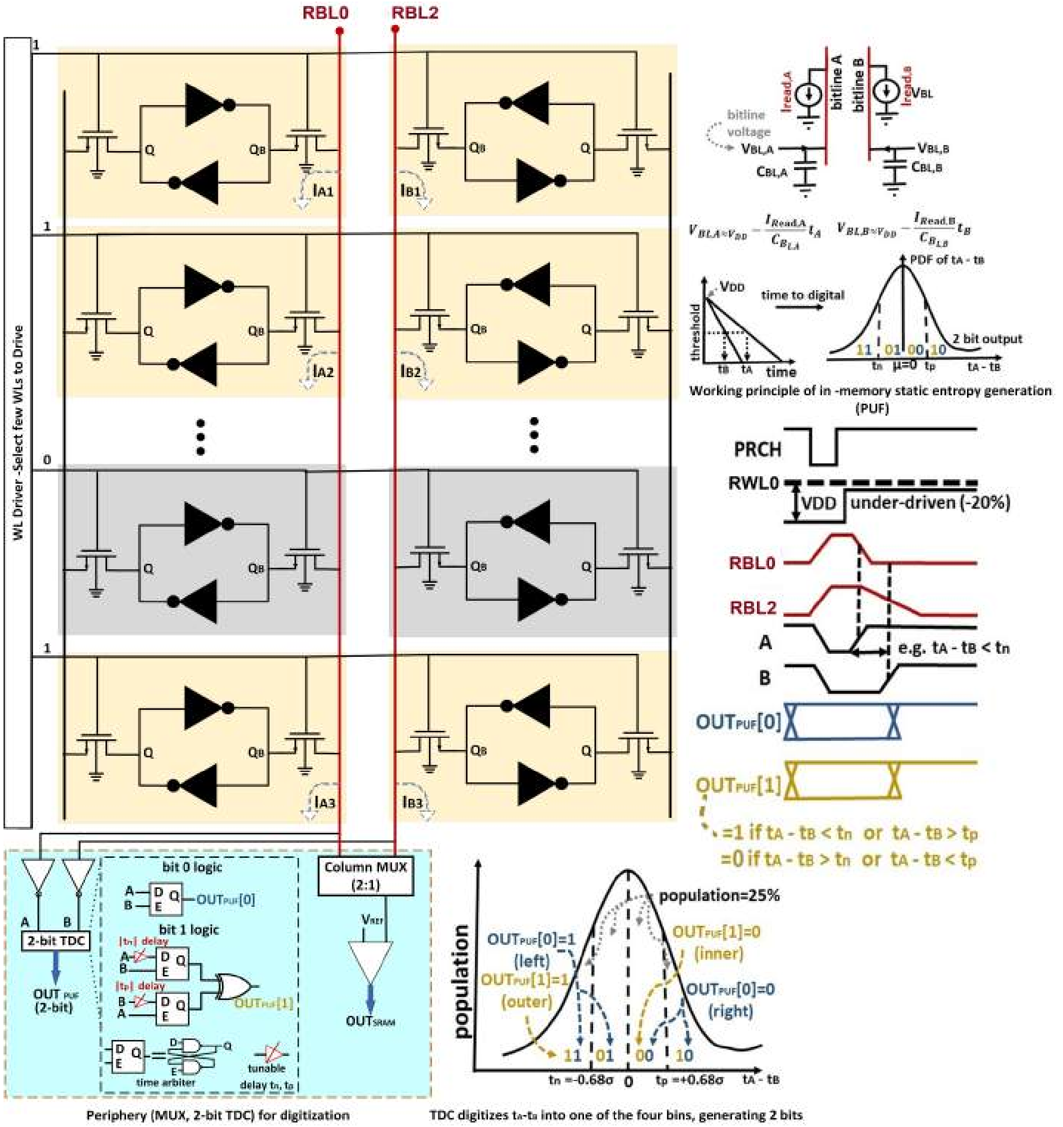


Figure 6.4: PUF implementation circuit with periphery for digitalization and working principal of in-memory static entropy generation, waveform of multi-bit static entropy generation and digitization.

low. For example, to write a logic '1,' BL is driven to V_{DD} and BLB to ground, whereas the opposite voltages are applied to write a '0.' The driver must provide sufficient current to overcome the feedback strength of the SRAM latch, ensuring that the existing data is reliably overwritten without causing excessive stress on the cell.

- **Precharge Circuit:** The precharge circuit prepares the bitlines for each read or write operation by charging them to a predetermined voltage level, typically V_{DD} or a fixed reference level. Before a memory access begins, the precharge enable signal activates PMOS transistors that charge the bitlines and an equalization transistor that ensures both lines reach the same voltage. This establishes a uniform initial condition across the memory array, reducing access time and power consumption in conventional SRAM systems. In PUF and entropy-extraction applications, this controlled starting voltage is especially important because the subsequent bitline discharge behavior depends directly on this initial state. Any mismatch or timing error in the precharging process may introduce bias or degrade the quality of the generated response.

- **Sense Amplifier:** The sense amplifier is responsible for detecting and amplifying the small voltage differences that develop on the bitlines during a read operation. When the word line is asserted, one bitline begins to discharge depending on the value stored in the SRAM cell, creating a small voltage difference between BL and BLB, typically on the order of millivolts. The sense amplifier rapidly amplifies this small signal into a full logic-level output, thereby enabling accurate data readout. In differential sensing, both BL and BLB are used as inputs, whereas in single-ended sensing (as in some 8T SRAM designs), the read bitline is compared with a reference voltage. The speed and sensitivity of the sense amplifier significantly influence read latency, power efficiency, and output reliability.

6.1.3 Bitline Discharge–Based PUF Mechanism with peripheral circuitry

In this work, a bitline discharge–based technique is employed using the proposed 10T bitcell to measure variations in bitline discharge behavior during read operations. The fundamental principle relies on observing differences in the bitline discharge rate, which arise due to inherent process-induced device mismatches. These variations introduce sufficient randomness in the discharge time, thereby enabling physical entropy extraction.

The operating principle and the corresponding PUF circuit implementation are illustrated in Figure 6.4. The discharge-based sensing mechanism enhances randomness by exploiting uncontrollable manufacturing variations, making the responses unique and difficult to replicate across different instances of the circuit.

Two adjacent bitcells, A and B, are used to analyze the difference in bitline discharge time between tA and tB. One wordline is enabled, and bitlines are initialized in the SRAM bank, and one wordline is activated in the SRAM bank under consideration. Stated differently, the identical value must be stored in each bitcell and array row utilized to

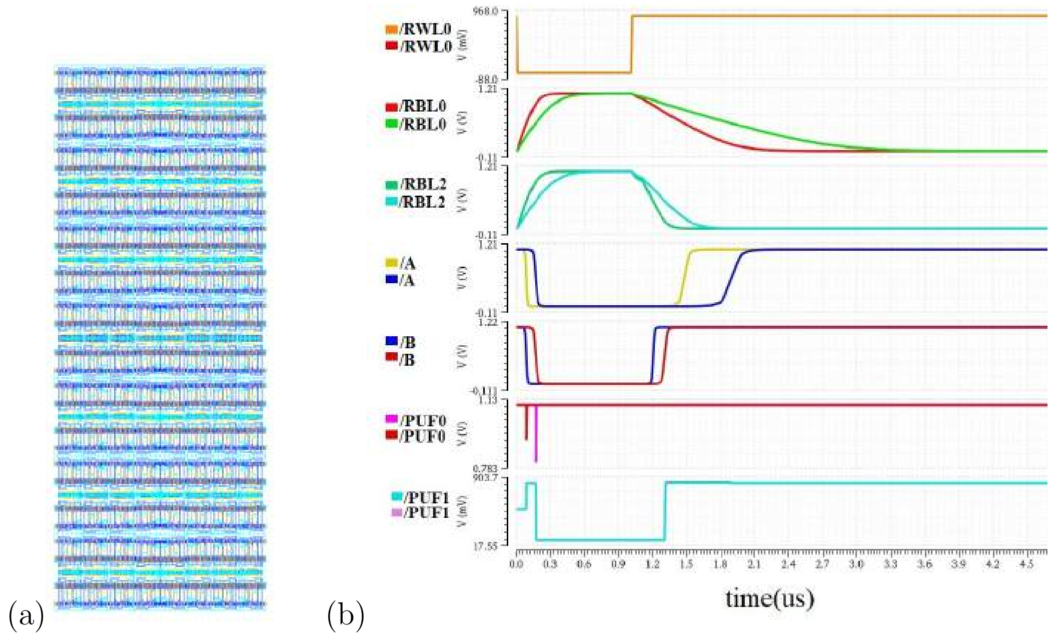


Figure 6.5: (a) Layout design of 32×64 8T SRAM array for PUF implementation (b) Transient response of post-layout simulation for PUF implementation.

generate PUF output. The bitline discharge time difference was digitally converted using a time-to-digital converter (TDC) to the digital output of PUF as shown in Figure 6.4.

The bitline discharge technique exploits the analog behavior of bitlines during a controlled read operation, unlike conventional SRAM-based approaches that rely only on the power-up state of memory cells. By leveraging variations caused by noise, process fluctuations, and transistor mismatch, this method provides a rich source of entropy and enables reliable device fingerprinting. The bitline discharge method consists of two stages: precharge and controlled discharge. When an SRAM cell read path is triggered, the technique primarily monitors the voltage drop on a precharged bitline.

Precharge phase: In a SRAM, the read bitline (RBL) is precharged to the supply voltage V_{DD} before the read operation begins. This precharging establishes a uniform initial voltage across all cells, ensuring consistent operating conditions and enabling reliable comparison during the read process.

Discharge phase: When the read word line is asserted, the read path becomes active. The conduction of the read transistor stack depends on the data stored in the SRAM cell. If the path is conductive, the precharged RBL starts discharging toward ground through the transistor stack. The discharge rate is primarily governed by the NMOS transistor characteristics, such as carrier mobility, threshold voltage, and channel length variations, as well as the stored cell state (Q = 1 or 0), along with noise and random process variations.

Sensing and output generation: After a predefined interval, the bitline voltage is sampled, typically using a voltage comparator or a sense amplifier. If the bitline voltage V_{BL} falls below a specified threshold V_{th} , the output is interpreted as a logic '1'; otherwise, if V_{BL} remains above V_{th}, it is interpreted as a logic '0'. This binary result, derived from the discharge behavior of each SRAM cell, forms the unique PUF response bit. When the discharge behavior is measured under controlled and repeatable conditions, the output remains consistent across multiple evaluations, enabling reliable key generation and device identification. The discharge rate of each SRAM cell is mainly influenced by static physical variations such as channel doping, oxide thickness, and threshold voltage. To improve robustness and reduce instability, error-correction techniques (e.g., fuzzy extractors) and environmental compensation methods can be employed.

6.2 Performance Analysis

This section describes the full implementation and outcomes of the suggested SRAM-based physical unclonable function using 10T SRAM cells and the bitline discharge approach. The Cadence Virtuoso design environment and UMC 40nm technology were used for the simulations. We have implemented the layout of the 32X64 10T-SRAM array for PUF design as showns in Figure 6.5. This chapter aims to analyse the outcomes under various voltage and layout settings and confirm the suggested architecture's functionality, unpredictability, and stability.

- **Time-to-Digital converter** The PUF circuits use a TDC to digitize the delay difference between matched pathways. It measures the time difference in digital form using a counter mechanism and a delay chain.

- **Digitization of PUF output** A time-to-digital converter is used to digitize the discharge-based PUF analog behavior. This guarantees a consistent 0 or 1 result for every bit. Sharp logic levels are ensured by comparing the digital output with the analog discharge voltage.

- **8-bit PUF output waveform** Figure 6.6 displays the collected 8-bit PUF output. Each SRAM instances uniqueness is confirmed by the waveform, which verifies steady and distinct bits produced across several runs.

- **Bit error rate vs supply voltage** The bit error rate is tested at several supply

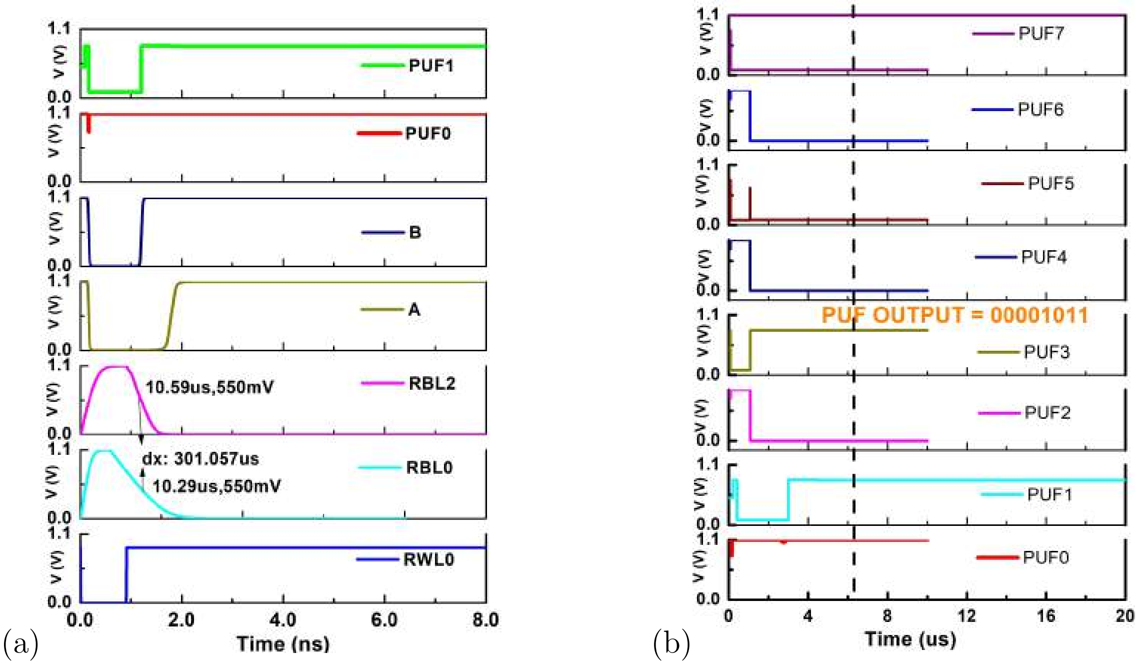
Table 6.3: Comparison of pre-layout and post-layout simulation results for PUF implementation

Parameter	**Simulation Results**	
	Pre-layout	**Post-layout**
Delay between RWL0 and RBL0 (ns)	444.45	842.36
Delay between RWL0 and RBL1 (ns)	180.922	282.8
Static power (mW)	1.22	1.18
Peak power (mW)	129	126.26

Post-layout results include parasitic extraction effects.

voltages between 0.8V and 1.3V in order to assess resilience. Figure 6.8 a illustrates how the BER rises at lower voltages because of smaller noise margins while staying within reasonable bounds under normal circumstances.

- **Instability vs supply voltage** PUF bit instability is examined across voltage ranges. The number of unstable bits when voltage varies is shown in Figure 6.8b. At nominal voltage 1.1V, the instability is reduced, confirming the designs dependability.



(a) (b)

Figure 6.6: Waveforms of (a) Time-to-Digital Converter and (b) 8-bit PUF Output.

- **Post-layout simulation** Extracted parasitics were used in post-layout simulations. The effect of layout-induced delays on the PUF output Although there were slight timing deteriorations, functionality was unaffected. Table 6.3 represent a comparison of pre-layout and post-layout simulation results for PUF implementation. Post-

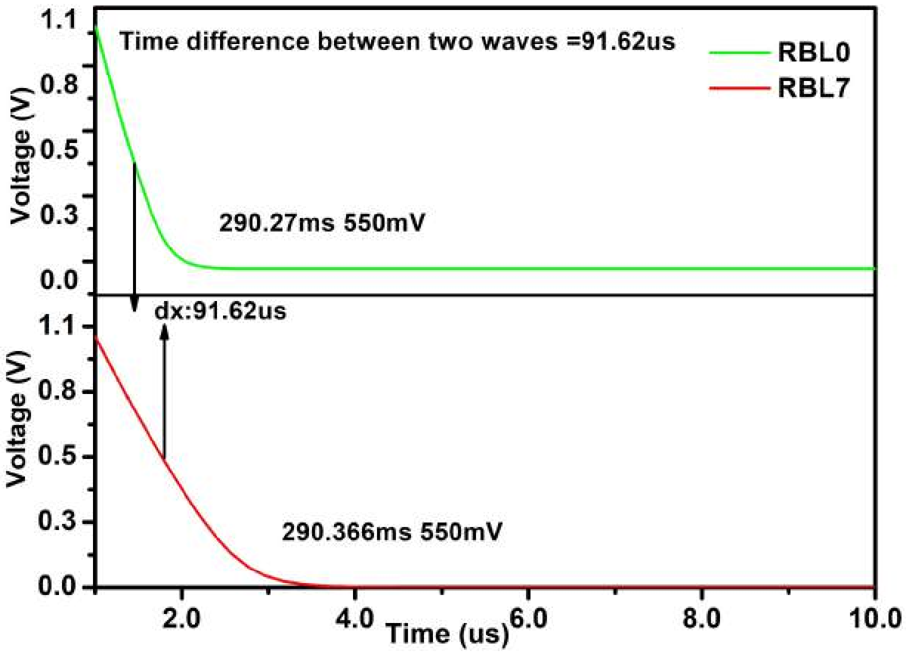
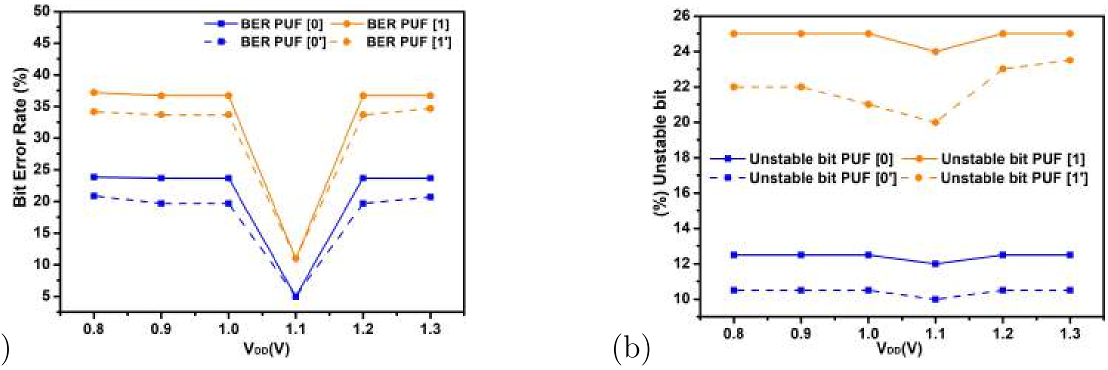


Figure 6.7: Voltage vs time for analog PUF output



(a)

(b)

Figure 6.8: Comparison of (a) BER and (b) instability versus supply voltage before and after applying the error reduction technique. BER PUF[0], PUF[1], and unstable bits PUF[0] and PUF[1] represent the results before the technique; PUF[0] and PUF[1] represent the results after the technique.

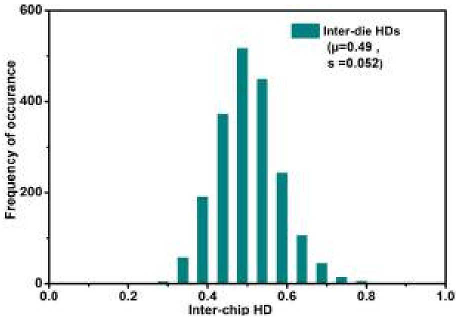


Figure 6.9: Interchip HD.

layout adjustments resulted in increased stability and BER. The BER and instability before and after arrangement are contrasted in Figures 6.8.

Table 6.4: Comparison of This Work with State-of-the-Art PUF Designs

Metric	**This Work**	**JSSC 2021 [82]**	**JSSC 2020 [84]**	**ISSCC 2021 [83]**
Technology (nm)	40	28	130	40
Entropy Source	Bitline discharge method	SRAM bitcell read current	Hybrid SRAM	Hybrid ring oscillator
Layout Area of 64 × 32 8T SRAM Array (μm^2)	1912	1125	2307	21,675
V_{DD} (V)	0.8–1.3	0.75–1.05	0.5–0.7	0.7–1.4
Temperature (°C)	−25 to 105	−25 to 100	−40 to 120	−40 to 125
Unstable Bits (%) @ Nominal V	10.2 (LSB), 20.4 (MSB)	11.4 (LSB), 29.5 (MSB)	2.71	0.39
Bit Error Rate (BER %) @ Nominal V	5 (LSB), 12 (MSB)	1.8 (LSB), 3.78 (MSB)	0.29	0.03
PUF Energy (fJ/bit)	85	72	16.76	39
Inter-chip HD	0.49	0.503	0.487	0.496

6.3 Summary

In this chapter, a physical unclonable function architecture based on 8T SRAM cells using bitline discharge techniques was designed, simulated, and analyzed. The study effectively shown that high entropy responses appropriate for secure key generation and device authentication can be achieved by carefully managing the bitline discharge path and taking use of process variation in 8T SRAM-based memory cells. The following are some of the main achievements:

- Design and simulation of 8T SRAM-based PUF: This design uses a small and effective 8T SRAM cell to combine hardware fingerprinting and randomness extraction. Pre-layout and post-layout simulations were used to evaluate the PUF module, guaranteeing its dependability in authentic parasitic scenarios.

- Methods for reducing bit error rates: A number of methods were investigated to increase the PUF responses stability and repeatability. Among these were improvements at the circuit level and the use of lightweight error correction to guarantee resilience to changes in the environment and voltage.

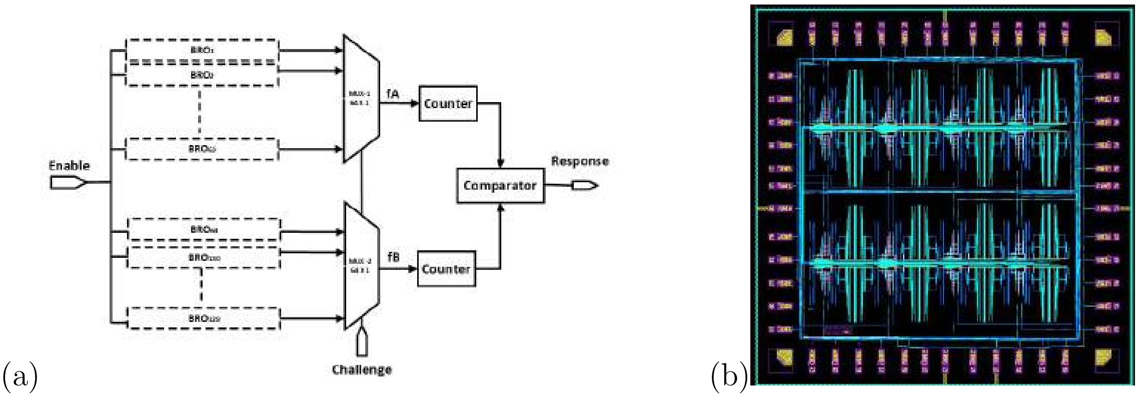
- Post-layout verification: The entire layout design was put into practice in UMC 40nm technology, and then post-layout simulations were run to assess timing, power, and bit error rate. This confirmed the design functional correctness and process robustness.

Chapter 7

Tapeout

7.1 BRO PUF

A BRO-PUF-based cryptographic security solution is implemented using configurable ring oscillators. The ring oscillators are constructed using tristate inverter logic connected back-to-back. The design aims to enhance security, flexibility, and resistance to side-channel attacks. A circuit logically equivalent to the proposed BRO-PUF was developed and tested on Basys3 board. Bistable ring operation was verified using an XOR latch. 256 PUF instances are implemented for testing.



(a)

(b)

Figure 7.1: Proposed tristate inverter based BRO PUF and its layout using SCL 180nm

7.1.1 CAD Tool and Design Flow

The complete schematic-to-GDSII implementation of the proposed design is carried out using Cadence Virtuoso. The design methodology follows a standard full-custom VLSI

Table 7.1: PUF Design Specifications

Parameter	**Value**
Technology (CMOS)	SCL 180 nm
Number of PUF Instances	16
Operating Frequency	778.4 MHz
PUF Output Length	32 bits
Power Consumption	59 nW
Supply Voltage	1.8 V
Die Area	4 × 4 mm^2

flow, starting from circuit description and concluding with physical layout generation. Design Process Steps from Schematic to GDS II

- **Schematic Entry** The complete circuit is captured in the Virtuoso Schematic Editor, including transistor-level implementation of the 128 instances of TL-based RO, 2 64 X 1 MUX, counter, and comparator for PUF logic.
- **Functional Simulation:** The schematic is simulated using the Virtuoso Analog Design Environment (ADE) to verify functionality, transient response, and signal integrity.
- **Pre-layout Verification:** Parametric analysis across process corners, supply variations, and temperature (PVT analysis) is performed to ensure robustness of the design.
- **Layout Design:** The physical layout is created using the Virtuoso Layout Editor, following design rules provided by the SCL 180nm foundry process design kit (PDK).
- **Design Rule Check (DRC)** DRC is performed to verify that the layout adheres to all manufacturing constraints specified in the technology file.
- **Layout Versus Schematic (LVS)** LVS is carried out to ensure logical equivalence between the schematic and the extracted layout.
- **Parasitic Extraction (PEX)** Parasitic resistances and capacitances are extracted from the layout using the extraction tool and back-annotated into the netlist.
- **Post-layout Simulation** The extracted netlist is simulated to validate delay, power, and frequency behavior under real layout conditions.
- **GDSII Generation (Stream-Out)** Once signoff checks are completed, the final layout is exported in GDSII format for fabrication.

7.2 Conventional Arbiter PUF

An Arbiter PUF is a delay-based hardware security primitive that exploits manufacturing variations in integrated circuits to generate unique, device-specific responses. It consists of a series of multiplexers that create two parallel signal paths with nearly identical delay characteristics. When a challenge is applied, signals race through both paths, and an arbiter (typically a latch) determines which signal arrives first, producing a one-bit response. By varying the input challenges, multiple unique CRPs can be generated. Arbiter PUFs are widely used for device authentication and key generation due to their simplicity and uniqueness.

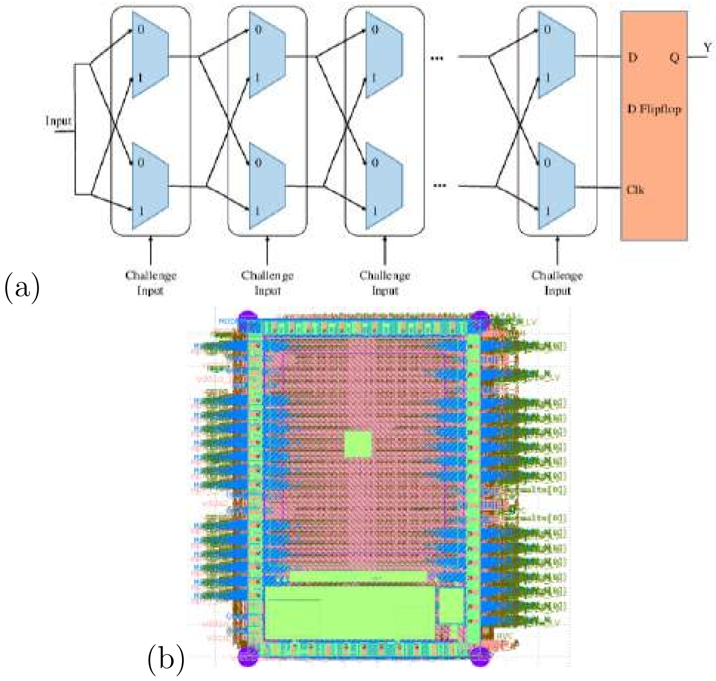


Figure 7.2: Conventional Arbiter PUF and its layout using Skywater 130nm

Table 7.2: Design Specifications

Parameter	Value
Technology (pdk)	Sky130 nm
Total Power	1.17 μW
Supply Voltage	1.8 V
Project Area	2676 μm^2

7.2.1 Design Tool and Implementation Flow

The design, simulation, and physical implementation of the conventional Arbiter PUF are carried out using an open-source digital implementation flow based on OpenLane. The complete design environment includes RTL design, synthesis, placement and routing, and layout generation. RTL-to-GDSII Design Flow (Open-Source CAD Flow)

The design flow for the Arbiter PUF from RTL to GDSII proceeds as follows:

- **RTL Design** The Arbiter PUF architecture is described using Verilog HDL, including the multiplexer chain, arbiter latch, and challenge input logic.

- **Functional Simulation** RTL simulation is performed to validate functional correctness and verify response generation under various challenges.

- **Logic Synthesis** The RTL code is synthesized into a gate-level netlist using a skywater130 PDK.

- **Floorplanning** The initial floorplan is generated, specifying die dimensions, core utilization, and placement constraints.

- **Placement** Standard cells are placed within the core area to optimize timing, area, and power.

- **Clock Tree Synthesis (CTS)** A balanced clock network is created to minimize skew and ensure synchronized triggering of the arbiter.

- **Routing** Global and detailed routing are performed to interconnect all standard cells.

- **Static Timing Analysis (STA)** Post-route timing is analyzed to ensure that signal paths meet setup and hold constraints.

- **Physical Verification** DRC: Ensures layout complies with process design rules. LVS: Confirms correspondence between schematic and layout.

- **GDSII Generation** After successful verification, the final layout is exported in GDSII format for tapeout readiness.

7.3 Limitition and Future Scope

The arbiter PUF was successfully taped out using the SkyWater 130 nm PDK and an open-source EDA tool flow, and the fabricated silicon has been received. However, detailed post-silicon measurement and characterization are currently ongoing and therefore silicon measurement results are not yet available at this stage.

Future work will focus on comprehensive testing of the arbiter PUF to evaluate standard PUF performance metrics, including uniqueness, reliability, uniformity, and stability under process, voltage, and temperature (PVT) variations. In addition, the integration of the arbiter PUF with edge devices is planned to enable practical evaluation in real-world authentication and secure key generation scenarios.

In parallel, a configurable ring oscillator (RO) PUF has been designed and taped out using the SCL 180 nm technology node through cadence flow. The fabricated silicon for the RO PUF has not yet been received, and therefore no silicon-level validation has been performed to date. Upon receipt, similar post-silicon testing and characterization will be conducted, followed by planned integration with edge devices to assess system-level performance and applicability.

Chapter 8

Conclusion and Future Scope

The increasing demand for secure and reliable electronic systems highlights the importance of developing robust hardware-based security primitives. This thesis presents a comprehensive exploration of memory-based and oscillator-based PUF architectures, proposing novel designs that enhance randomness, reliability, and resistance to modeling attacks. By unifying SRAM-based entropy generation with delay-based ring oscillator structures, this work establishes a new framework for developing reconfigurable and high-entropy PUF systems.

Three PUF architectures are analyzed: a 10T SRAM-based PUF using in-memory computing , a CIM enabled MBRO-PUF and a configurable RO PUF. The work shows that integrating CIM principles into security-oriented circuit design is an effective approach for building next-generation PUF implementations with lower power consumption, increase latency, and superior entropy quality. Overall, this thesis contributes a novel architectural viewpoint that bridges memory-centric computing with hardware security, offering scalable and reconfigurable PUF solutions for modern computing platforms.

Future Scope

The research presented in this thesis opens several promising directions for further exploration:

- **SoC-Level Integration with Emerging Memory Technologies** Future work may focus on implementing the proposed RO-PUF and SRAM-PUF architectures in SoC environments using memory technologies such as NV-SRAM, RRAM, and memristors. This integration would enable non-volatile secure key storage and enhance system-level trust mechanisms.

- **Application in IoT and Edge Devices** The proposed lightweight and energy-efficient PUF designs are well suited for IoT devices, edge computing platforms, and embedded systems. Future research can focus on large-scale deployment studies, hardware prototyping, and long-term aging analysis under real operating conditions.
- **Enhanced Reliability and Security Evaluation** Further enhancements may include integrating error correction mechanisms, adaptive calibration techniques, and advanced response conditioning to improve stability. Comprehensive evaluation against machine-learning-based modeling attacks and side-channel attacks will further strengthen security confidence.

Future work will also focus on comprehensive testing of the arbiter PUF and Configurable RO PUF to evaluate standard PUF performance metrics, including uniqueness, reliability, uniformity, and stability under process, voltage, and temperature (PVT) variations. In addition, the integration with edge devices is planned to enable practical evaluation in real-world authentication and secure key generation scenarios.

Bibliography

[1] Synopsys, Inc., “The reliability of sram PUF,” *Synopsys, Inc., Tech. Rep.*, 2025, accessed: 2025- 12-02. [Online]. Available: https://www.synopsys.com/designware-ip/security-ip/reliability- sram-puf.html.

[2] Z. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of things for smart cities,” *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[3] S.Gaudin, “Get ready to live in a trillion-device world,” https://www.computerworld.com/article/2983155/get-ready-to-live-in-a-trillion-device world.html, 2015, accessed: 2020-03-28.

[4] R. Dobbs, J. Manyika, and J. Woetzel, “Unlocking the potential of the Internet of Things,” McKinsey Company, 2015. [Online]. Available: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world . Accessed: Mar. 28, 2020.

[5] L. S. Vailshery, “Number of Internet of Things connected devices 2020–2033, by region,” Statista, 2024. [Online].

[6] T. Xu, J. B. Wendt, and M. Potkonjak, “Security of IoT systems: Design challenges and opportunities,” in Proc. 2014 *IEEE/ACM Int. Conf. Computer-Aided Design (ICCAD)*, 2014, pp. 417–423.

[7] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, *“Security, privacy and trust in Internet of Things: The road ahead,” Computer Networks,* vol. 76, pp. 146–164, 2015.

[8] A. R. Sadeghi, C. Wachsmann, and M. Waidner, “Security and privacy challenges in industrial Internet of Things,” *in Proc. 52nd Annu. Design Autom. Conf. (DAC), ACM*, San Francisco, CA, USA, p. 54, Jun. 2015.

[9] B. Halak, J. Murphy, and A. Yakovlev, "Power-balanced circuits for leakage-power-attacks resilient design," *in Proc. Science and Information Conf. (SAI), IEEE,* July 2015, pp. 1178–1183.

[10] S. Devadas, G. E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of PUF-based 'unclonable' RFID ICs for anti-counterfeiting and security applications," *in Proc. 2008 IEEE Int. Conf. RFID,* pp. 58–64,April 2008.

[11] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, Sep. 2002.

[12] W. J. Herschel, The Origin of Finger-Printing. London: Oxford University Press, 1916.

[13] E. Computing, "Protecting the iot with invisible keys," Embedded Com- puting, *Tech. Rep.*, 2025, accessed: 2025-12-02. [Online].

[14] Y. Yilmaz, L. Aniello, and B. Halak, "ASSURE: A hardware-based security protocol for Internet of Things devices," in Authentication of Embedded Devices: Technologies, Protocols and Emerging Applications, Cham, Switzerland: *Springer Int. Publishing*, pp. 55–87, Jan. 2021.

[15] C. Herder, M. D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE,* vol. 102, no. 8, pp. 1126–1141, May 2014.

[16] P. Radanliev, "Digital security by design," *Security Journal*, vol. 37, no. 4, pp. 1640–1679, Dec. 2024.

[17] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," *in Proc. 9th ACM Conf. Computer and Communications Security (CCS)*, pp. 148–160, Nov. 2002.

[18] A. Maiti, "A systematic approach to design an efficient physical unclonable function," Ph.D. dissertation, Virginia Polytechnic Institute and State University (Virginia Tech), 2012.

[19] P. Bulens, F. X. Standaert, and J. J. Quisquater, "How to strongly link data and its medium: The paper case," *IET Inf. Security*, vol. 4, no. 3, pp. 125–136, Sep. 2010.

[20] G. Hammouri, A. Dana, and B. Sunar, "CDs have fingerprints too," *in Proc. Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, Berlin, Germany: Springer Berlin Heidelberg, pp. 348–362, Sep. 2009.

[21] G. DeJean and D. Kirovski, "RF-DNA: Radio-frequency certificates of authenticity," *in Proc. Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, Berlin, Germany: Springer Berlin Heidelberg, pp. 346–363, Sep. 2007.

[22] J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls, "Physical unclonable functions and public-key crypto for FPGA IP protection," *in 2007 Int. Conf. Field Programmable Logic and Applications (FPL)*, pp. 189–195, Aug. 2007.

[23] 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 Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1876–1891, Aug. 2013.

[24] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up SRAM state as an identifying fingerprint and source of true random numbers," *IEEE Trans. Computers*, vol. 58, no. 9, pp. 1198–1210, Nov. 2008.

[25] V. Van der Leest, G. J. Schrijen, H. Handschuh, and P. Tuyls, "Hardware intrinsic security from D flip-flops," *in Proc. 5th ACM Workshop on Scalable Trusted Computing (STC)*, pp. 53–62, Oct. 2010.

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

[27] Y. Su, J. Holleman, and B. P. Otis, "A digital 1.6 pJ/bit chip identification circuit using process variations," *IEEE J. Solid-State Circuits*, vol. 43, no. 1, pp. 69–77, Jan. 2008.

[28] P. Simons, E. van der Sluis, and V. van der Leest, "Buskeeper PUFs, a promising alternative to D flip-flop PUFs," *in 2012 IEEE Int. Symp. Hardware-Oriented Security and Trust (HOST)*, pp. 7–12, Jun. 2012.

[29] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," *in Proc. 44th Annu. Design Autom. Conf. (DAC)*, pp. 9–14, Jun. 2007.

[30] C. E. Yin and G. Qu, "Temperature-aware cooperative ring oscillator PUF," *in 2009 IEEE Int. Workshop on Hardware-Oriented Security and Trust (HOST)*, pp. 36–42, Jul. 2009.

[31] Synopsys, Inc., "Sram puf – the secure silicon fingerprint," *Synopsys, Inc., Tech. Rep.*,2025, accessed: 2025-12-02. [Online].

[32] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," *in Towards Hardware-Intrinsic Security: Foundations and Practice*, pp. 3–7, Oct. 2010.

[33] J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," *in Proc. Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, Berlin, Germany: Springer Berlin Heidelberg, pp. 63–80, Sep. 2007.

[34] S. Yu, Semiconductor Memory Devices and Circuits. *CRC Press*, 2022.

[35] R. Sarikaya, G. E. Hinton, and A. Deoras, "Application of deep belief networks for natural language understanding," *IEEE/ACM Trans. Audio, Speech, Lang. Process.*, vol. 22, no. 4, pp. 778–784, Feb. 2014.

[36] T. Singh, S. Rangarajan, D. John, C. Henrion, S. Southard, H. McIntyre, A. Novak, S. Kosonocky, R. Jotwani, A. Schaefer, and E. Chang, "3.2 Zen: A next-generation high-performance ×86 core," *in 2017 IEEE Int. Solid-State Circuits Conf. (ISSCC)*, pp. 52–53, Feb. 2017.

[37] A. Sebastian, M. Le Gallo, R. Khaddam-Aljameh, and E. Eleftheriou, "Memory devices and applications for in-memory computing," *Nature Nanotechnology*, vol. 15, no. 7, pp. 529–544, Jul. 2020.

[38] V. Sharma, H. Kim, and T. T. Kim, "A 64 kb reconfigurable full-precision digital ReRAM-based compute-in-memory for artificial intelligence applications," *IEEE Trans. Circuits Syst. I, Reg.* Papers, vol. 69, no. 8, pp. 3284–3296, Apr. 2022.

[39] M. Ali, S. Roy, U. Saxena, T. Sharma, A. Raghunathan, and K. Roy, "Compute-in-memory technologies and architectures for deep learning workloads," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 30, no. 11, pp. 1615–1630, Sep. 2022.

[40] N. Maheshwari, M. Panchore, and S. K. Vishvakarma, "BRO PUF: A bi-directional ring oscillator-based PUF for IoT security," *Institution of Electronics and Telecommunication Engineers Jounral Res.*, pp. 1–4, Sep. 2025.

[41] F. Yuan, P. Parekh, and Y. Zhou, "Bi-directional gated ring oscillator time integrator," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 70, no. 9, pp. 3461–3473, Aug. 2023.

[42] Y. Cui, C. Wang, W. Liu, Y. Yu, M. O'Neill, and F. Lombardi, "Low-cost configurable ring oscillator PUF with improved uniqueness," *in 2016 IEEE Int. Symp. Circuits Syst. (ISCAS)*, pp. 558–561, May 2016.

[43] S. Tao and E. Dubrova, "Reliable low-overhead arbiter-based physical unclonable functions for resource-constrained IoT devices," *in Proc. 4th Workshop on Cryptography and Security in Computing Systems (CS2)*, pp. 1–6, Jan. 2017.

[44] S. Tao and E. Dubrova, "Physical unclonable functions based on temperature compensated ring oscillators," *Cryptology ePrint Archive*, 2016.

[45] S. Khan, A. P. Shah, N. Gupta, S. S. Chouhan, J. G. Pandey, and S. K. Vishvakarma, "An ultra-low power, reconfigurable, aging resilient RO PUF for IoT applications," *Microelectronics J.*, vol. 92, p. 104605, Oct. 2019.

[46] 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 Trans. Embedded Comput. Syst. (TECS)*, vol. 18, no. 3, pp. 1–21, Apr. 2019.

[47] M. Benmoussa, A. Benhadria, and L. Bahi, "Design and simulation of a cmos 3-stage ring oscillator-based voltage reference circuit," *in 2019 International Conference on Computing, Electrical and Electronics Engineering (ICCEEE). IEEE*, 2019, pp. 126–129.

[48] M. Goudarzi and M. Shahmohammadi, "A low-power 3-stage ring oscillator-based voltage ref- erence in 40nm cmos technology," *in 2020 18th Iranian Conference on Electrical Engineering (ICEE). IEEE,* 2020, pp. 1287–1291.

[49] W.-D. Chang and Y.-C. Cheng, "A high-performance 3-stage ring oscillator-based cmos volt- age reference," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 56, no. 8, pp. 633–637,April 2009.

[50] J. Zhang and X. Ma, "A low-power voltage reference circuit using a 3-stage ring oscillator in 40 nm cmos," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 60, no. 3, pp. 130–134, Feb 2013.

[51] Z. Xu, M. Zhang, Q. Chen, and J. Ma, "Ring oscillator puf evaluation: quality over quantity," *Journal of Computer Science and Technology*, vol. 31, no. 4, pp. 803–811, July 2016.

[52] A. Maiti and P. Schaumont, "Improved ring oscillator PUF: An FPGA-friendly secure primitive," *J. Cryptol.*, vol. 24, no. 2, pp. 375–397, Apr. 2011.

[53] L. Zhang, C. Wang, W. Liu, M. O'Neill, and F. Lombardi, "XOR gate based low-cost configurable RO PUF," *in 2017 IEEE Int. Symp. Circuits Syst. (ISCAS)*, pp. 1–4, May 2017.

[54] K. H. Chuang, E. Bury, R. Degraeve, B. Kaczer, D. Linten, and I. Verbauwhede, "A physically unclonable function using soft oxide breakdown featuring 0% native BER and 51.8 fJ/bit in 40-nm CMOS," *IEEE J. Solid-State Circuits*, vol. 54, no. 10, pp. 2765–2776, Jul. 2019.

[55] S. Taneja, A. B. Alvarez, and M. Alioto, "Fully synthesizable PUF featuring hysteresis and temperature compensation for 3.2% native BER and 1.02 fJ/b in 40 nm," *IEEE J. Solid-State Circuits*, vol. 53, no. 10, pp. 2828–2839, Sep. 2018.

[56] L. Lu, Y. Z. Chen, and T. T. Kim, "A configurable randomness enhanced RRAM PUF with biased current sensing scheme," *in 2021 IEEE Int. Symp. Circuits Syst. (ISCAS)*, pp. 1–5, May 2021.

[57] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, "14.2 A physically unclonable function with BER ¡ 10 for robust chip authentication using oscillator collapse in 40 nm CMOS," *in 2015 IEEE Int. Solid-State Circuits Conf. (ISSCC) Digest of Technical Papers*, pp. 1–3, Feb. 2015.

[58] 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. 105287–105297, Jul. 2019.

[59] P. Dehghanzadeh, S. Mandal, and S. Bhunia, "MBM PUF: A multi-bit memory-based physical unclonable function," *IEEE Trans. Circuits Syst. I*, Reg. Papers, Jan. 2025.

[60] M. C. Tsai, Y. W. Lin, H. I. Yang, M. H. Tu, W. C. Shih, N. C. Lien, K. D. Lee, S. J. Jou, C. T. Chuang, and W. Hwang, "Embedded SRAM ring oscillator for in-situ measurement of NBTI and PBTI degradation in CMOS 6T SRAM array," *in Proc. 2012 VLSI Design, Automation and Test*, pp. 1–4, Apr. 2012.

[61] S. K. Pillay, "A 0.8 V, tri-state inverter based SRAM cell for SoC applications," *in 2024 37th Int. Conf. VLSI Design and 2024 23rd Int. Conf. Embedded Syst. (VLSID)*, pp. 79–83, Jan. 2024.

[62] N. Maheshwari, A. P. Shah, and S. K. Vishvakarma, "Gated logic controlled 10T-SRAM for low-power bidirectional ring oscillators," *Integration the VLSI Jounral,* p. 102588, Oct. 2025. [Online].

[63] Srivastava S, Verma A, Shah AP. BTI resilient TG-based high-performance ring oscillator for PUF design. *Analog Integrated Circuits and Signal Processing.* 2023 Aug;116(1-2):69-80.

[64] C. Rajan and D. P. Samajdar, "Design principles for a novel lightweight configurable PUF using a reconfigurable FET," *IEEE Trans. Electron Devices,* vol. 67, no. 12, pp. 5797–5803, Oct. 2020.

[65] M. T. Rahman, F. Rahman, D. Forte, and M. Tehranipoor, "An aging-resistant RO-PUF for reliable key generation," *IEEE Trans. Emerg. Top. Comput.*, vol. 4, no. 3, pp. 335–348, Sep. 2015.

[66] R. Sharma, D. Mondal, and A. P. Shah, "Radiation hardened 12T SRAM cell with improved writing capability for space applications," *Memories-Mater., Devices, Circuits Syst.*, vol. 5, p. 100071, Oct. 2023.

[67] A. P. Shah, N. Yadav, A. Beohar, and S. K. Vishvakarma, "On-chip adaptive body bias for reducing the impact of NBTI on 6T SRAM cells," *IEEE Trans. Semicond. Manuf.*, vol. 31, no. 2, pp. 242–249, Feb. 2018.

[68] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 10, pp. 1200–1205, Oct. 2005.

[69] S. Huang, H. Jiang, X. Peng, W. Li, and S. Yu, "Secure XOR-CIM engine: Compute-in-memory SRAM architecture with embedded XOR encryption," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 29, no. 12, pp. 2027–2039, Oct. 2021.

[70] P. Parekh, F. Yuan, and Y. Zhou, " Time-to-digital converter with current-steering vernier time integrator," *Analog Integr. Circuits Signal Process.*, vol. 114, no. 3, pp. 325–343, Mar. 2023.

[71] E. Grossar, M. Stucchi, K. Maex, and W. Dehaene, "Read stability and write-ability analysis of SRAM cells for nanometer technologies," *IEEE J. Solid-State Circuits*, vol. 41, no. 11, pp. 2577–2588, Oct. 2006.

[72] N. Maheshwari, B. B. Gupta, and S. K. Vishvakarma, "CIM-enabled MBRO PUF: Integrating multistage BRO and reconfigurable SRAM for edge security applications," *IEEE Internet of Things J.*, pp. 1–1, 2025.

[73] Z. Chen, M. Wu, Y. Zhou, R. Li, J. Tan, and D. Ding, "PUF-CIM: SRAM-based compute-in-memory with zero bit-error-rate physical unclonable function for lightweight secure edge computing," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 31, no. 8, pp. 1234–1247, Jun. 2023.

[74] J. Tsai, S. O. Toh, Z. Guo, L. T. Pang, T. J. Liu, and B. Nikolic, "SRAM stability characterization using tunable ring oscillators in 45 nm CMOS," *in 2010 IEEE Int. Solid-State Circuits Conf. (ISSCC)*, pp. 354–355, Feb. 2010.

[75] Y. He, M. Choi, K. K. Kim, and Y. B. Kim, "A time-domain computing-in-memory micro using ring oscillator," *in 2021 18th Int. SoC Design Conf. (ISOCC)*, pp. 107–108, Oct. 2021.

[76] V. O. Nyangaresi, M. Ahmad, L. A. Maghrabi, and T. Althaqafi, "Cost-effective PUF and ECC based authentication protocol for secure Internet of Drones communication," *IEEE Internet of Things J.*, Jun. 2025.

[77] X. Feng and B. Zhang, "Reputation evaluation scheme based on PUF and blockchain with channel congestion mitigation in the Internet of Vehicles," *IEEE Internet of Things J.*, Feb. 2025.

[78] M. S. Alkatheiri, Y. Zhuang, M. Korobkov, and A. R. Sangi, "An experimental study of the state-of-the-art PUFs implemented on FPGAs," *in 2017 IEEE Conf. Dependable and Secure Computing (DSC)*, pp. 174–180, Aug. 2017.

[79] A. Verma, S. Srivastava, and A. P. Shah, "Aging resilient and energy efficient ring oscillator for PUF design," *in Int. Symp. VLSI Design and Test*, Cham, Switzerland: Springer Nature, pp. 199–211, Jul. 2022.

[80] L. Lu, Y. Z. Chen, and T. T. Kim, “A configurable randomness enhanced RRAM PUF with biased current sensing scheme,” *in 2021 IEEE Int. Symp. Circuits Syst. (ISCAS)*, pp. 1–5, May 2021.

[81] K. H. Chuang, E. Bury, R. Degraeve, B. Kaczer, D. Linten, and I. Verbauwhede, “A physically unclonable function using soft oxide breakdown featuring 0% native BER and 51.8 fJ/bit in 40-nm CMOS,” *IEEE J. Solid-State Circuits,* vol. 54, no. 10, pp. 2765–2776, Jul. 2019.

[82] S. Taneja, V. K. Rajanna, and M. Alioto, “In-memory unified TRNG and multi-bit PUF for ubiquitous hardware security,” *IEEE J. Solid-State Circuits*, vol. 57, no. 1, pp. 153–166, Dec. 2021.

[83] J. Park and J. Y. Sim, “ A physically unclonable function combining a process mismatch amplifier in an oscillator collapse topology,” *in 2021 IEEE Int. Solid-State Circuits Conf. (ISSCC)*, vol. 64, pp. 504–506, Feb. 2021.

[84] K. Liu, X. Chen, H. Pu, and H. Shinohara, “A 0.5-V hybrid SRAM physically unclonable function using hot carrier injection burn-in for stability reinforcement,” *IEEE J. Solid-State Circuits*, vol. 56, no. 7, pp. 2193–2204, Nov. 2020.