Development and Analysis of a Physically Unclonable Function Circuit

Christina Olympia Soldatou

Diploma Thesis

Supervisor: Prof. Georgios Tsiatouhas

Ioannina, February 2025

ΤΜΉΜΑ ΜΗΧ. Η/Υ & ΠΛΗΡΟΦΟΡΙΚΉΣ
ΠΑΝΕΠΙΣΤΉΜΙΟ ΙΩΑΝΝΊΝΩΝ
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF IOANNINA

Acknowledgments

I dedicate this work to my family and my partner for their unwavering love, support, and belief in me. Their presence has been my guiding light and a source of strength throughout this journey. This work is a token of my deep appreciation for all they have done for me.

I would also like to express my heartfelt gratitude to my professor, Georgios Tsiatouhas, for his invaluable guidance, support, and knowledge throughout this process. Additionally, I extend my sincere thanks to Dimosthenis Georgoulas, on whose work this thesis is based, for his generous assistance and insights. Their contributions have been instrumental in shaping this work, and I am truly grateful.

Ioannina, February 2025

Christina Olympia Soldatou

Περίληψη

Σολδάτου Χριστίνα Ολυμπία, Δίπλωμα, Τμήμα Μηχανικών Η/Υ και Πληροφορικής, Πολυτεχνική Σχολή, Πανεπιστήμιο Ιωαννίνων, Φεβρουάριος 2025.

Μη Κλωνοποιήσιμες Φυσικές Συναρτήσεις σε Λειτουργία Ρεύματος: Ανάλυση και Αξιολόγηση.

Επιβλέπων: Γεώργιος Τσιατούχας, Καθηγητής.

Η ασφάλεια των ηλεκτρονικών συστημάτων αποτελεί βασική προτεραιότητα στη σύγχρονη εποχή, καθώς οι συσκευές IoT, τα συστήματα έξυπνου σπιτιού και οι φορητές συσκευές ενσωματώνονται ολοένα και περισσότερο στην καθημερινότητά μας. Η ραγδαία εξάπλωση αυτών των συστημάτων δημιουργεί αυξημένες απαιτήσεις για την προστασία της ιδιωτικότητας και την ακεραιότητα των δεδομένων. Μια από τις πιο ελπιδοφόρες τεχνολογίες για την ενίσχυση της ασφάλειας είναι οι Μη Κλωνοποιήσιμες Φυσικές Συναρτήσεις (PUFs). Οι PUFs αξιοποιούν τις μικρές, μη ελεγχόμενες διαφορές που προκύπτουν κατά τη διαδικασία κατασκευής ολοκληρωμένων κυκλωμάτων για τη δημιουργία μοναδικών «αποτυπωμάτων» τα οποία λειτουργούν ως κρυπτογραφικά κλειδιά. Η μη αποθήκευση αυτών των κλειδιών στη μνήμη καθιστά τα συστήματα πιο ανθεκτικά σε επιθέσεις, όπως ανάγνωση της μνήμης ή επιθέσεις ανάκτησης δεδομένων.

Ωστόσο, πολλές από τις υπάρχουσες υλοποιήσεις PUF παρουσιάζουν προβλήματα αξιοπιστίας, ειδικά εξαιτίας διακυμάνσεων της θερμοκρασίας και της τάσης τροφοδοσίας. Σε αυτή την εργασία, προτείνεται ένα νέο κύκλωμα PUF που βασίζεται στις διαφορές ρεύματος αντί των διαφορών τάσης, ώστε να βελτιωθεί η ανθεκτικότητα στις περιβαλλοντικές διακυμάνσεις. Η αξιολόγηση του προτεινόμενου κυκλώματος PUF πραγματοποιήθηκε με τη χρήση της τεχνολογίας CMOS στα 90nm της UMC. Ο σχεδιασμός και η προσομοίωση του PUF υλοποιήθηκαν στις πλατφόρμες Virtuoso και Spectre της Cadence. Ο σχεδιασμός περιλαμβάνει ένα πλέγμα από 256 γραμμές και 3 στήλες κυττάρων PUF, εκ των οποίων οι 128 γραμμές είναι ενεργές. Τα κύτταρα αυτά παράγουν ρεύματα τα οποία υπόκεινται σε τυχαίες διακυμάνσεις λόγω μεταβολών κατά τη διαδικασία κατασκευής και χρησιμοποιούνται για τη δημιουργία μοναδικών κλειδιών.

Για τη σύγκριση των παραγόμενων ρευμάτων, χρησιμοποιούνται συγκριτές ρεύματος. Κάθε συγκριτής συγκρίνει δύο στήλες του πλέγματος και καθορίζει τη «νικητήρια» στήλη βάσει του ισχυρότερου ρεύματος.

Η αξιολόγηση του προτεινόμενου κυκλώματος πραγματοποιήθηκε μέσω 5.000 προσομοιώσεων Monte-Carlo για κάθε συνδυασμό περιβαλλοντικών παραμέτρων (θερμοκρασία και τάση). Τα αποτελέσματα δείχνουν μέση αξιοπιστία 96.81% σε διακυμάνσεις τάσης και 98.04% σε μεταβολές θερμοκρασίας, με μέση μοναδικότητα 49.96% και ομοιομορφία 48.57%.

Λέξεις Κλειδιά: Μη Κλωνοποιήσιμες Φυσικές Συναρτήσεις (PUFs), Λειτουργία Ρεύματος, Ασφάλεια, Αξιοπιστία, Κρυπτογραφικά Κλειδιά, Συσκευές IoT, Ασφάλεια Υλικού, Συγκριτής Ρεύματος, Προσομοιώσεις Monte Carlo, Κατασκευαστικές Διακυμάνσεις.

Abstract

Soldatou Christina Olympia, Diploma, Department of Computer Science and Engineering, School of Engineering, University of Ioannina, February 2025.

Physically Unclonable Functions in Current Mode: Analysis and Evaluation.

Supervisor: Yiorgos Tsiatouhas, Professor.

The security of electronic systems is a key priority in the modern era, as IoT devices, smart home systems, and portable devices are increasingly integrated into our daily lives. The rapid expansion of these systems has created heightened demands for privacy protection and data integrity. One of the most promising technologies to enhance security is Physically Unclonable Functions (PUFs). PUFs exploit small, uncontrolled variations that occur during the manufacturing process of integrated circuits to create unique "fingerprints" that function as cryptographic keys. The fact that these keys are not stored in memory makes systems more resilient to attacks, such as memory readout and data recovery attacks.

However, many existing PUF implementations face reliability issues, especially under variations in temperature and supply voltage. This study proposes a novel PUF circuit that operates based on current differences rather than voltage differences, with improved reliability characteristics against environmental variations. For the evaluation of the proposed PUF circuit we utilized UMC's 90nm CMOS technology. The design and simulation of the PUF were conducted using Cadence's Virtuoso and Spectre platforms. The design includes an array of 256 rows and 3 columns of PUF cells, of which 128 rows are active. These cells generate currents that are subject to random fluctuations due to process variations and are used to generate unique cryptographic keys.

For the comparison of the generated currents, current mode comparators are utilized. Each comparator compares a pair of columns in the array and identifies the "winning" column based on the strongest current..

The evaluation of the proposed circuit was conducted through 5,000 Monte-Carlo simulations for each combination of environmental parameters (temperature and voltage). Results show an average

reliability of 96.81% with respect to power supply fluctuations and 98.04% with respect to temperature variations, along with a uniqueness of 49.96% and uniformity of 48.57% on average.

Keywords: Physically Unclonable Functions (PUFs), Current Mode Operation, Security, Reliability, Cryptographic Keys, IoT Devices, Hardware Security, Current Sensing Comparator, Monte Carlo Simulations, Process Variations.

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION **10**

1.1 Introduction 10

1.2 Research Objectives and Methodology 11

1.3 Thesis outline 11

CHAPTER 2. PHYSICAL UNCLONABLE FUNCTIONS **13**

2.1 Introduction to Physical Unclonable Functions (PUFs) 13

2.1.1 Definition and Purpose of PUFs 13

2.1.2 Fundamental Characteristics of PUFs 14

2.1.3 Applications of PUFs 14

2.2 Weak vs. Strong PUFs 15

2.2.1 Definition of Challenge-Response Pairs (CRPs) 16

2.2.2 Characteristics and Use Cases of Weak PUFs 16

2.2.3 Characteristics and Use Cases of Strong PUFs 16

2.2.4 Strength Determination 17

2.3 PUF Architectures 17

2.3.1 Delay-Based PUFs 17

2.3.1.1 Arbiter PUF (APUF) 17

2.3.1.2 Ring Oscillator PUF (RO-PUF) 18

2.3.2 Memory-Based PUFs 19

2.3.2.1 SRAM PUF 19

2.3.2.2 DRAM and GPU-based PUFs 20

2.3.3 Current-Based PUFs 21

2.3.3.1 Subthreshold Current Array (SCA-PUF) 21

2.3.3.2 Proportional to Absolute Temperature (PTAT) PUF 22

2.3.3.3 Two Chooses One (TCO-PUF) 25

2.3.4 Compute-in-Memory (CIM) PUFs 25

2.3.4.1 Bitline-based PUFs (e.g., SiCBit-PUF) 26

2.3.4.2 Compute-in-Memory (CIM) and PUF Integration 28

2.4 Security Threats and Vulnerabilities 30

2.4.1 Machine Learning (ML) Attacks 30

2.4.2 Side-Channel Attacks 30

2.4.3 Aging and Environmental Sensitivity 30

2.5 Evaluation Metrics of PUFs 31

2.5.1 Uniqueness 31

2.5.2 Uniformity 32

2.5.3 Reliability 33

2.5.4 Bit Error Rate (BER) 34

2.6 Summary 35

CHAPTER 3. PROPOSED CURRENT-MODE PUF ARCHITECTURE 36

3.1 PUF Cells 36

3.1.1 PUF Cells 36

3.1.2 Existing 6T PUF Cell Design 37

3.1.2.1 Schematic and Operational Principles 38

3.1.2.2 Strengths of the 6T PUF Design 38

3.1.3 Analysis of Initial 7T PUF Designs 39

3.1.3.1 First 7T PUF Design 39

3.1.3.2 Second 7T PUF Design 39

3.1.4 The Proposed 8T PUF Cell Design 40

3.2 PUF Array Architecture 41

CHAPTER 4. DESIGN AND SIMULATION RESULTS 44

4.1 Design 44

4.1.1 Buffers 44

4.1.2 The Comparators 45

4.1.2.1 The N Current Mode Comparator (NCMC) *45*

4.1.2.2 The P Current Mode Comparator (PCMC) *46*

4.2 Operation Phases 47

4.2.1 Discharge-Equalization Phase *48*

4.2.2 Activation Phase *48*

4.2.3 Sense Phase *49*

4.3 Final Layout Description 49

4.4 Simulation Results 50

4.4.1 Analysis of Environmental Factors *50*

4.4.2 Behavior and Timing Characteristics of the PUF *50*

4.4.3 Analysis and Selection of Transistors in the Design *52*

4.4.4 Performance Metrics and Reliability Analysis *54*

4.4.5 Power Consumption and Silicon Area Estimation *58*

4.4.6 Comparative Analysis with State-of-the-Art PUFs *59*

CHAPTER 5. CONCLUSIONS **60**

Bibliography **63**

CHAPTER 1

INTRODUCTION

1.1 Introduction

In an era where digital connectivity plays a central role in daily life, ensuring the security of electronic systems is essential. The widespread adoption of smart devices and Internet of Things (IoT) technology has introduced significant challenges in safeguarding data confidentiality, integrity, and availability. Security breaches in these systems can lead to devastating consequences, from privacy violations to potentially life-threatening incidents.

Numerous real-world examples illustrate the increasing sophistication of cyberattacks. For instance, hackers have taken control of web-connected baby monitors to spy on families, while in another high-profile incident, attackers remotely hacked a 2014 Jeep Cherokee [H18], demonstrating how vulnerabilities in connected technologies can be exploited to compromise user safety.

These incidents underscore the urgent need for robust hardware security solutions, especially for critical applications such as financial transactions, biometric access systems, and connected vehicles. However, designing secure hardware is a complex undertaking due to the sheer scale of modern electronic systems, which often feature billions of transistors and complex component interactions.

One promising approach to enhancing security is the use of Physical Unclonable Functions (PUFs), which exploit natural variations in hardware manufacturing processes to generate unique outputs that can serve as cryptographic keys. Unlike traditional methods, PUFs eliminate the need to store

sensitive information in memory. However, despite their potential, PUF circuits are susceptible to fluctuations in environmental conditions, such as changes in power supply voltage and temperature, which can impact their reliability.

1.2 Research Objectives and Methodology

The main goal of this thesis is to highlight the crucial role of current-mode PUFs in ensuring data security and protecting sensitive information, particularly by enhancing their reliability under varying voltage conditions. To overcome the limitations of traditional designs, this research introduces a current-mode PUF architecture that shifts away from the conventional voltage-based approach. The proposed design utilizes an array of cells acting as current generators, specifically engineered to reduce dependence on power supply variations and improve overall reliability . By arranging these cells in a matrix configuration, the architecture aims to produce a robust PUF capable of generating a large number of Challenge-Response Pairs (CRPs) while maintaining low power consumption and minimal response latency. This design improves resilience and makes the PUF highly suitable for security-critical applications that require frequent on-demand cryptographic key generation.

To assess the performance of the proposed PUF, extensive simulations were carried out under a wide range of environmental conditions. These included a temperature of **0°C** with supply voltage combinations of **1.1V** and **0.9V**, a nominal condition of **27°C** with a supply voltage of **1V**, and a temperature of **80°C** with supply voltage combinations of **1.1V** and **0.9V**. The simulations used various activation patterns within a 256-row array, with 128 rows activated per challenge. A total of 25 simulation sessions were performed, with each session consisting of 5,000 Monte Carlo iterations to ensure comprehensive testing across different scenarios. The results of these simulations were used to evaluate key metrics such as reliability, uniqueness, uniformity, power consumption, and latency. Additionally, the performance of the proposed current-mode PUF was compared against state-of-the-art PUF architectures to demonstrate its efficiency .

1.3 Thesis outline

The thesis is structured as follows:

Chapter 2: Physical Unclonable Functions (PUFs)

This chapter introduces the concept of PUFs, their fundamental characteristics, and applications. It discusses the classification of PUFs into weak and strong types, intrinsic and extrinsic designs, and highlights various PUF architectures such as delay-based, memory-based, and current-based PUFs. Additionally, it discusses key security threats, evaluation metrics (e.g., uniqueness, reliability, and uniformity), and compares different PUF implementations.

Chapter 3: The proposed Current-Mode PUF

This chapter focuses on the proposed current-mode PUF design. It includes a detailed discussion of its main components, such as current-generation cells, buffers, and comparators, along with the operational phases of the circuit. The transistor-level design is analyzed to demonstrate the mechanisms contributing to the performance and robustness of the PUF.

Chapter 4: Simulation Results and Discussion

In this chapter, the results from Monte Carlo simulations under varying environmental conditions are presented and analyzed. Key performance metrics, including reliability, uniqueness, uniformity, area, power consumption, and latency, are evaluated. The performance of the proposed design is compared with existing state-of-the-art PUF architectures to highlight its advantages.

Chapter 5: Conclusions and Future Work

The thesis concludes with a summary of the research findings, emphasizing the contributions of the proposed PUF design.

CHAPTER 2

PHYSICAL UNCLONABLE FUNCTIONS

2.1 Introduction to Physical Unclonable Functions (PUFs)

2.1.1 Definition and Purpose of PUFs

A **Physical Unclonable Function (PUF)** is a hardware security primitive that leverages inherent physical variations introduced during the manufacturing process of integrated circuits (ICs) to generate unique, device-specific responses.These responses are generated when a specific digital input, known as a challenge, is applied to the PUF, producing a corresponding output. As Böhm and Hofer state, *"the input (challenge) may alter the internal combination of the mismatching components, which changes the output (response)"* [BH12]. Unlike traditional key storage mechanisms that store cryptographic keys in memory, PUFs eliminate the need for persistent key storage, as the response is dynamically generated from the device's physical characteristics.

The purpose of PUFs is to enhance the security of electronic systems by providing a robust mechanism for device authentication, secure key generation, and identification. Their reliance on the unique randomness of hardware makes them resistant to cloning and reverse engineering, providing a physical "fingerprint" for each device. According to Maes,

"PUFs serve as a physical root of trust to enable various higher-level security operations" [M12].

PUFs have become a key technology in hardware security due to their lightweight implementation and ability to generate cryptographic secrets without requiring non-volatile memory storage. By leveraging the physical characteristics of the device, PUFs create a secure and cost-effective solution for Internet of Things (IoT) devices, embedded systems, and security-sensitive applications, where hardware-based security is essential.

2.1.2 Fundamental Characteristics of PUFs

The effectiveness of a PUF depends on three key characteristics: unclonability, randomness, and reliability.

- **Unclonability**: Unclonability refers to the inability to replicate the physical properties that define a PUF, even if the exact manufacturing process is replicated. As Li and Seok note, *"This type of PUF is also known as Physically Obfuscated Key (POK)"* [LS16]. This characteristic arises from the inevitable variations introduced during semiconductor fabrication, which are random and unique for each chip. These variations occur at the microscopic level and cannot be controlled or predicted, making each PUF response distinct and unrepeatable.
- **Randomness**: Randomness measures how unpredictable and unbiased the responses of a PUF are when subjected to different challenges. Herder et al. describe that *"a strong PUF can support a large enough number of challenges such that complete determination/measurement of all challenge–response pairs (CRPs) within a limited timeframe is not feasible"* [HYKD14]. An ideal PUF should produce responses that are equally distributed between 0s and 1s, ensuring that responses do not exhibit any exploitable patterns.
- **Reliability**: Reliability defines the PUF's ability to produce consistent responses under varying environmental conditions, such as changes in temperature, supply voltage, and aging effects. High reliability is crucial to avoid authentication errors or failed key generation, making error correction a key design feature.

2.1.3 Applications of PUFs

1. **Authentication**

   PUFs play a vital role in device authentication, where the goal is to verify the identity of a device without the need for storing static secret keys. By using challenge-response pairs (CRPs), PUFs enable secure authentication protocols in which a verifier sends a random challenge to the device, and the device responds with a unique response generated by the PUF. Since the response is derived from the physical characteristics of the chip, it is infeasible for an adversary to reproduce or predict the correct response without access to the original device. This makes PUFs an attractive solution for securing Internet of Things (IoT) devices, smart cards, and secure access systems.

2. **Cryptographic Key Generation**

   PUFs can be used to generate cryptographic keys dynamically, eliminating the need for long-term key storage in non-volatile memory. Instead of storing a key, the device reconstructs it on demand by applying a specific challenge to the PUF and using the resulting response as the key. This approach enhances security by minimizing the risk of key extraction through physical attacks, such as side-channel analysis or invasive probing. Additionally, the inherent uniqueness of PUF responses ensures that each device generates a distinct cryptographic key, further strengthening system security.

3. **Integrated Circuit (IC) Identification**

   The unique and unclonable nature of PUFs makes them ideal for identifying and tracking individual ICs. Each IC, embedded with a PUF, can be assigned a unique identifier based on its PUF response. This identifier can be used for various purposes, such as supply chain management, counterfeit detection, and intellectual property protection. By embedding PUF-based identifiers in hardware, manufacturers can ensure the authenticity and integrity of their products throughout their lifecycle.

2.2 Weak vs. Strong PUFs

PUFs are classified based on their ability to generate Challenge-Response Pairs (CRPs), which form the foundation of their security and functionality. This classification broadly divides PUFs into Weak and Strong, depending on the number of CRPs they can produce, as well as their application scenarios.

Weak PUFs are limited in the number of CRPs they can generate, making them more susceptible to tampering and brute force attacks [HYKD14]. In contrast, Strong PUFs are identified by the exponential scaling of their CRPs, while linear or polynomial scaling is typical of Weak PUFs [MYWR19].

Strong PUFs include digital and memory-based types, such as SRAM-based PUFs that leverage the inherent random variations in SRAM cells [XTT23][CWZ+23][LYK22]. They are distinguished by their enhanced unclonability, as it is not feasible to fully determine or measure all CRPs within a limited timeframe [HYKD14].

2.2.1 Definition of Challenge-Response Pairs (CRPs)

PUFs function by mapping a unique challenge (input) to a corresponding response (output), forming Challenge-Response Pairs (CRPs). These CRPs are central to PUF classification and are used to evaluate their strength and applicability. A strong PUF generates a vast number of unique CRPs, making it suitable for robust security applications, whereas a weak PUF has a limited set of CRPs and is often used in less complex scenarios such as key storage.

2.2.2 Characteristics and Use Cases of Weak PUFs

Weak PUFs are designed to generate a small number of CRPs, sometimes even just one, making them simpler but less versatile in security applications. This type of PUF is often referred to as a **Physically Obfuscated Key (POK)** [LS16] due to its limited capability. Weak PUFs are vulnerable to brute force and tampering attacks because the low number of CRPs can be easily enumerated or cloned. Despite these limitations, weak PUFs are widely employed for **cryptographic key generation** and **device identification**, where the low computational overhead is an advantage.

2.2.3 Characteristics and Use Cases of Strong PUFs

Strong PUFs generate an exponentially large number of Challenge-Response Pairs (CRPs), making it computationally infeasible for adversaries to clone or enumerate all possible CRPs. As McGrath et al. explain, *"if the number of CRPs scales exponentially, the PUF is considered strong, while linear or polynomial increment typically corresponds to weak PUFs*"[MYWR19]. This scalability makes strong PUFs ideal for applications like hardware authentication, particularly in IoT devices and low-power systems, where secure direct authentication without cryptographic algorithms is needed.

Strong PUFs incorporate non-linear behaviors or complex architectures, such as Arbiter PUFs and **Ring Oscillator PUFs (RO-PUFs)**, to enhance unpredictability and attack resistance. However, early strong PUFs, like the **Arbiter PUF,** were vulnerable to Machine Learning (ML) attacks. Advanced designs, such as **feed-forward PUFs** and **XOR-based PUFs**, address these vulnerabilities by introducing non-linear behaviors, ensuring high unclonability and resilience against attacks.

2.2.4 Strength Determination

The strength of a PUF is determined by the scaling of CRPs with its size. Weak PUFs typically exhibit a linear or polynomial growth in CRPs, while Strong PUFs scale exponentially. Additionally, Strong PUFs must ensure high unclonability and unpredictability to withstand attacks. While early Strong PUFs, such as Arbiter PUFs, faced vulnerabilities to ML attacks, improved designs have mitigated these threats by incorporating non-linear responses.

2.3 PUF Architectures

2.3.1 Delay-Based PUFs

Delay-based PUFs are one of the earliest and most widely used architectures for implementing strong PUFs. These architectures exploit the inherent variations in manufacturing processes to generate unique and unpredictable responses.

2.3.1.1 Arbiter PUF (APUF)

The Arbiter PUF is proposed in [MMT20], and it is a classic delay-based PUF architecture that compares the delays of two identical paths within an integrated circuit. A challenge input configures a series of switches, altering the paths' configuration. The faster path is determined using an arbiter, typically implemented as a latch, which generates a 1-bit output.

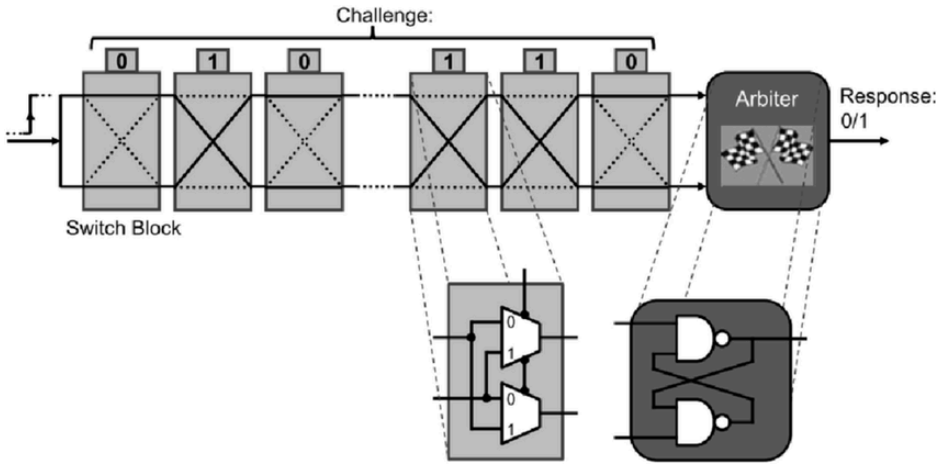

Figure 2.1: The structure of the Arbiter PUF [LG+04].

Arbiter PUFs are highly scalable in terms of the number of challenge-response pairs (CRPs), as they allow a large input space for generating responses. However, they are vulnerable to machine learning (ML) attacks due to the linear relationship between input challenges and output responses. Enhancements such as feed-forward configurations and XOR-based Arbiter PUFs have been proposed to mitigate these vulnerabilities, though they may impact robustness and power consumption.

2.3.1.2 Ring Oscillator PUF (RO-PUF)

The Ring Oscillator PUF relies on frequency differences between multiple ring oscillators to generate a response. In this design, the challenge selects two oscillators, and their frequency comparison determines the output bit. The randomness arises from process variations that affect the oscillators' frequencies.

RO-PUFs [SD07] are considered robust and offer better resistance to environmental variations like temperature and voltage fluctuations. They are also more resistant to ML attacks compared to basic Arbiter PUFs. However, the scalability of their CRPs is lower, as the number of CRPs depends on the number of oscillators available on the chip. Despite this limitation, RO-PUFs are widely adopted for their simplicity and reliability.

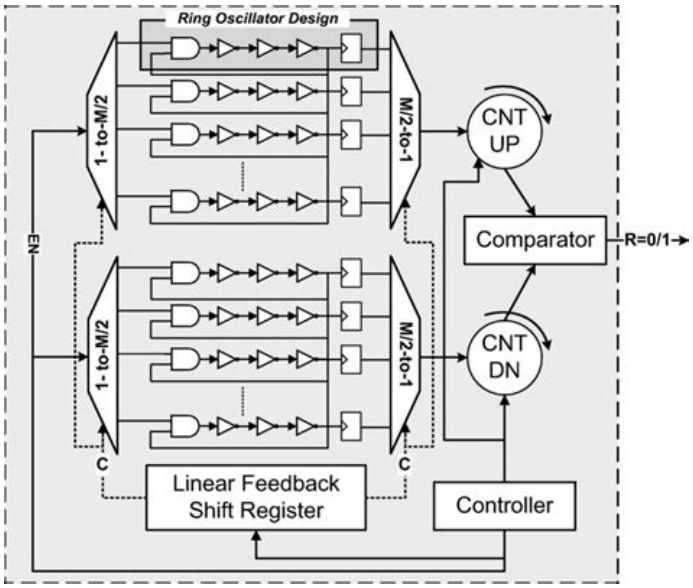

Figure 2.2: The ring oscillator based PUF design consists of M ring oscillators. The input and output can be represented as a tuple of challenge-response pair (C, R). The challenges have applied using a maximal length LFSR design [CSM19].

Both architectures exemplify the use of delay variations to establish unique device fingerprints. While they have strengths, such as scalability (APUF) and robustness (RO-PUF), their vulnerabilities to modeling attacks have prompted the development of alternative PUF designs, such as current-based and memory-based PUFs.

2.3.2 Memory-Based PUFs

Memory-based PUFs rely on intrinsic process variations in memory cells, such as SRAM or DRAM, to generate unique responses. These architectures take advantage of the start-up behavior or access patterns of memory cells, making them an efficient choice for reusing existing hardware components.

2.3.2.1 SRAM PUF

SRAM-based PUFs (Static Random-Access Memory PUF [SD07]) exploit the power-up state of SRAM cells. Each cell randomly settles to either a 0 or 1 state due to variations in transistor thresholds during manufacturing. This randomness creates a distinct, device-specific fingerprint. These PUFs are commonly used in authentication and cryptographic key generation applications, particularly for IoT devices, due to their high reliability and ease of integration.

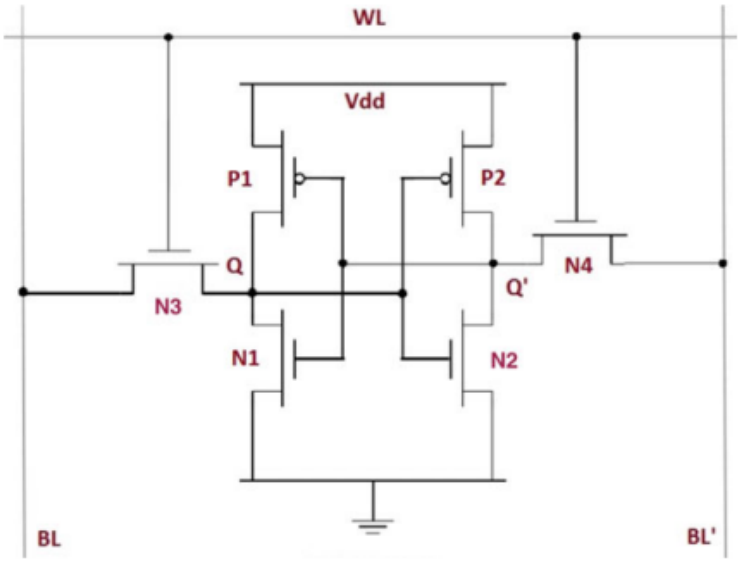

Figure 2.3: A generic 6-transistor SRAM cell [H18].

2.3.2.2 DRAM and GPU-based PUFs

DRAM-based PUFs (Dynamic Random Access Memory [S+17]) utilize variations in the access or refresh operations of memory cells to generate unique responses. Similarly, GPU-based PUFs harness the intrinsic variations in memory components of graphical processing units to produce PUF responses.

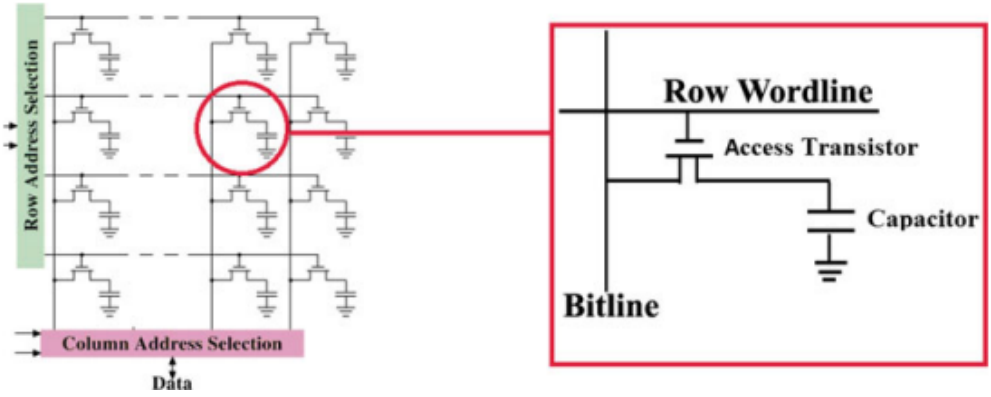

Figure 2.4: A generic structure for a DRAM cell [H18]

Both architectures are advantageous in scenarios requiring re-purposing of existing memory blocks but may introduce latency and require modifications to memory topology.

2.3.3 Current-Based PUFs

Current-based PUFs generate responses by leveraging current variations caused by transistor mismatches. These designs are valued for their compact area and power efficiency.

2.3.3.1 Subthreshold Current Array (SCA-PUF)

The Subthreshold Current Array (SCA-PUF) [ZZNS19] is a robust current-mode PUF designed to leverage subthreshold transistor operation and process-induced variations for secure response generation. It consists of two $n\,x\,k$ arrays (SCA_a and SCA_b), a common-mode feedback (CMFB) circuit, and a comparator. The arrays are driven by the same challenge inputs (C_{ij}).

Each unit cell within the arrays contains:

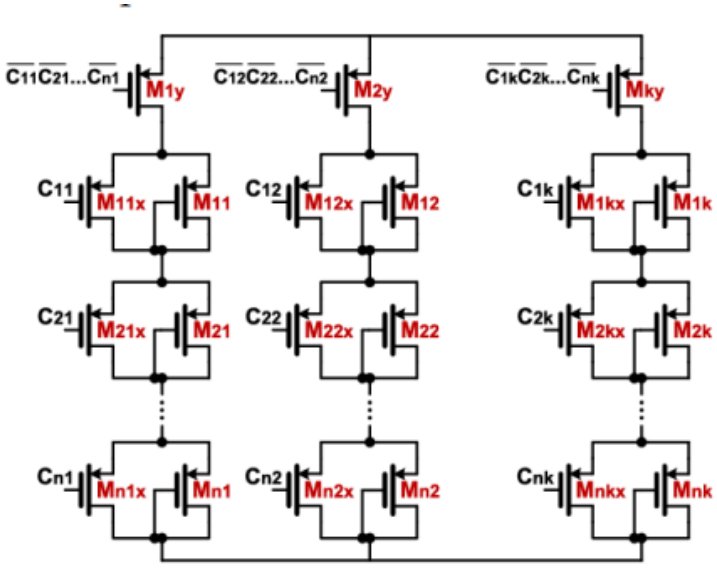

Figure 2.5: The subthreshold current array consists of n rows and k columns of controllable unit cells.[ZZNS19].

- **Stochastic Transistors (Mij):** Operate in the subthreshold region and exhibit high VthV_{th}Vth variability, introducing randomness.
- **Non-Stochastic Switches (Mijx):** Sized to ensure consistent behavior, controlled by the challenge signals (Cij).

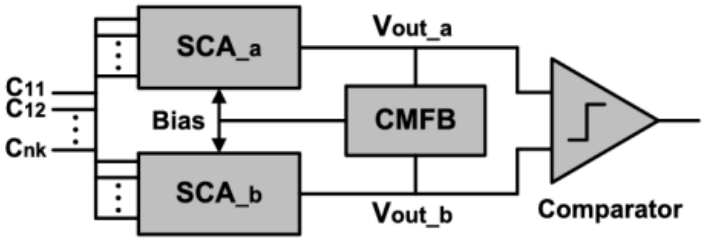

Figure 2.6: The architecture of SCA-PUF consisting of a pair of arrays, a comparator, and a common-mode feedback (CMFB) circuit [ZZNS19].

When Cij=1, the stochastic transistors contribute to the output voltage. Due to process variations, the two arrays produce slightly different output voltages, which are compared to generate a binary response.

This architecture is resistant to machine learning attacks, efficient in power consumption, and robust under varying environmental conditions, making it ideal for IoT and secure hardware applications.

2.3.3.2 Proportional to Absolute Temperature (PTAT) PUF

In [LS16], an alternative current-mode PUF design is introduced, which significantly differs from the earlier SCA-PUF architecture. The PTAT PUF leverages the principle of proportional-to-absolute-temperature voltage generation for creating a robust and reliable physically unclonable function. This PUF architecture is based on an array of bit cells, each consisting of transistors operating in the subthreshold region, and is particularly noted for its high reliability across a wide range of temperatures and supply voltages.

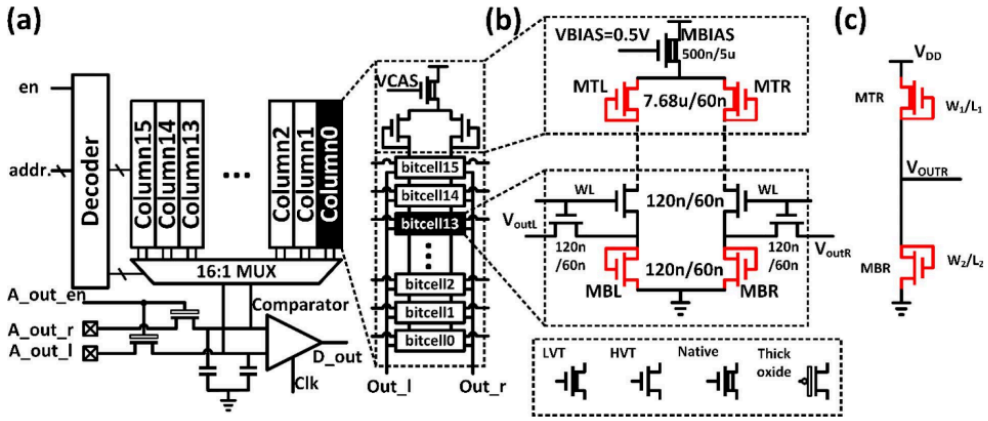

Figure 2.7: (a) Proposed 256-bit PUF. It is composed of a bitcell array, an address decoder, an analog multiplexer, and a 1-bit comparator. (b) A bitcell and a shared header in a column. (c) A PTAT generator, two of which form a single PUF bitcell [LS16].

Architecture

The PTAT PUF, as shown in the reference figure, is composed of:

- **Bitcell Array:** Each bitcell contains four transistors, organized in a differential structure to exploit mismatch variations between transistors.
- **PTAT Generator:** Each bitcell includes a PTAT voltage generator consisting of transistors MTL, MTR, MBL, and MBR, which operate in the subthreshold region.
- **Decoder and Multiplexer:** Used to address specific bit cells within the array.
- **1-bit Comparator:** A classic sense amplifier with a PMOS differential pair and an NMOS cross-coupled latch, which outputs the digital response based on the voltage difference.

Operation

The PTAT voltage is generated based on the subthreshold current equation:

$$I_{sub} = \mu C_{ox} \frac{W}{L} (m - 1) V_t^2 \, exp(\frac{V_{gs} - V_{th}}{m V_t})(1 - exp(-\frac{V_{ds}}{V_t}))$$

Here, V_t mismatch among transistors is utilized to create random and unclonable responses. The current generated by transistors is highly dependent on process variations, particularly threshold voltage (Vth) differences, while remaining robust to environmental conditions.

The output voltage (V_{OUT}) of the PTAT generator can be calculated as:

$$V_{OUT} = V_{th2} - \frac{m_2}{m_1} V_{th1} + K_{Vth}(T - T_0) + \textit{temperature-independent terms}$$

Features

- **High Reliability:** The PTAT PUF achieves a reliability of 99.55% across temperatures from 0°C to 80°C and supply voltages ranging from 0.6V to 1.2V.
- **Temperature Independence:** Due to its PTAT operation, it effectively compensates for temperature variations.
- **Small Area:** The array-like structure enables compact implementation, reducing the silicon footprint.
- **Robustness:** The symmetric layout and differential design minimize environmental impact and process-induced asymmetries.

Advantages for Hardware Security

The PTAT PUF's capability to generate unique responses based on physical variations in silicon makes it ideal for use in secure hardware systems. Its strong reliability and environmental robustness ensure consistent operation under varying conditions, which is critical for applications such as cryptographic key storage and device authentication.

In the context of your thesis, the PTAT PUF's reliance on subthreshold operation and precise thermal compensation mechanisms provides a solid foundation for further exploration of

current-mode PUF architectures. The inherent randomness in its response generation process, combined with robust operational stability, makes it a promising candidate for enhancing the security of integrated circuits.

2.3.3.3 Two Chooses One (TCO-PUF)

The Two Chooses One (TCO-PUF) [MHCZ15] is a subthreshold physical unclonable function designed to enhance the practicality and performance of subthreshold current array (SCA) PUFs. It leverages the stochastic characteristics of transistors operating in the subthreshold region, which are highly sensitive to threshold voltage variations, to improve reliability and output voltage range.

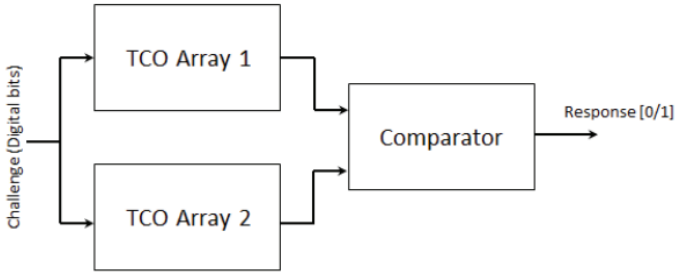

Figure 2.8: Top level of TCO-PUF architecture [MHCZ15].

The TCO-PUF architecture consists of two identical transistor arrays, each with stochastic and non-stochastic transistors. The stochastic transistors, with deliberately maximized variability, contribute to the randomness required for unique PUF responses. The "Two Chooses One" mechanism ensures a stochastic transistor is always active for each challenge bit, enhancing variability and robustness. A built-in voltage divider mechanism stabilizes the output voltage, ensuring compatibility with conventional comparators.

The TCO-PUF achieves a uniqueness of approximately 50.23% and a reliability of 91.58% under wide environmental conditions, including temperatures from **-40°C** to **125°C** and supply voltages from **0.9V** to **1.1V**. Its enhanced design also resists machine learning attacks through the non-linear behavior of subthreshold currents, making it a secure and practical solution for hardware authentication and identification.

2.3.4 Compute-in-Memory (CIM) PUFs

Compute-in-Memory (CIM) architectures are emerging as a transformative approach to addressing the growing computational and energy demands of edge computing and deep neural networks (DNNs). Unlike traditional Von Neumann architectures, which separate storage and computation, CIM allows computations to occur directly within the memory, minimizing data transfer bottlenecks and significantly reducing power consumption. This paradigm shift has paved the way for innovations such as PUF-CIM, which combines the security capabilities of Physical Unclonable Functions (PUFs) with the efficiency of CIM.

The Role of CIM in Modern Computing

In conventional systems, memory components such as SRAM are primarily used for data storage. During computation, data must travel back and forth between the memory and the Arithmetic Logic Unit (ALU), creating a bottleneck in terms of transfer rates, latency, and power consumption. CIM addresses these challenges by enabling the execution of basic computations, such as dot products or XOR operations, directly within the memory cells.

Neural network operations, like dot products (multiplying input and weight vectors) and XOR operations (binary multiplications), are simple and computationally efficient, making them ideal for CIM architectures.

2.3.4.1 Bitline-based PUFs (e.g., SiCBit-PUF)

Bitline-based PUFs, exemplified by the SiCBit-PUF, leverage the intrinsic properties of SRAM bitlines to generate unique and unclonable responses. These PUFs operate on the principle of systematic bitflips occurring during computations in-memory, which are induced by the simultaneous activation of SRAM wordlines. Unlike traditional SRAM operations, where a single wordline is activated, bitline-based PUFs exploit concurrent wordline activations to create collisions along the bitlines, forming a reliable entropy source.

Architecture

The SiCBit-PUF was proposed as a **Strong In-Cache Bitflip PUF (SiCBit-PUF)** by the authors in [XTT23]. It is designed using a standard 6T SRAM array, where multiple SRAM cells share common bitlines. The novelty lies in activating multiple wordlines

simultaneously, which causes collisions on the shared bitlines. These collisions result in systematic and reproducible bitflips that are dependent on the physical properties and process variations of the SRAM array.

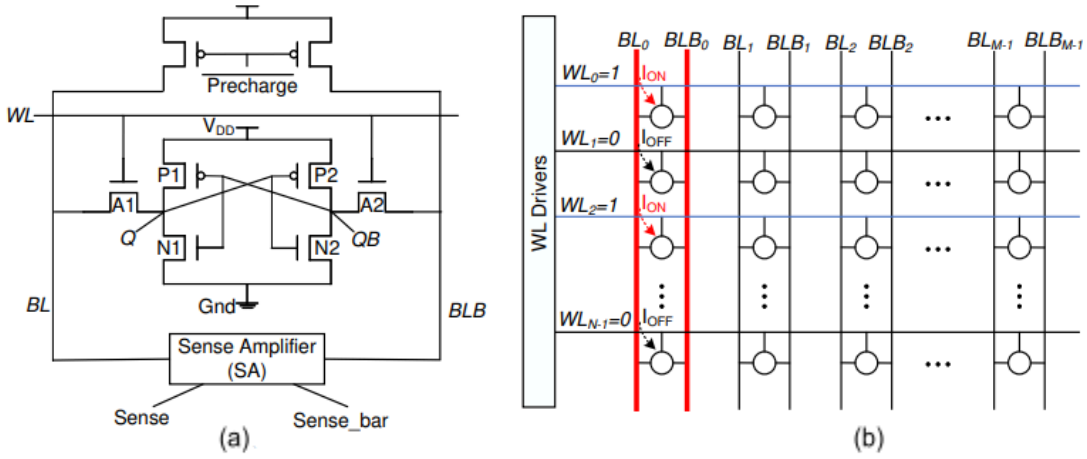

Figure 2.9: (a) 6T SRAM cell; (b) Bitline Computing Architecture [XTT23].

Key Features

1. **Systematic Bitflips**: The SiCBit-PUF generates predictable and repeatable bitflips by leveraging process variations during concurrent wordline activation. This ensures security and reliability in PUF responses.
2. **Strong PUF Characteristics**: With a high Challenge-Response Pair (CRP) density, the SiCBit-PUF is classified as a strong PUF, capable of handling exponentially increasing CRPs for secure hardware authentication.
3. **Low Overhead**: The SiCBit-PUF reuses existing SRAM structures, minimizing area and power overhead while achieving high-security performance.
4. **High Robustness**: The SiCBit-PUF demonstrates consistent and reliable responses under varying environmental conditions, including temperature changes (0°C–100°C) and voltage fluctuations (±10%).

Performance Metrics

- **Uniqueness**: The SiCBit-PUF achieves a near-optimal uniqueness of 50%, ensuring highly distinguishable responses across PUF instances.

- **Uniformity**: Responses are well-balanced, with uniformity metrics close to the ideal value of 50%.
- **Reliability**: The PUF exhibits excellent reliability, with response stability above 97.4% under temperature variations and 95.2% under voltage noise.

Bitline-based PUFs like the SiCBit-PUF are particularly promising in computing in-memory and System-on-Chip (SoC) designs. By reusing existing memory structures, they offer a cost-effective, low-latency solution for secure key generation and hardware authentication, enhancing the overall security of modern computing systems.

2.3.4.2 Compute-in-Memory (CIM) and PUF Integration

Integration of PUF in CIM: PUF-CIM

An interesting concept of a PUF-CIM has been introduced, which leverages SRAM for both computation and security purposes. The design integrates CIM functionality into SRAM cells, enabling lightweight DNN model protection and secure computation. By incorporating PUFs into CIM, this approach ensures the confidentiality of neural network models while reducing the reliance on external cryptographic mechanisms [CWZ+23].

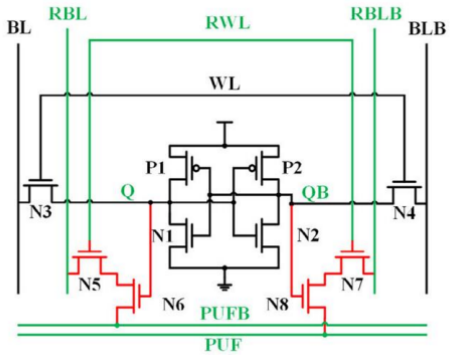

Figure 2.10: The 10T SRAM cell [CWZ+23].

The proposed architecture uses specially designed SRAM cells capable of performing XOR-based encryption for securing DNN weights. This dual functionality ensures that the SRAM not only stores data but also serves as a secure computation engine, protecting sensitive information from attacks like reverse engineering or side-channel analysis.

Key Features of PUF-CIM:

- **Weight Encryption:** Neural network weights stored in SRAM are encrypted using PUF-generated keys to ensure model confidentiality. The encrypted weight is computed as:

$$\overline{W_e} = \overline{W} \oplus PUF$$

  where $\overline{W_e}$ is the encrypted weight, $\overline{W}$ is the original weight, and PUF is the *PUF* response.

- **Binary Multiplication:** Neural network operations, such as binary multiplications, are performed in-memory using the equation:

$$M = IN \cdot (\overline{W_e} \oplus PUF) = IN \cdot \overline{W}$$

  where *IN* is the input vector and *M* is the result of the operation.

- **Time-to-Digital Converter (TDC):** The TDC generates PUF responses by calculating discharge rate differences within SRAM cells, ensuring unique, stable, and reliable PUF values.
- **Enhanced Security:** PUF integration and XOR encryption protect against tampering and cloning, securing neural network weights.

The integration of Compute-in-Memory (CIM) and Physical Unclonable Functions (PUFs) presents significant advantages in applications like edge computing, where lightweight DNNs benefit from efficient and secure operations, and IoT security, where the architecture enables secure key generation and data processing. Additionally, the embedded encryption mechanism ensures the confidentiality of neural network models, protecting intellectual property.

Despite its promise, PUF-CIM faces challenges such as managing tradeoffs between CRP density, area overhead, and Bit Error Rate (BER). Scalability remains a concern for adapting the architecture to larger DNN models, while maintaining reliability under varying environmental conditions is critical for consistent performance.

2.4 Security Threats and Vulnerabilities

In this section, we explore the key security challenges associated with Physical Unclonable Functions (PUFs), focusing on machine learning-based attacks, side-channel vulnerabilities, and environmental factors affecting PUF reliability.

2.4.1 Machine Learning (ML) Attacks

Machine learning (ML) techniques, such as Support Vector Machines (SVM) and Logistic Regression, have emerged as powerful tools for modeling PUF behavior. These attacks exploit the predictable response patterns of some PUF architectures, such as Arbiter PUFs, by training ML models on collected Challenge-Response Pairs (CRPs). For example, the linear delay differences in Arbiter PUFs make them susceptible to being mathematically modeled, rendering their responses predictable. Despite efforts to introduce non-linearities, such as XOR-PUFs and Feed-Forward PUFs, ML attacks remain a significant threat, especially when adversaries gather a substantial number of CRPs.

2.4.2 Side-Channel Attacks

Side-channel attacks target the physical implementation of PUFs rather than their logical structure. These attacks can be classified into passive and active types. Passive side-channel attacks, such as power and timing analysis, involve monitoring the power consumption or operation timing of the PUF during normal operation to infer its response. Active attacks, like fault injection, deliberately disrupt the PUF's operation by altering environmental conditions, such as temperature or voltage, to extract sensitive information. For instance, modifying the power supply can force the PUF into a predictable state, compromising its security.

2.4.3 Aging and Environmental Sensitivity

PUF responses are influenced by environmental factors such as temperature, voltage, and device aging. For example, variations in temperature can cause inconsistencies in PUF responses, reducing their reliability. Similarly, aging effects, like transistor wear-out, can alter the intrinsic variability exploited by PUFs, potentially leading to degraded performance

over time. Mitigation strategies include differential reading techniques and the design of PUF circuits with compensation mechanisms to enhance stability under varying conditions.

By addressing these vulnerabilities, PUF designs can achieve greater robustness, ensuring their utility as secure hardware primitives in authentication and cryptographic applications.

2.5 Evaluation Metrics of PUFs

The evaluation of Physically Unclonable Functions (PUFs) is critical to assess their performance and ensure their suitability for secure applications. Several key metrics have been established to quantify the quality and reliability of a PUF. These include **Uniqueness**, **Reliability**, and **Uniformity**, which are defined based on the structural properties of the generated responses, such as **Hamming Distance** and **Hamming Weight**. Each of these metrics offers insights into how a PUF performs under different conditions and aids in comparing it to other implementations.

Hamming Distance and Hamming Weight

The **Hamming Distance (HD)** measures the difference between two binary words of equal length by counting the number of positions where the corresponding bits differ. For a binary word $a = (a_1, a_2, \dots, a_n)$ and $b = (b_1, b_2, \dots, b_n)$, the Hamming Distance is defined as: $d(a, b) = \sum_{i=1}^{n} (a_i \oplus b_i)$ where $\oplus$ denotes the XOR operation.

The **Hamming Weight (HW)** of a binary word aaa is the number of non-zero bits, defined as: $HW(a)=d(a, 0)$. These metrics form the foundation for the calculation of Uniqueness, Reliability, and Uniformity.

2.5.1 Uniqueness

Uniqueness measures the ability of a PUF to generate responses that are uniquely distinguishable across different chips. It ensures that no two chips produce the same output for the same input challenge, reflecting the physical variability in the manufacturing process.

The metric is calculated using the **Inter-chip Hamming Distance (HD)** between the responses of different PUF instances $R_i(n)$ and $R_j(n)$ to the same challenge:

$$HD_{INTER} = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(R_i(n), R_j(n))}{n} \times 100\%$$

where k is the number of chips, and n is the length of the response.

Ideally, Uniqueness should approach **50%**, indicating maximum distinguishability. For example, if two instances of a PUF generate responses with a Hamming Distance of 50% of the total response length, they are considered highly unique. This property is crucial for applications such as device authentication, where unique identifiers are necessary to differentiate between devices [H18].

2.5.2 Uniformity

Uniformity evaluates the balance between 0s and 1s in the response bits generated by a PUF for a given challenge. It ensures that the responses are unbiased and equally distributed, which is crucial for maintaining randomness and preventing predictability.

Uniformity is defined as the proportion of 1s in the total response bits of a PUF. For a PUF response of n-bits, where r_i represents the Hamming Weight of the i^{th} response. Uniformity can be calculated using the formula:

$$\text{Uniformity} = \frac{1}{k} \sum_{i=1}^{k} \frac{r_i}{n} \times 100\%$$

where:

- k is the total number of responses,
- r_i is the number of 1s in the i^{th} response,
- n is the total number of bits in the response.

The ideal Uniformity value is **50%**, which indicates a perfectly balanced distribution of 0s and 1s. This balance ensures that the PUF responses are random and not biased toward a specific bit value.

Importance of Uniformity

1. **Randomness**: A uniform response distribution ensures that the PUF outputs exhibit high randomness, making them resistant to attacks that exploit predictable patterns.
2. **Robustness**: Uniformity contributes to the robustness of cryptographic systems by reducing the likelihood of response predictability.
3. **Security**: Balanced responses help to enhance security by preventing an adversary from inferring a bias in the generated outputs.

Deviations from Ideal Uniformity

If Uniformity deviates significantly from 50%, it indicates a bias in the PUF's response generation mechanism. Such biases can arise due to:

- Variations in manufacturing processes,
- Environmental factors such as temperature and voltage fluctuations,
- Design inefficiencies in the PUF architecture.

To mitigate deviations, techniques like differential reading or bias correction mechanisms can be employed, ensuring the Uniformity of PUF responses remains close to the ideal value [H18].

2.5.3 Reliability

Reliability is a critical evaluation metric that determines the consistency of a PUF's responses under varying environmental conditions, such as changes in temperature, voltage, and aging. It is essential for ensuring the robustness and stability of the PUF in practical applications, where environmental fluctuations are unavoidable.

The reliability metric is calculated using the **Intra-chip Hamming Distance (HD)**. This measures the variation in responses generated by a single PUF instance when subjected to

the same challenge C, across different environmental conditions. Mathematically, it is expressed as:

$$HD_{INTER} = \frac{1}{k} \sum_{i=1}^{k} \frac{HD(R_i(n), R_i^{'}(n))}{n} \times 100\%$$

where:

- $R_i(n)$ is the reference response of the i-th PUF instance under nominal conditions,
- $R_i^{'}(n)$ is the response of the same PUF under varying conditions,
- n is the length of the response, and k is the number of PUF instances evaluated.

The **Reliability** is then defined as:

$$Reliability = 100\% - HD_{INTRA}$$

An ideal PUF should exhibit a reliability value close to 100%, indicating minimal variation in its responses across different environmental conditions. This high reliability ensures that the PUF can generate consistent and repeatable challenge-response pairs, which is crucial for applications like secure authentication and key generation.

In practical terms, deviations from 100% reliability can occur due to noise, process variations, or extreme environmental conditions. Mitigation strategies, such as error correction codes and differential sensing, are often employed to enhance reliability and ensure the PUF's performance remains robust in real-world scenarios[H18].

2.5.4 Bit Error Rate (BER)

Definition: The Bit Error Rate (BER) measures the proportion of incorrect or altered bits in a PUF's response under varying environmental conditions, such as temperature or voltage changes. It is expressed as:

$$BER = \frac{Number\ of\ Error\ Bits}{Total\ Number\ of\ Bits} \times 100\%$$

BER evaluates the reliability of a PUF by quantifying how consistently it generates the same response when given the same challenge. A low BER indicates higher reliability and better performance, especially for secure applications like authentication and key generation.

Ideally, BER should be as close to 0% as possible, meaning the response remains stable without errors.

Common methods to reduce BER include using error correction codes, differential measurement, and robust circuit designs to mitigate environmental impacts.

2.6 Summary

This chapter provided an in-depth exploration of Physical Unclonable Functions (PUFs), covering their fundamental characteristics, classifications, architectures, and evaluation metrics. Key PUF types, including delay-based, memory-based, and current-based PUFs, were discussed, highlighting their unique features and applications in hardware security. These architectures, such as Arbiter PUFs, SRAM PUFs, and advanced designs like PTAT PUFs and TCO-PUFs, demonstrate the versatility of PUFs in device authentication, cryptographic key generation, and integrated circuit identification.

Evaluation metrics like Uniqueness, Reliability, Uniformity, and Bit Error Rate were outlined to assess PUF performance and robustness under varying conditions. These metrics emphasize the importance of randomness, consistency, and security in PUF responses.

As PUFs continue to evolve, future designs must address challenges like resistance to machine learning attacks, scalability for complex systems, and adaptability to new computing paradigms such as Compute-in-Memory (CIM). Emerging trends focus on combining PUFs with lightweight security solutions for edge computing, IoT, and AI-driven applications, ensuring secure and efficient hardware systems in the face of growing technological demands.

CHAPTER 3

THE PROPOSED CURRENT-MODE PUF

3.1 PUF Cells

This thesis introduces an array-based Physical Unclonable Function (PUF) circuit designed to operate in current mode. The primary objective is to create a PUF that remains resilient to voltage variations by utilizing a current-generation circuit with minimal dependency on power supply fluctuations.

The proposed PUF design extends an earlier work by Georgoulas Dimosthenis, which focused on a 6T current mode and array type PUF [G24][GTT25]. As in the original paper, it provides an improved array structure to enhance performance and increase the number of Challenge-Response Pairs (CRPs) aiming to significantly boost security. Additionally, the PUF relies on current comparators to assess and compare the generated column currents.

3.1.1 PUF Cells

At the heart of our PUF design lies a current-generation cell topology designed to minimize its dependency on power supply variations. The role of the PUF cell is to generate a stable current determined primarily by the sizes of its transistors. Such circuits are widely used in analog systems, particularly for generating bias currents.

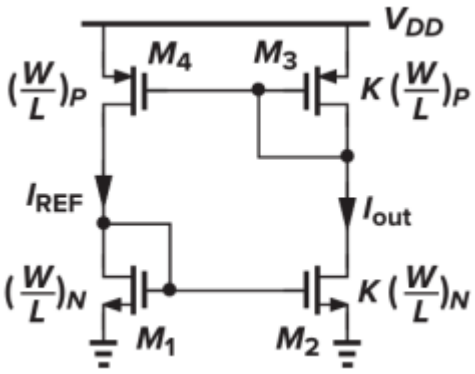

Figure 3.1: Reduced supply dependency current generation circuit.[R05].

The current generation circuit under consideration, is illustrated in Figure 3.1 [R05], and comprises four transistors (M1, M2, M3, and M4) arranged to form two complementary current mirrors. On the top M3 and M4 constitute the PMOS current mirror, while M1 and M2 form the NMOS current mirror on the bottom. This complementary arrangement enables the circuit to self-bias, with both PMOS and NMOS diode-connected transistors (M3 and M1, respectively) sharing a coupled current source. This self-biasing mechanism ensures that the current remains relatively independent of supply voltage fluctuations.

The operation of the circuit relies on maintaining a balance between the PMOS and NMOS mirrors. The output current I_{out} is determined by the reference current I_{REF} scaled by the transistor size ratio ***K***, given as:

$$I_{out} = K \cdot I_{REF}$$

K represents the size ratio of the transistors in the current mirrors. Ideally, if all transistors are identical (K=1), the currents in both branches are equal. However, process variations introduce mismatches, causing K to deviate from unity and creating a slight imbalance, which adds randomness crucial for PUF functionality.

3.1.2 Existing 6T PUF Cell Design

The 6T PUF cell design in [G24][GTT25] represents a foundational implementation of a Physical Unclonable Function (PUF) based on current generation and mirroring principles. This design emphasizes simplicity, scalability, and low power consumption while addressing key requirements such as reliability and uniformity. Below, we present its schematic, operational principles, and an analysis of its strengths and limitations.

3.1.2.1 Schematic and Operational Principles

The 6T PUF cell consists of six transistors configured to generate and mirror currents through complementary PMOS and NMOS current mirrors. The design leverages process variations during fabrication to introduce randomness in the generated currents, which form the basis for the PUF's unique responses.

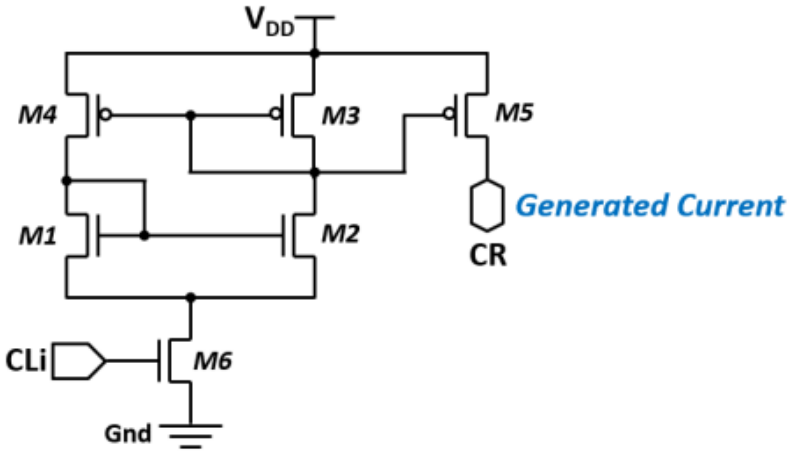

Figure 3.2: 6T PUF cell design[G24][GTT25] .

The 6T PUF cell design operates on the principle of stable current generation achieved through complementary PMOS (M3, M4) and NMOS (M1, M2) current mirrors. These mirrors are carefully configured to produce currents that remain largely independent of supply voltage variations, leveraging precise transistor sizing and a self-biasing mechanism. A key feature of the design is the inclusion of an NMOS switch transistor (M6), which provides selective activation of the cell based on the challenge input. This switch also minimizes leakage during standby mode by cutting off the current path when inactive. Additionally, the generated current is mirrored to a bitline using a PMOS transistor (M5), which plays a crucial role in isolating the PUF cell from the rest of the array components. This ensures the integrity and reliability of the generated response, making the 6T PUF cell an effective and efficient design for PUF implementations.

3.1.2.2 Strengths of the 6T PUF Design

This PUF cell design stands out for its simplicity and scalability, as its compact 6-transistor configuration minimizes silicon area and power consumption, making it ideal for large-scale array implementations. A significant advantage of this design lies in its reduced dependency on supply voltage variations, achieved through the use of complementary current mirrors that ensure consistent performance across varying conditions. Furthermore, the inherent fabrication-induced process variations introduce natural randomness in the generated

currents, enabling the production of unique and unclonable responses. Additionally, the low transistor count and efficient power usage make the design both resource-efficient and cost-effective, reinforcing its suitability for a wide range of PUF applications.

3.1.3 Analysis of Initial 7T PUF Designs

3.1.3.1 First 7T PUF Design

The first **7T PUF Cell design**, as shown in *Figure 3.3*, was initially chosen as an alternative approach. Its key innovation lies in the use of an extra transistor MN3 for the generation of a second current from the same cell. With the addition of MN3, the circuit employs two read bit lines: RBL_N (Negative Read Bit Line) and RBL_P (Positive Read Bit Line), compared to the 6T PUF Cell [G24][GTT25].

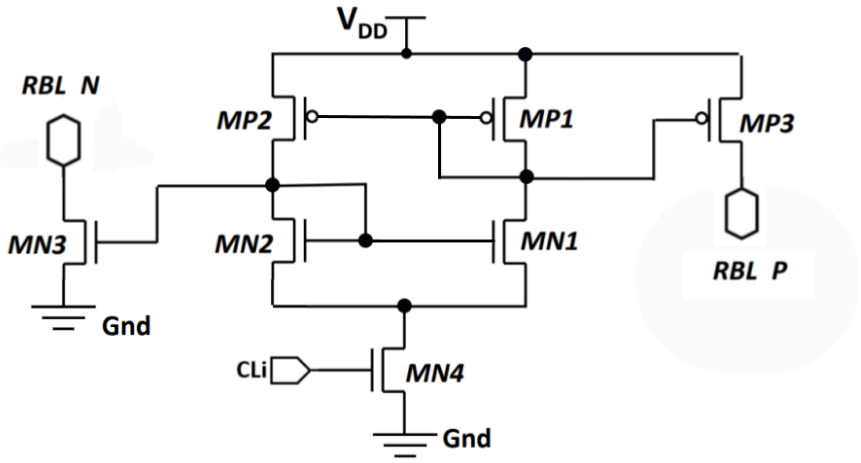

Figure 3.3: First 7T PUF cell design.

Despite the promising theoretical advantages of this design, a primary issue arose from the constant grounding of **MN3**, which establishes a permanent current path even at the idle state of the circuit. This resulted in a significant increase in static power consumption. Consequently, the first 7T PUF Cell design was deemed non-functional for the desired application.

3.1.3.2 Second 7T PUF Design

The second **7T PUF Cell**, as illustrated in *Figure 3.4*, was developed as an enhancement over the first 7T design, with the primary objective to eliminate the excessive leakage currents of the previous design. This circuit also incorporates two read bitlines, RBL_N and RBL_P, that provide a pair of working currents. Transistor MN4 plays the role of the activation switch for

the whole design. However, the current through MN3 influences the current mirrors' operation and this negatively affects the PUF functionality.

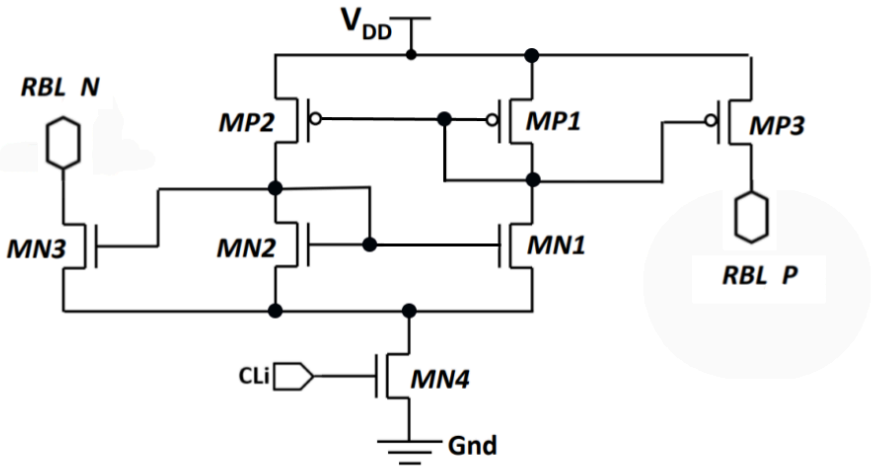

Figure 3.4: Second 7T PUF cell design.

Despite its promising design, this 7T PUF Cell did not perform as expected since the current through MN3 influences thecurrents generated by the current mirror pair.

To overcome the limitations of the 7T PUF Cell, the design was further refined with the introduction of an 8T PUF Cell.

3.1.4 The Proposed 8T PUF Cell Design

The proposed 8T PUF Cell design introduces significant improvements over its predecessors by addressing the challenges faced in the earlier 7T designs. Transistor MN5 is added in the design to restrict leakage current through MN3 during the idle mode of operation. This innovative schematic leverages an additional transistor to drastically reduce leakage currents and eliminate the influence on the current generation block. Below, we provide a detailed analysis of the schematic, its key components, and functionality.

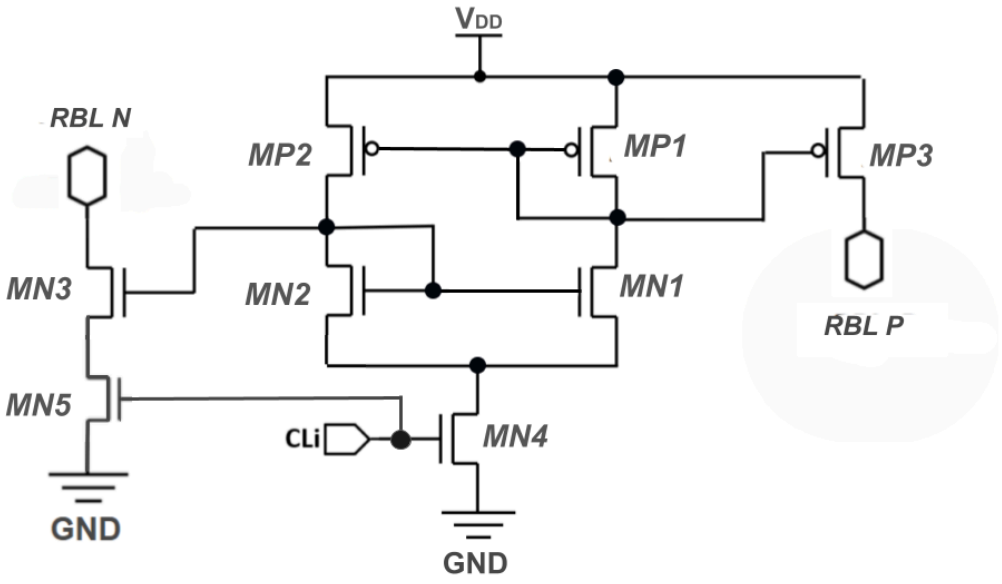

Figure 3.5: The Proposed 8T PUF Cell.

The design has the NMOS switch transistor (MN4) at the base of the current generation unit to enable dynamic activation and minimize leakage during standby. When MN4 is deactivated (OFF), no current flows through the circuit, and the internal nodes connected at the drains of MP1 and MP2 are pulled to V_{DD}, drastically reducing static power dissipation. Upon activation, MN4 ON, a current begins to flow from both branches defined by the transistor sizes

The generated currents of the current generation block are then mirrored and directed to two bitlines, RBL_P and RBL_N, via MP3 and MN3. MP3 drives the RBL_P, while MN3 drives RBL_N. These transistors play an essential role in the design by delivering the current from each active cell to the shared bitlines. This ensures the correct circuit operation since each cell remains electrically isolated from the others..

All eight transistors in the cell are designed with minimum dimensions and selecting the high threshold voltage of the technology to minimize silicon area and reduce leakage currents.

3.2 PUF Array Architecture

Array-based Physical Unclonable Functions (PUFs) represent a robust approach to enhancing security through the generation of a high number of unique Challenge-Response Pairs (CRPs). The architecture leverages process variations across the array of cells, ensuring that each response is inherently unique and unpredictable. Our PUF adopts the

concept of a current-mode array PUF, wherein the responses are generated based on the current differences arising from process-induced mismatches in the structural cells.

The Current-Mode PUF Array

The proposed PUF array, as shown in *Figure 3.6*, consists of n rows and m+1 columns. The cells of a row are activated by a common wordline which is driven by a dedicated bit of the challenge. The cells of each column feed with current two bitlines (RBL_N and RBL_P). Thus, each activated cell within the array contributes with its current to the total current of the two bitlines attached to it.

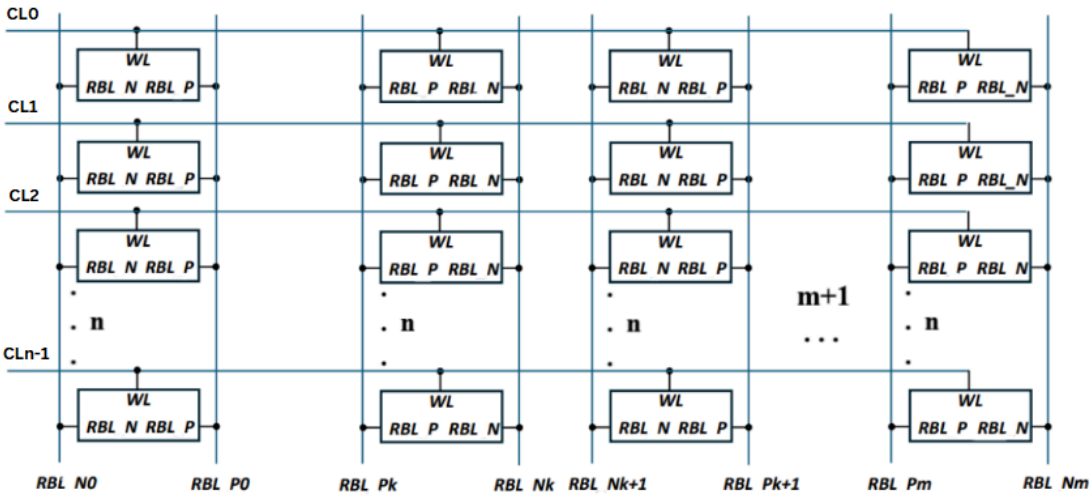

Figure 3.6: PUF Array for current mode of operation.

The cells in the array are based on the 8T PUF cell design discussed earlier. The activation of rows is controlled by the challenge provider block, enabling specific selection of rows. The generated currents are sensed through dedicated read bitlines (RBL_P and RBL_N) by current-mode comparators.

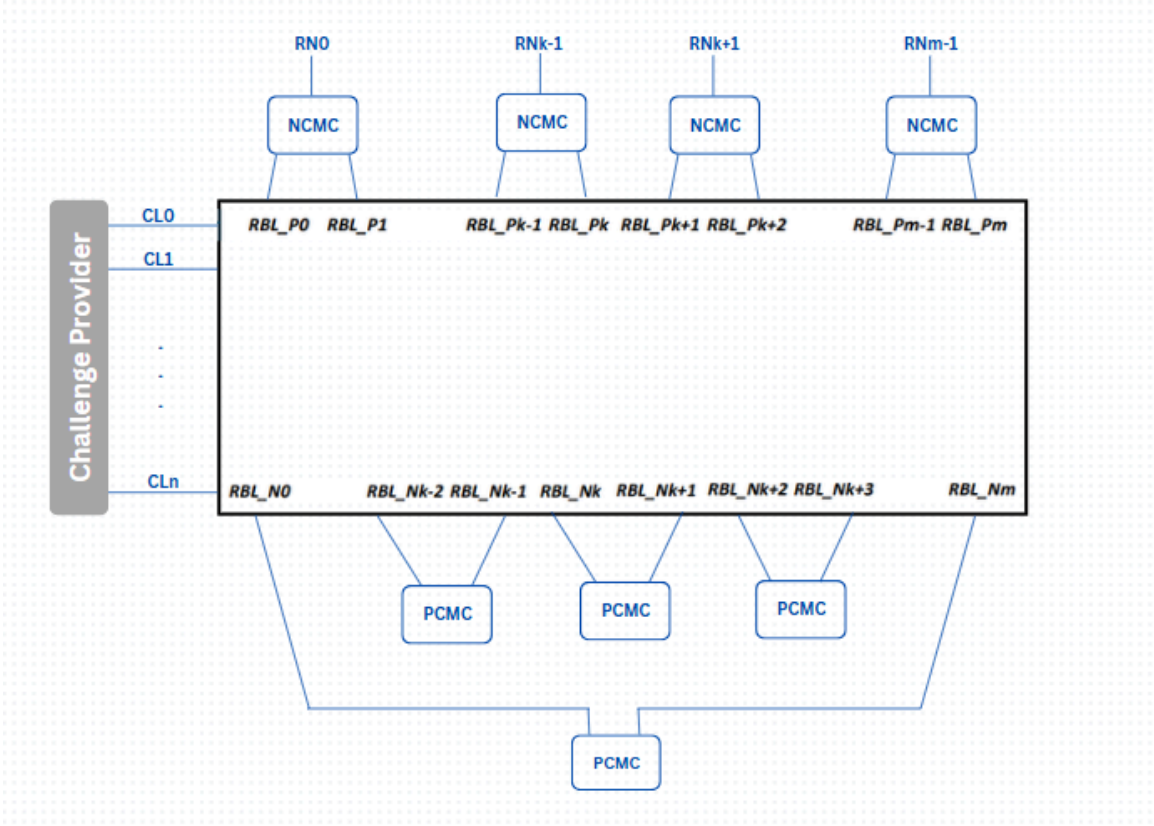

Figure 3.7: PUF Array for current mode of operation.

The architecture of the entire system is further detailed in *Figure 3.7.* This figure illustrates how the P-type current-mode comparators (PCMC) are paired with the RBL_P columns and the N-type current-mode comparators (NCMC) are paired with the RBL_N columns. The PCMC and NCMC comparators perform differential sensing of the input currents. The modular design, with separate comparators for each bitline pair, ensures scalability and efficient operation even in larger arrays. A detailed analysis of the comparators and their functionality will be provided in the following chapter.

CHAPTER 4

PUF DESIGN AND SIMULATION RESULTS

4.1 Design

To ensure proper functionality and response generation in the PUF array, certain peripheral components play a crucial role in the system's operation. Two of the most important peripheral elements in our design are the **buffers** and the **comparators**. Buffers are responsible for driving signals across the array, particularly in high-capacitance environments, while comparators evaluate and generate digital outputs by sensing current differences. Both of these components significantly impact overall PUF efficiency—buffers introduce drawbacks by increasing delays, consuming more power, and taking up additional space, while comparators affect the reliability of PUF responses.

4.1.1 Buffers

Buffers play a critical role in the operation of the PUF array by amplifying and stabilizing signals to ensure accurate row activation. Each challenge input (CL_i) is passed through these buffers to drive the $m + 1$ transistors in a single row.

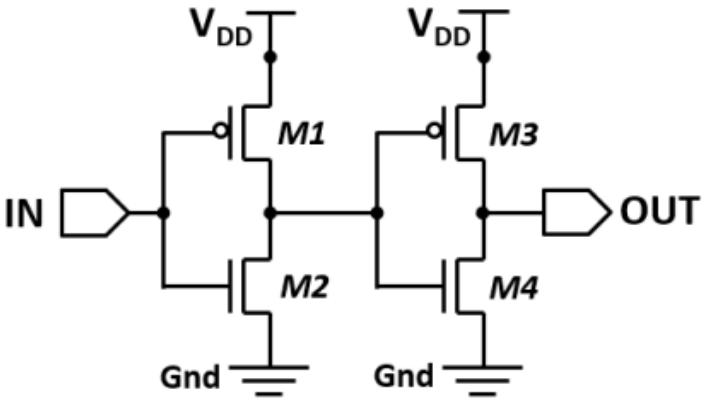

Figure 4.1: Buffer topology [G24][GTT25].

As shown in *Figure 4.1*, each buffer consists of two cascaded inverters. The second provides sufficient strength to drive all $m + 1$ NMOS transistors in a row. This ensures even signal distribution across the entire row, reducing signal delays and large ramp-up times caused by the large number of activated cells.

Additionally, these same buffers are used for the signals feeding the comparators. Accurate comparator evaluation depends on this fast and stable signal delivery, further highlighting the importance of buffers in the overall architecture.

4.1.2 The Comparators

In current-mode PUF arrays, comparators are essential for evaluating the differences between the currents of the associated bitlines, enabling the generation of reliable digital responses. Each column in the array drives two comparators simultaneously. The comparators significantly influence the PUF's performance and reliability, as they directly impact the response generation process.

4.1.2.1 The N-type Current Mode Comparator (NCMC)

The N-type Current Mode Comparator (NCMC) is an essential component of the PUF array, designed to compare currents between two-bit lines (BL). For this purpose, the Current Mode Sense Amplifier (CMSA) is employed (see *Figure 4.2*), a well-established comparator designed specifically for evaluating small current differences. This circuit, originally proposed by Blalock [BJ91], has been adapted in our implementation with adjustments to transistor sizes and signal timings to better suit the requirements of our PUF architecture. The same CMSA design was also used in a previous PUF implementation[G24], demonstrating its robustness and versatility for current-mode applications.

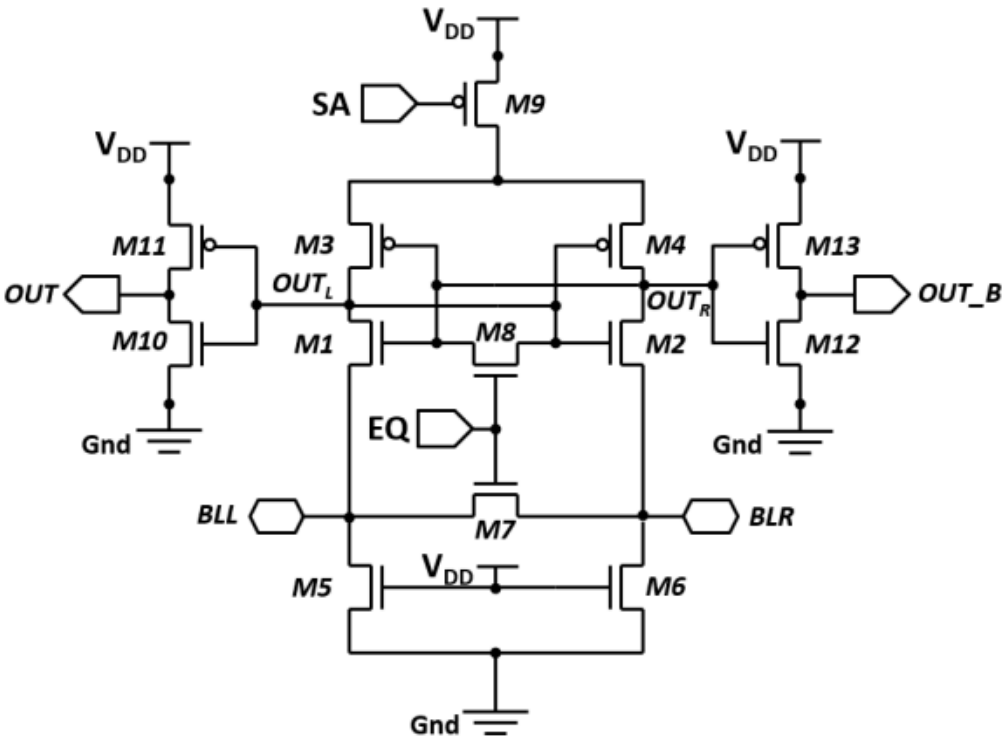

Figure 4.2: Current Mode Comparator - NCMC [G24].

The CMSA compares the current flowing through adjacent columns and amplifies even small differences, allowing for a rapid and precise response. As depicted in *Figure 3.7*, every NCMC comparator is fed by two adjacent RBL_P read bitlines and identifies the *"winner bitline,"* which has the higher current.

The CMSA's architecture, illustrated in *Figure 4.2*, consists of several key components that contribute to its functionality. A cross-coupled latch formed by transistors M1, M2, M3, and M4 provides bistable operation, ensuring distinct and stable outputs. The equalization transistors M7 and M8 equalize to Gnd the internal nodes during the precharge phase. The transistors M5 and M6 operate in the linear region and control the current flow, playing a crucial role in circuit operation. Additional inverters, including M10, M11, M12, and M13, sharpen the output signals, while the M9 transistor is used for the activation of the sense amplifier via the SA signal.

4.1.2.2 The P-type Current Mode Comparator (PCMC)

The P-type Current Mode Comparator (PCMC) depicted in Figure 4.3 is a complementary structure to that of the NCMC comparator with exactly the same functionality. It compares currents from two adjacent bitlines (*BLL* and *BLR*) and determines the "winner bitline" with the higher current.

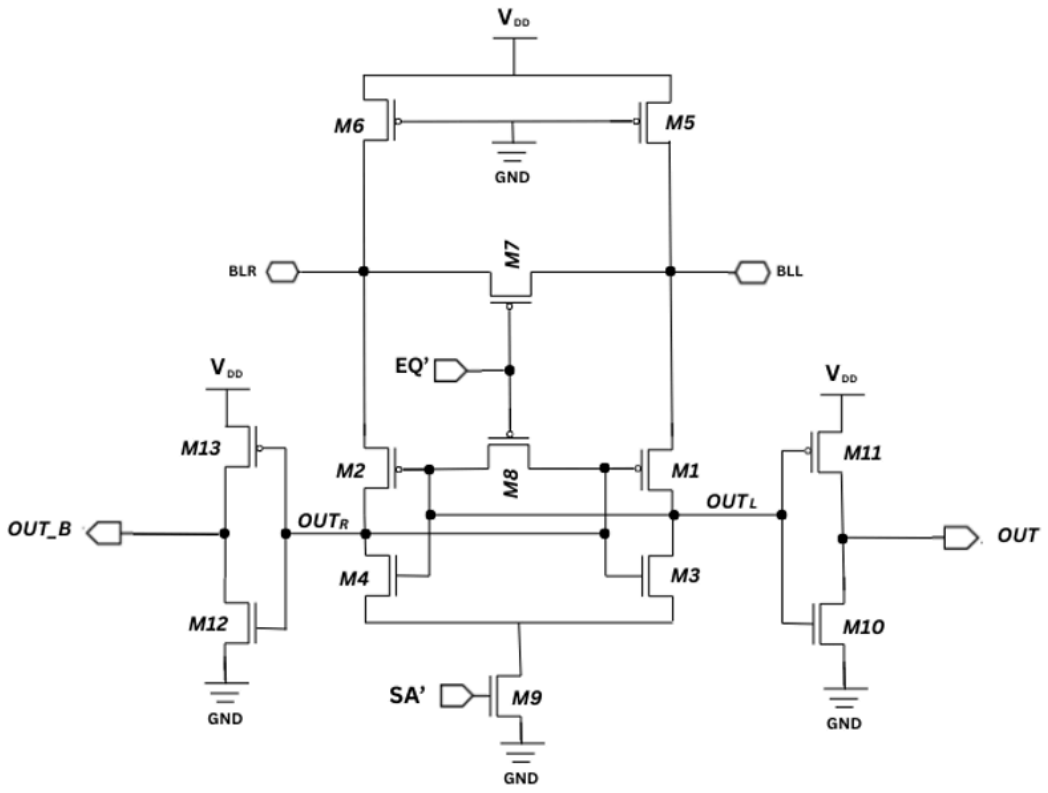

Figure 4.3: Current Mode Comparator - PCMC.

The circuit uses a cross-coupled latch (M1-M4), equalization transistors (M7, M8) to reset internal nodes to VDD, via the EQ' signal, and PMOS transistors (M5, M6) which serve as active resistors by operating in the linear region. The outputs (OUT and OUT_B) are stabilized by additional inverters (M10-M13), ensuring reliable operation. Lastly, transistor M9 is used for the activation of the sense amplifier via the SA' signal.

4.2 Operation Phases

The operation of the proposed PUF is divided into three distinct phases: **Discharge-Equalization**, **Activation**, and **Sense** phases. Each phase is crucial to ensure the proper functionality, stability, and reliability of the system. The indicative waveforms of all control signals are shown in *Figure 4.4*. It is important to note that the timing between the signals in the waveform is illustrative and not explicitly defined. The purpose of this figure is to aid in understanding the relationships between the signals and the corresponding operational phases of the circuit. Below, a detailed description of each phase is provided.

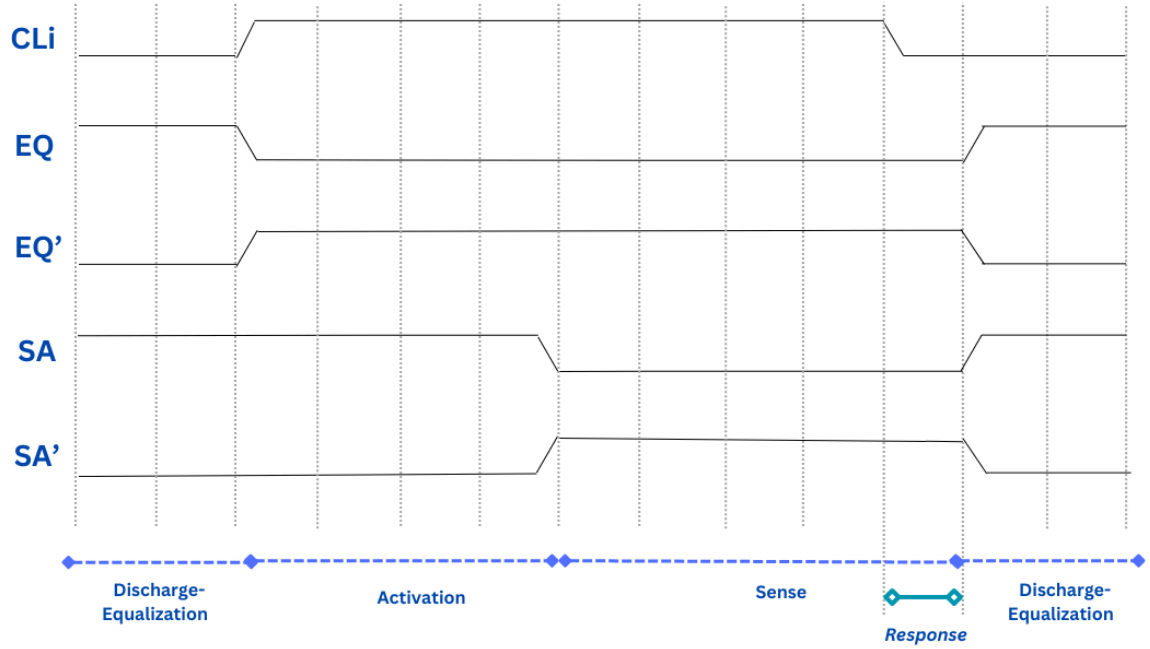

Figure 4.4: Indicative control signal waveforms and their phases.

4.2.1 Discharge-Equalization Phase

This phase serves as the reset and initialization stage of the PUF. Before applying a challenge, the circuit enters an idle state where the EQ signal is set high, while its complementary signal, EQ', is set low. The SA signal is set to high to remain inactive and the SA' is set to low. During this time, transistors M5 and M6 initialize the internal nodes of the comparator and the bitlines to Gnd for the NCMC comparator and to VDD for the PCMC comparator. Simultaneously, the equalization transistors M7 and M8 ensure that the internal nodes of the comparator are equalized, preventing any potential biasing that could influence the next operation. This phase ensures that the bitlines and nodes start from a neutral state, eliminating any residual effects from previous operations.

4.2.2 Activation Phase

Once the discharge-equalization phase is complete, the circuit transitions to the activation phase, marked by the application of a challenge. During this phase, one or more challenge lines (CLi) are driven high, activating the corresponding PUF cells in the selected rows. This activation sets the CLi signal of the chosen cells to high, turning on their respective NMOS transistors (MN4 in Figure 3.5). As a result, current begins to flow through the active cells: The EQ (EQ') signal is now set low (high) to disable the equalization mechanism, allowing the circuit to establish stable current levels on the bitlines. This phase ensures that the

bitlines carry currents representative of the inherent process variations within the PUF cells.

4.2.3 Sense Phase

The final phase is the sense phase, where the PUF generates its digital response. During this phase, the comparators are activated by setting the SA signal low and its complementary signal SA' high. The currents flowing through the associated bitlines. The CMSA structure ensures a fast and accurate comparison, with the output nodes (OUT and OUT_B) generating the final digital response. The sense phase is critical for converting the current differences into a secure and reliable binary output (0 or 1) which is the *Response*. Once the comparison is complete, the circuit prepares for the next session by resetting both the EQ and SA signals to logical high, returning the system to the discharge-equalization phase.

4.3 Overall Design

The top level design of the current-mode PUF system integrates all the key components necessary for its functionality, as depicted in *Figure 4.5*. The system is centered around the **PUF Array**, which consists of 256 input challenge lines (CL0 to CL255) corresponding to word lines (WL) that control the activation of rows in the PUF cell array. Each challenge line activates a row in the PUF array, driving the associated word line (WL) through dedicated buffers.

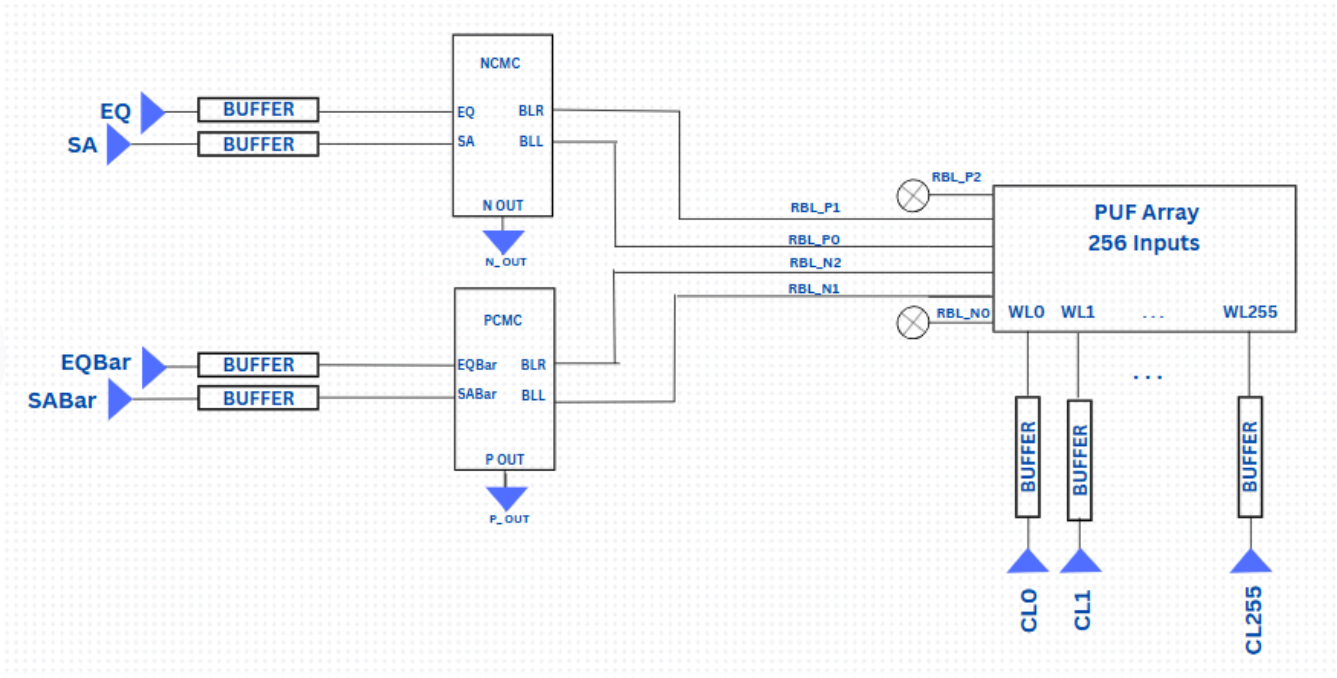

Figure 4.5: Layout with all the components.

The outputs of the PUF Array are the RBL_P read bitlines and the RBL_N read bitlines , which are routed to two current-mode comparators: the P-type and the N-type Current Mode Comparators. These comparators are responsible for evaluating the current differences on their respective bitlines. The PCMC processes the RBL_P bitlines to determine the "winning" line, generating the output P_OUT, while the NCMC evaluates the RBL_N bitlines to identify the "winning" line, producing the output N_OUT.

Control signals (EQ, SA, EQBar, and SABar) are used to manage the circuit's operation across its phases. These signals pass through dedicated buffers before reaching the comparators to ensure proper timing and signal strength.

4.4 Simulation Results

This section provides an in-depth evaluation of the performance of our proposed PUF. We closely monitored key performance indicators, including reliability, uniqueness, uniformity, response time, power consumption, the total number of Challenge-Response Pairs (CRPs), and the silicon area required for implementation.

4.4.1 Analysis of Environmental Factors

In the PUF design we use the commercial UMC 90nm CMOS technology exploiting the Virtuoso tool of CADENCE. To evaluate the performance and robustness of the PUF, we conducted extensive Monte Carlo SPECTRE simulations, considering variations arising from the fabrication process. Our goal was to assess how reliable the PUF is under different environmental conditions, such as temperature and voltage fluctuations.

We carried out a total of 25 simulation sessions, each consisting of 5,000 Monte Carlo runs. Specifically, we tested the PUF performance across a range of temperatures, 0°C, 27°C, and 80°C, to simulate different operating environments. Additionally, we examined how its functionality is affected by power supply voltage variations, adjusting it by ±10% from the nominal value of 1V (i.e., from 0.9V to 1.1V).

For our analyses, we activated 128 rows, while the proposed PUF architecture includes a total of 256 rows and 3 columns. The results were adjusted for 64 columns.

4.4.2 Behavior and Timing Characteristics of the PUF

The outputs of the PUF (*N_OUT* and *P_OUT*) generated by each comparator represent the combined responses of the PUF and should be treated as a unified dataset when computing all relevant metrics. However, it is also insightful to examine the behavior of each comparator individually.

In *Figures 4.6* and *4.7*, we present a sample of 10 Monte Carlo simulations. The first figure illustrates the output from the NCMC comparator, while the second depicts the output from the PCMC comparator. In both cases, we observe that approximately half of the responses quickly stabilize at ‘0’ while the remaining half settle at ‘1,’ as expected.

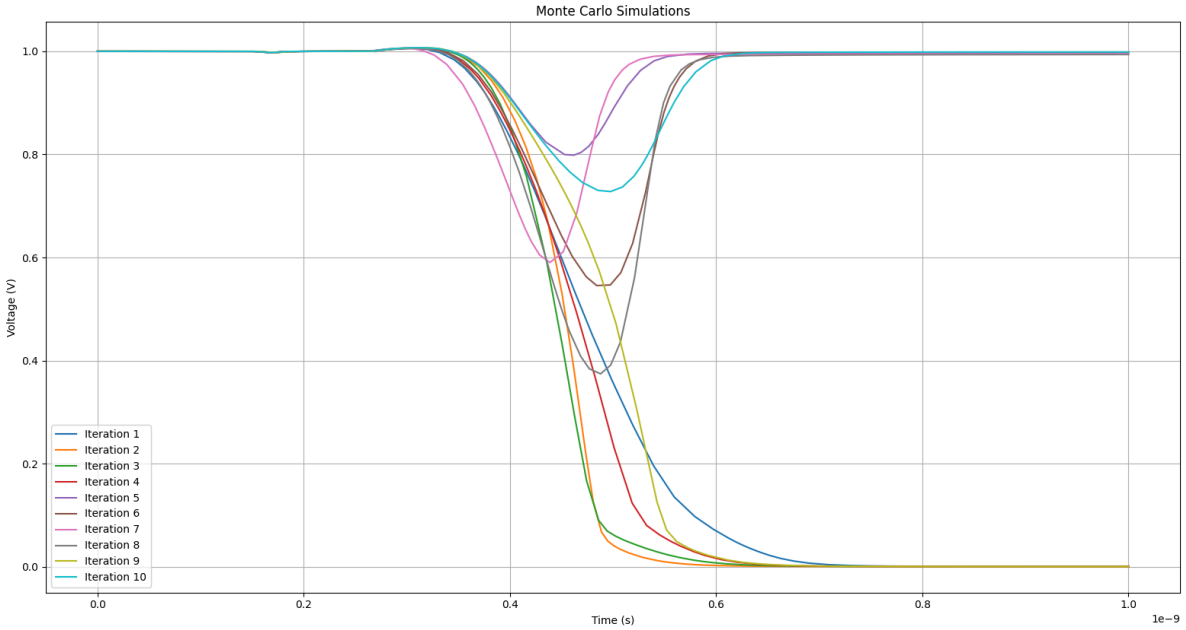

Figure 4.6: Indicative Monte Carlo Simulation Results for the NCMC Output.

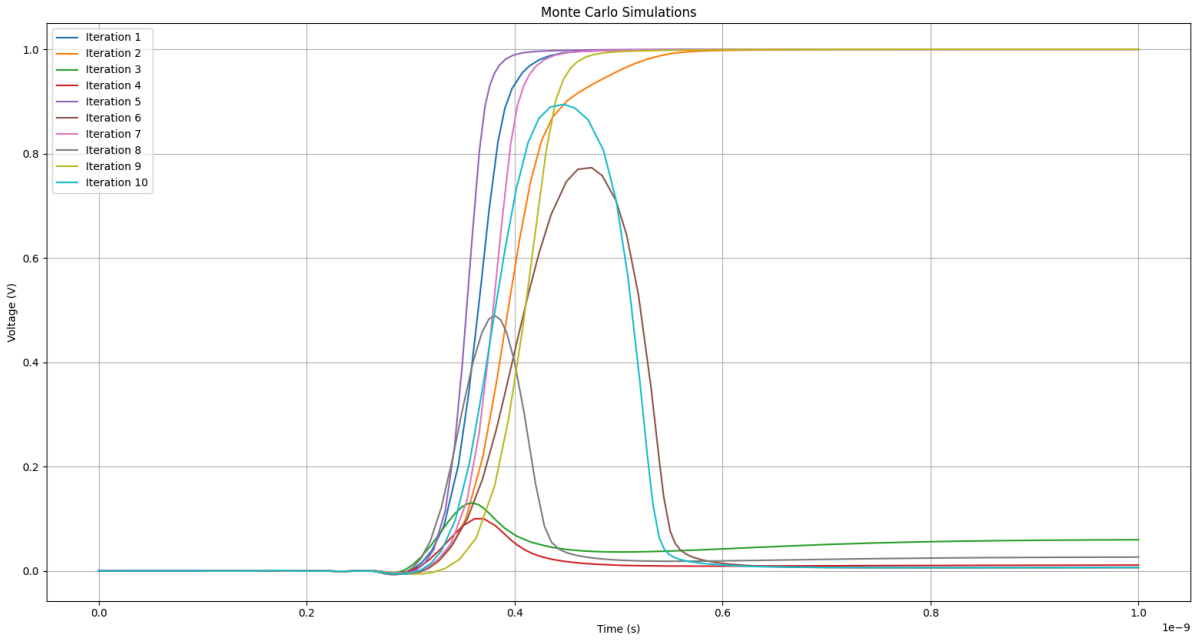

Figure 4.7: Indicative Monte Carlo Simulation Results for the PCMC Output.

It is important to note that both simulations were conducted under nominal conditions, specifically at a temperature of 27°C and a supply voltage of 1V.

The example illustrates that the PUF stabilizes rapidly, requiring approximately 250ps. During operation, the bitline behavior and the NCMC comparator follow a predictable pattern. When '*BLL*' is greater than '*BLR*,' the output signals are 'OUT_L' = 1 and 'OUT_R' = 0. Conversely, when '*BLR*' exceeds '*BLL*,' the signals switch to 'OUT_L' = 0 and 'OUT_R' = 1. For the PCMC comparator, the exact opposite occurs, ensuring that in both comparators, the output eventually settles at either '0' or '1.'

4.4.3 Analysis and Selection of Transistors in the Design

The performance of the PUF heavily depends on the types and sizes of transistors used in its key components, such as PUF cells, comparators, and buffers. Careful selection is essential, and for our implementation.

Beginning with the **PUF cell**, we choose for minimum-size transistors with a width (W) of 120nm and a length (L) of 80nm to minimize the required silicon area. For transistors MN1, MN2, MN3, MP1, MP2, and MP3, we use standard process (SP) transistors. Additionally, to reduce static power consumption, we select high-threshold voltage (HTV) transistors for MN4 and MN5. A detailed table of transistor dimensions follows.

Id	Width	Length	Type
NM1, NM2, NM3	120nm	80nm	NMOS SP
NM4, NM5	120nm	80nm	NMOS HVT
MP1, MP2, MP3	120nm	80nm	PMOS SP

Table 4.1: Sizes and types of puf cell transistors.

Regarding the **comparators**, the design considerations become more complex. While we decided to use SP transistors, a key focus was on the transistor pair M5 and M6. For the PCMC, we settled on a width of 8μm, whereas for the NCMC we chose a width of 4μm. The detailed tables of transistor dimensions follows.

Id	Width	Length	Type
M1, M2	1.2µm	160nm	NMOS SP
M3, M4	1.2µm	160nm	PMOS SP
M5, M6	4µm	80nm	NMOS SP
M7, M8, M10, M12	120nm	80nm	NMOS SP
M9, M11, M13	120nm	80nm	PMOS SP

Table 4.2: Sizes and types of NCMC comparator transistors.

Id	Width	Length	Type
M1, M2	1.2µm	160nm	PMOS SP
M3, M4	1.2µm	160nm	NMOS SP
M5, M6	8µm	80nm	PMOS SP
M7, M8, M11, M13	120nm	80nm	PMOS SP
M9, M10, M12	120nm	80nm	NMOS SP

Table 4.3: Sizes and types of PCMC comparator transistors.

While not the most critical component, the **buffer** still plays a significant role in the circuit's overall function. It has a measured delay of around 50ps, which is low enough to allow the use of just two inverters instead of a longer chain.

The transistor specifications for the buffer are outlined in Table 4.4. In designing the first inverter, we opted for an NMOS transistor, paired with a PMOS transistor that is four times larger. This sizing compensates for the lower hole mobility, which is approximately four times less than electron mobility in the UMC90nm technology we use. Additionally, the second inverter is scaled up to be about 3.6 times larger than the first, ensuring stable and efficient signal transmission.

Id	Width	Length	Type
M1	480nm	80nm	PMOS SP
M2	120nm	80nm	NMOS SP
M3	1.73µm	80nm	PMOS SP
M4	430nm	80nm	NMOS SP

Table 4.4: Sizes and types of buffer transistors.

4.4.4 Performance Metrics and Reliability Analysis

Uniqueness is a key metric for evaluating the ability of a PUF to produce distinct responses across different implementations of the same design. An ideal *Uniqueness* approaches the value of 50%, ensuring maximum distinguishability between implementations.

Uniqueness (%)			
V(V) \ T(°C)	0°C	27°C	80°C
0,9 V	50.00	-	49.92
1 V	-	49.98	-
1,1 V	49.95	-	49.96

Table 4.4: Measured Uniqueness (%) Across Different Voltage and Temperature Conditions.

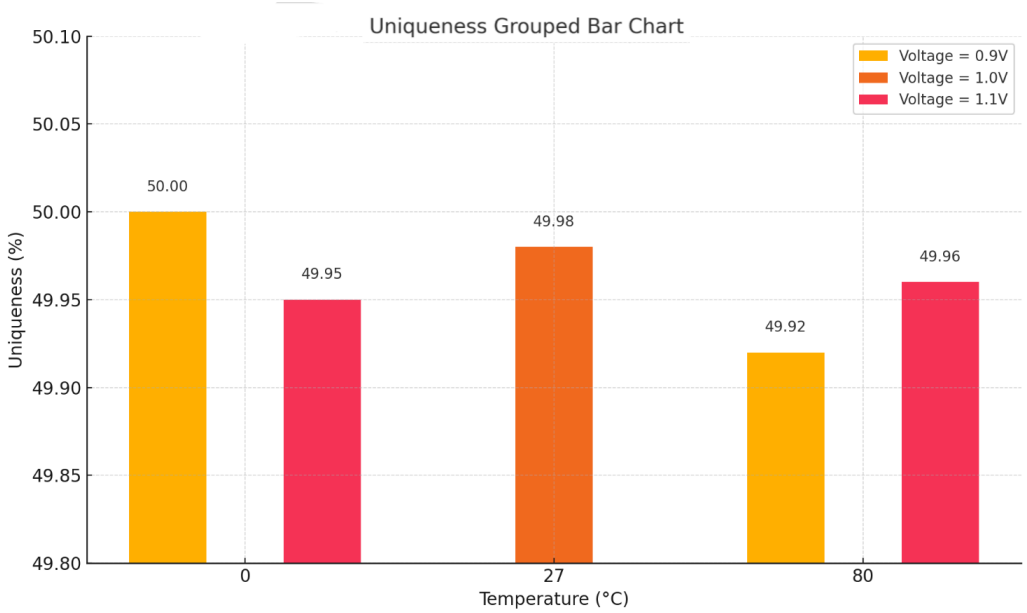

Figure 4.8: Uniqueness Analysis Across Voltage and Temperature Levels.

Based on the results presented in the table, the **average measured uniqueness** across all tested conditions (tested temperatures and power supply voltages) is **49.96%**, . The deviations from the ideal value are minimal, confirming the reliability of the PUF across varying operating conditions.

Uniformity is a metric that measures the unpredictability of a PUF's responses by assessing the proportion of 0's and 1's in the response bits. An ideal *Uniformity* is 50%, reflecting a perfectly random response distribution.

Uniformity (%)			
V(V) \ T(°C)	0°C	27°C	80°C
0,9 V	49.58	-	48.00
1 V	-	48.98	-
1,1 V	48.37	-	48.52

Table 4.5: Measured Uniformity (%) Across Different Voltage and Temperature Conditions.

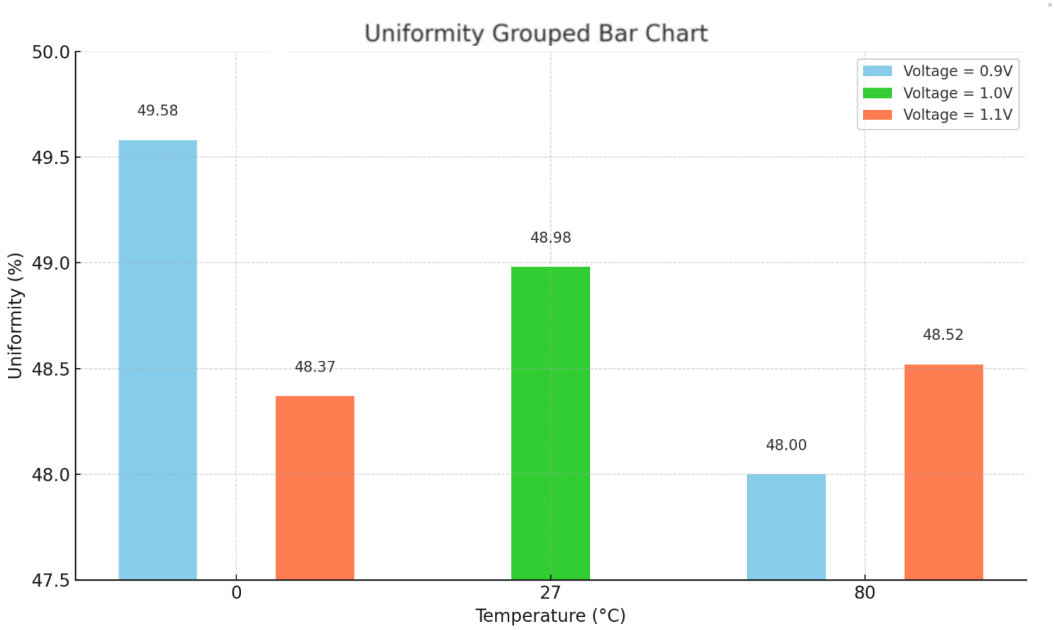

Figure 4.8: Uniformity Analysis Across Voltage and Temperature Levels.

Based on the results presented in the table, the **average measured uniformity** across all tested conditions is **48.57%**, slightly below the ideal value of 50%. While this indicates minor deviations from perfect randomness, the results still demonstrate a reasonably high degree of unpredictability. Specifically:

- The uniformity decreases slightly at higher temperatures (e.g., 48.00% at 80°C for 0.9V).
- The values are relatively consistent across different voltages and temperatures, showcasing stable behavior.

Reliability measures a PUF's ability to consistently produce the same response R for a given challenge C, despite changes in environmental conditions like temperature and voltage. Ideally, it reaches 100%, indicating zero intra-chip Hamming distance.

In this evaluation, nominal conditions (27°C and 1V) were used as a baseline to assess reliability across extreme operating points. Both *N_OUT* and *P_OUT* responses were treated as a unified response for the calculations. The measured reliability values are presented in the table below:

Reliability(%)		
V(V) \ T(°C)	0°C	80°C
0,9 V	98.58	97.88
1,1 V	95.09	97.70

Table 4.5: Measured Reliability (%) Across Different Voltage and Temperature Conditions.

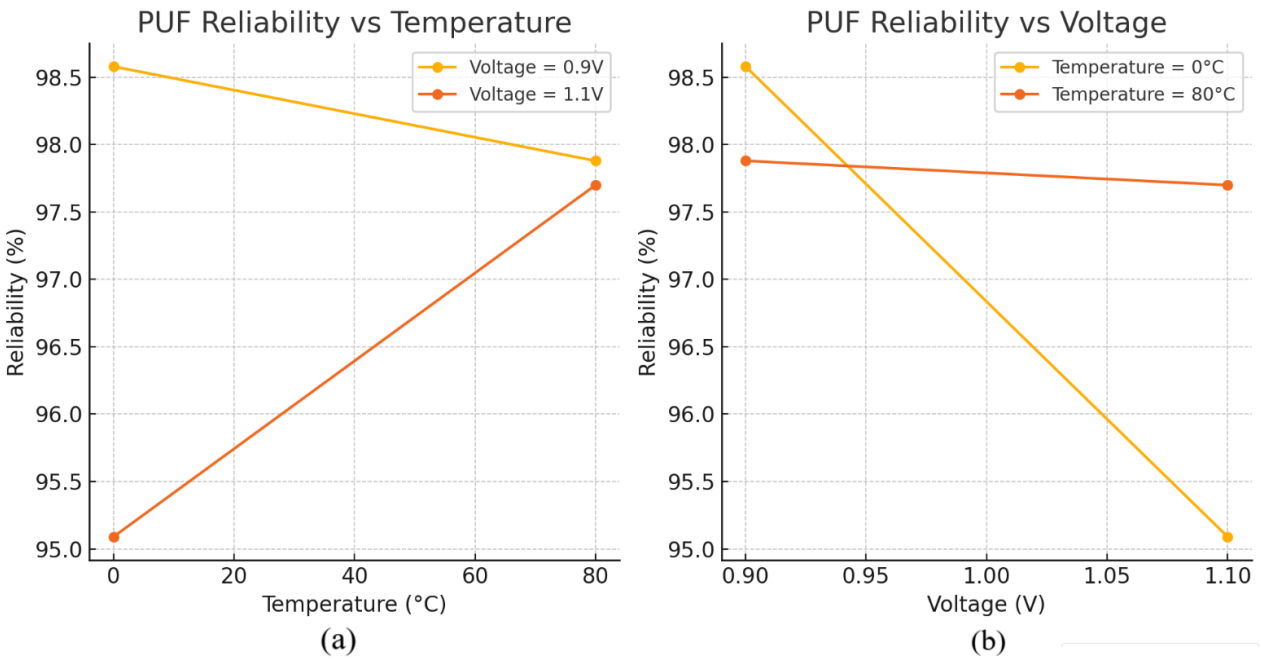

Figure 4.9: PUF reliability vs Temperature and Power Supply Voltage

The reliability ranges from 95.09% to 98.58% under supply voltage variations, with an average of **96.81%** and variability of 1.74%, reflecting minimal dependency on power supply changes. Under temperature variations, it ranges from 97.70% to 98.58%, averaging **98.04%** with a variability of 0.44%, demonstrating strong stability across different temperatures.

4.4.5 Power Consumption and Silicon Area Estimation

To assess the robustness of the PUF, it is essential to determine the total number of Challenge-Response Pairs (CRPs). In our implementation, each challenge activates a number of the 256 available rows. Comparators process the generated currents, converting them into binary values (0 or 1) with each comparator producing 1 bit, forming the unique 64-bit response of the PUF. The total number of CRPs is defined by the combinatorial equation:

$$CRPs = \sum_{k=1}^{n} \binom{n}{k} = 2^n - 1$$

where:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

For $n = 256$, the theoretical CRP count is:

$$2^{256} - 1$$

This study focuses on activating k=128 rows (*n/2*), as in the previous research [GTT25]. Selecting k=128 provides the maximum number of CRPs with respect to every other k value:

$$\binom{256}{128} \approx 5.768658823 \times 10^{75}$$

For the required silicon area assessments of the proposed PUF, we initially conducted experiments with the topology of **256 rows x 3 columns**. However, for a more comprehensive evaluation, we extrapolate the results for a topology with **256 rows and 64 columns**.

For the estimation and the comparisons of the required silicon area, the area of the transistor gates (W×L) is taken into account. The PUF array in this configuration contains **8 transistors of minimum size** (W=120 nm and L=80 nm), resulting in a total area of **1,258.29 μm²**.

To support the 256 rows in the PUF array, with the estimated total buffer area amounting to 84.78 μm². Additionally, the current NCMC comparators occupy an estimated silicon area of 23.60 μm², while the PCMC comparators occupy an estimated silicon area of 33.84 μm². The total estimated silicon area occupied by the PUF is **1,400.51 μm²**.

Considering the previously discussed parameters, given that 128 wordlines are activated, we also evaluated energy consumption. By accounting for both static and dynamic energy , at **1V and 27°C**, the total energy consumption was determined to be **39.75 pJ/bit**.

4.4.6 Comparative Analysis with State-of-the-Art PUFs

The proposed PUF design stands out for its reliability, low power consumption, and minimal silicon footprint, achieving excellent performance across key metrics. The measurements include both the buffers and the NCMC and PCMC comparators, but factors such as circuit aging and error correction mechanisms have not been considered.

In many cases, details like area per bit and energy consumption per bit are often omitted, making it difficult to compare this implementation with other proposed PUF designs. However, a particularly relevant comparison is with the design in [GTT25], which served as the foundation and inspiration for this research.

Our design introduces improvements by combining a robust and highly reliable PUF. Additionally, unlike many architectures that operate only during system startup, the proposed circuit can be utilized at any time, offering greater flexibility and enhanced security.

Finally, most state-of-the-art PUF implementations analyzed in the previous sections are presented in *Table 4.6*, alongside the proposed design, for direct comparison.

CHAPTER 5

CONCLUSIONS

In this thesis, we propose a new design for a Physical Unclonable Function (PUF) circuit, which demonstrates intriguing features. The proposed current-mode array PUF is both strong and reliable, showcasing resilience to temperature and power supply variations. Additionally, the array structure of this PUF ensures its scalability for larger implementations.

Given the close relationship between the proposed 8T PUF and the CAS-PUF [GTT25], it is essential to present a comparative analysis of their characteristics and performance. Both designs are implemented in 90nm technology, operate in current mode, and are classified as strong PUFs. However, there are notable differences in their design complexity, silicon area, power consumption, and reliability metrics.

A key distinction lies in the number of transistors per cell. The CAS-PUF employs a simpler 6-transistor design, whereas the proposed 8T PUF utilizes 8 transistors per cell. This added complexity in the 8T PUF increases the silicon area to 1,400.51 μm^2, compared to 958.464 μm^2 for the CAS-PUF. Another fundamental difference is that the proposed 8T PUF incorporates two types of comparators, **PCMC** and **NCMC**, whereas the CAS-PUF uses a simpler comparator design. Additionally, the 8T PUF employs a greater number of buffers, which contributes to its increased complexity, higher silicon area, and power consumption.

In terms of reliability, the proposed 8T PUF achieves 98.04% reliability under temperature variations, surpassing the CAS-PUF's 96.45%. However, the CAS-PUF exhibits slightly better reliability under voltage variations, with a value of 97.69%, as opposed to 96.81% for the 8T PUF. This trade-off suggests that the 8T PUF is better suited for temperature-sensitive environments, while the CAS-PUF is preferable for voltage-sensitive applications.

Both designs achieve excellent metrics for uniqueness and uniformity. The CAS-PUF has a slight edge in uniformity, scoring 49.59% compared to 48.57% for the 8T PUF. Uniqueness

values are nearly identical, with 50.01% for the CAS-PUF and 49.96% for the 8T PUF, indicating highly distinctive responses in both cases.

Power consumption presents another significant difference. The CAS-PUF reports dynamic power consumption of 3.23mW/b and static power of 78.11nW/b. In contrast, the 8T PUF has a dynamic power consumption of 159mW and static power of 5.22μW. This leads to a total energy consumption of 39.75 pJ/b.

Both designs support the same temperature range (0–80°C) and voltage range (0.9–1.1V). They also achieve an identical number of Challenge-Response Pairs (CRPs), estimated at 5.76×10^{75}, highlighting their scalability and robustness for handling extensive challenges and responses.

Finally, an interesting difference between the 6T CAS PUF and the proposed in this thesis 8T PUF is that in CAS PUF each read bitline (RBL) feeds a pair of current mode comparators while in the 8T PUF each bitline feeds a single current mode comparator. This characteristic of the 8T PUF eliminates a possible interference between the pairs of comparators that may exist in the CAS PUF design, due to their connectivity through the common RBL.

In conclusion, the CAS-PUF is more efficient in terms of silicon area and power consumption, making it ideal for resource-constrained applications. On the other hand, the proposed 8T PUF offers improved temperature reliability, along with the elimination of a possible interference between the comparators . The choice between these designs ultimately depends on the specific application requirements and the trade-offs between area, power, and reliability.

Design	Arbiter PUF [MMT20]	RO PUF [SD07]	SCA-PUF [ZZNS19]	PTAT [LS16]	SiCBit-PUF [XTT23]	PUF-CIM [CWZ+23]	SPUF [LYK22]	CAS-PUF [GTT25]	**Proposed 8T PUF**
Technology	45nm	FPGA 90nm	130nm	65nm	32nm	55nm	65nm	90nm	**90nm**
Operation mode	Voltage	Voltage	Current	Current	Voltage	Voltage	Voltage	Current	**Current**
Total area (μm^2)	2168	NA	44700	7.42/bit	NA	395×10^3	12580	958.464	**1,400.51**
Temperature range (°C)	0 - 100	-20 - 100	-20 - 80	0 - 80	0 - 100	-40 -125	-10 - 80	0 - 80	**0 - 80**
Voltage range (V)	0.9 -1.1	1.08 -1.2	1.08-1.32	0.6 - 1.2	0.9 - 1.1	1.1 - 1.3	0.5 - 1	0.9 - 1.1	**0.9 - 1.1**
Reliability (T=c) (%)	97.01	NA	NA	99	95.2	NA	NA	96.45	**98.04**
Reliability (V=c) (%)	94.49	NA	NA	96.5	97.4	NA	NA	97.69	**96.81**
Avg. Reliability (%)	NA	99.52	91.00	NA	98.2	98.9	97	NA	**NA**
Uniqueness (%)	49.99	46.15	49.9	50.01	49.99	49.97	49.47	50.01	**49.96**
Uniformity (%)	50.094	NA	52.8	49.3	49.74	49.76	50.11	49.59	**48.57**

Table 4.6: Comparison table between state-of-the-art PUFs and the proposed 8T PUF.

BIBLIOGRAPHY

[BJ91] T. Blalock and R. Jaeger, *"A high-speed clamped bit-line current-mode sense amplifier,"* vol. 4, pp. 542--548, 1991.

[LYK22] L. Lu, T. Yoo, and T. T.-H. Kim, *"A 6T SRAM based two-dimensional configurable challenge-response PUF for portable devices,"* IEEE Transactions on Circuits and Systems I, 2022.

[BH12] C. Böhm and M. Hofer, *Physical Unclonable Functions in Theory and Practice,* Springer, 2012.

[M12] R. Maes, *Physically Unclonable Functions: Constructions, Properties, and Applications,* Ph.D. dissertation, Katholieke Univ. Leuven, Belgium, 2012.

[SD07] G. E. Suh and S. Devadas, *"Physical Unclonable Functions for Device Authentication and Secret Key Generation"*, Proc. 44th Annual Design Automation Conf., 2007.

[LS16] J. Li and M. Seok, *"Ultra-compact and robust physically unclonable function based on voltage-compensated proportional-to-absolute-temperature voltage generators",* IEEE, 2016.

[HYKD14] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "*Physical Unclonable Functions and Applications: A Tutorial"*, Proceedings of the IEEE, 2014.

[MYWR19] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "*A PUF taxonomy,*" Applied Physics Reviews, vol. 6, no. 1, 2019.

[MMT20] M. Moradi, R. Mirzaee, and S. Tao, *"CMOS arbiter physical unclonable function with selecting modules,"* in IEEE, 2020.

[LG+04] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, *"A technique to build a secret key in integrated circuits for identification and authentication applications,"* Proceedings of the Symposium on VLSI Circuits, Digest of Technical Papers, pp. 176–179, 2004.

[CSM19] A. S. Chauhan, V. Sahula, and A. S. Mandal, *"Novel Randomized Placement for FPGA Based Robust ROPUF with Improved Uniqueness,"* Journal of Electronic Testing, vol. 35, pp. 581–601, 2019.

[H18] B. Halak, *Physically Unclonable Functions: From Basic Design Principles to Advanced Hardware Security Applications*, Springer International Publishing, 2018. ISBN 978-3-319-76803-8.

[S+17] A. Schaller et al., *"Intrinsic rowhammer pufs: Leveraging the rowhammer effect for improved security,"* in 2017 IEEE HOST, pp. 1–7, 2017.

[ZZNS19] H. Zhuang, X. Xi, N. Sun, and M. Orshansky, *"A strong subthreshold current array PUF resilient to machine learning attacks,"* vol. 1, pp. 135–144, 2019.

[MHCZ15] M. S. Mispan, B. Halak, Z. Chen, and M. Zwolinski, *"TCO-PUF: A Subthreshold Physical Unclonable Function,"* Proc. IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 105–108, 2015.

[XTT23] A. Xynos, V. Tenentes, and Y. Tsiatouhas, *"SiCBit-PUF: Strong in-Cache Bitflip PUF Computation for Trusted SoCs,"* in IEEE, 2023.

[CWZ+23] M. 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,"* 2023.

[G24] D. Georgoulas, *"Current Mode, Array-Based Physical Unclonable Function Circuit,"* Master's Thesis, Department of Computer Science and Engineering, University of Ioannina, Greece, 2024.

[GTT25] D. Georgoulas, Y. Tsiatouhas and V. Tenentes, *"CAS-PUF: Current-mode Array-Type Strong PUF for Secure Computing in Area Constrained SoCs,"* to be presented in the Design, Automation and Test in Europe (DATE), 2025.

[R05] B. Razavi, Design of Analog CMOS Integrated Circuits, 2005.