**A ROBUST AUTHENTICATION
METHODOLOGY USING PHYSICALLY
UNCLONABLE FUNCTIONS IN DRAM
ARRAYS**

by

MARYAMSADAT HASHEMIAN

Submitted in partial fulfillment of the requirements

for the degree of Doctor of Philosophy

Department of Electrical, Computer, and Systems Engineering

CASE WESTERN RESERVE UNIVERSITY

August, 2020

CASE WESTERN RESERVE UNIVERSITY
SCHOOL OF GRADUATE STUDIES

We hereby approve the dissertation of

MaryamSadat Hashemian

candidate for the degree of **Doctor of Philosophy***.

Committee Chair

Dr. Christos Papachristou

Committee Member

Dr. Evren Gurkan-Cavusoglu

Committee Member

Dr. Francis Merat

Committee Member

Dr. Daniel Saab

Committee Member

Dr. Francis Wolff

Date of Defense

July 17, 2020

*We also certify that written approval has been obtained

for any proprietary material contained therein.

In memory of my beloved brother Mohsen

Contents

List of Tables	v
List of Figures	viii
Acknowledgments	xv
Abstract	xvii
1 Introduction	1
1.1 Motivation	2
1.2 Thesis Contributions	3
1.3 Thesis Outline	4
2 Background	6
2.1 An Overview of PUFs	6
2.1.1 Security Properties of an Ideal PUF	6
2.1.2 PUF based Authentication Scheme	8
2.1.3 Applications of PUFs	10
2.1.4 Different Variants of PUFs	12
2.1.5 Attacks on PUFs	13
2.2 Current DRAM-based PUF Technologies	15

3	Proposed DRAM Authentication Methodology	18
3.1	Design Architecture	18
3.2	Authentication Methodology	20
4	Simulation Model and Results	23
4.1	Simulation Model	23
4.2	Simulation Results	24
4.2.1	Write Duty Cycle	24
4.2.2	Randomness	25
4.2.3	Uniqueness	26
4.2.4	Robustness	27
4.2.5	Hardware Overhead	32
4.2.6	Summary	32
5	Experimental Setup	34
5.1	High-Performance Chip Tester	36
5.1.1	DUT Board Preparation	37
5.1.2	PinList Preparation	37
5.1.3	Initialization	37
5.1.4	Test Vector Creation	38
5.1.5	Pin and Group Assignments	38
5.1.6	Stimulus Format, Timing, and Logic Levels Definition	39
5.1.7	Downloading Test Vectors	41
5.1.8	DUT Power Setup	42
5.1.9	Run Setup	42
5.1.10	DUT Continuity Test	42
5.1.11	Functional Test Run and Analysis	44
5.1.12	Calibration and Diagnostics	46

5.2	Precision Temperature Forcing System	48
5.2.1	Precision Temperature Control	50
5.2.2	DUT Sensor	50
5.2.3	Integrated Thermal Test Head and Motorized Arm	50
6	Experimental Results on DRAM	51
6.1	DRAM Technology Overview	51
6.2	The PowerUp Approach	53
6.2.1	Stable Cells	53
6.2.2	Randomness	56
6.2.3	Uniqueness	57
6.2.4	Robustness	59
6.3	The WRITE Approach	62
6.3.1	Write Duty Cycle	65
6.3.2	Stable Cells	67
6.3.3	Randomness	70
6.3.4	Uniqueness	71
6.3.5	Robustness	73
6.4	Summary	76
7	Experimental Results on SRAM	79
7.1	SRAM Technology Overview	79
7.2	The PowerUp Approach	80
7.2.1	Stable Cells	81
7.2.2	Randomness	82
7.2.3	Uniqueness	84
7.2.4	Robustness	84
7.3	The WRITE Approach	88

7.3.1	Write Duty Cycle	90
7.3.2	Stable Cells	92
7.3.3	Randomness	95
7.3.4	Uniqueness	95
7.3.5	Robustness	96
7.4	Summary	100
8	Analysis	102
8.1	PUF Based Multi-key Authentication Scheme	102
8.2	PUF Evaluation	104
8.2.1	Cell Stability Evaluation	104
8.2.2	Randomness Evaluation	104
8.2.3	Uniqueness Evaluation	106
8.2.4	Robustness Evaluation	107
8.2.5	Hardware Overhead Evaluation	109
8.2.6	Vulnerability Evaluation	110
8.3	Comparisons	110
9	Conclusion	114
9.1	Summary	114
9.2	Future Research Directions	115
	Bibliography	117

List of Tables

4.1	Summary of Simulation Results	33
5.1	Stimulus Formats Supported by ETS Software (adapted from [1]) . .	40
5.2	Run Setup Parameters (adapted from [2])	43
5.3	Diagnostic Descriptions (adapted from [2])	47
6.1	Percentage of Unstable Cells in the Signatures Obtained from Ten DRAM Chips Using the PowerUp Approach	55
6.2	Fractional Hamming Weight Values for Signatures Obtained from Ten DRAM Chips Using the PowerUp Approach	57
6.3	Inter-die Hamming distance Values for Pairwise Comparison of Signa- tures Obtained from ten DRAM Chips Using the PowerUp Approach	58
6.4	Intra-die Hamming distance Values of Signatures Obtained from ten DRAM Chips Under Temperature Variation Using the PowerUp Ap- proach	60
6.5	Intra-die Hamming Distance Values of Signatures Obtained from ten DRAM Chips Under Supply Voltage Variation Using the PowerUp Ap- proach	62
6.6	Write Duty Cycles for DRAM Chips	67
6.7	Percentage of Unstable Cells in Signatures Obtained from ten DRAM Chips Using the WRITE Approach	69

6.8	Fractional Hamming Weight for Signatures Obtained from ten DRAM Chips Using the WRITE Approach	71
6.9	Inter-die Hamming Distance Values for Pairwise Comparison of Signatures Obtained from ten DRAM Chips Using the WRITE Approach	72
6.10	Inter-die Hamming distance Values of Signatures Obtained from ten DRAM Chips Under Temperature Variation Using the WRITE Approach	73
6.11	Inter-die Hamming distance Values of Signatures Obtained from ten DRAM Chips Under Supply Voltage Variation Using the WRITE Approach	76
6.12	Summary of DRAM Experimental Results	78
7.1	Percentage of Unstable Cells in Signatures Obtained from eight SRAM Chips Using the PowerUp Approach	82
7.2	Fractional Hamming Weight for Signatures Obtained from eight SRAM Chips Using the PowerUp Approach	83
7.3	Inter-die Hamming distance Values for Pairwise Comparison of Signatures Obtained from eight SRAM Chips Using the PowerUp Approach	85
7.4	Intra-die Hamming Distance Values of Signatures Obtained from eight SRAM Chips Under Temperature Variation Using the PowerUp Approach	86
7.5	Intra-die Hamming Distance Values of Signatures Obtained from eight SRAM Chips Under Supply Voltage Variation Using the PowerUp Approach	88
7.6	Write Duty Cycles for Signatures Obtained from eight SRAM Chips Using the WRITE Approach	91
7.7	Percentage of Unstable Bits in Signatures Obtained from eight SRAM Chips Using the WRITE Approach	94

7.8	Fractional Hamming Weight for Signatures Obtained from eight SRAM Chips Using the WRITE Approach	95
7.9	Inter-die Hamming distance Values for Pairwise Comparison of Signatures Obtained from eight SRAM Chips Using the WRITE Approach	96
7.10	Intra-die Hamming distance Values of Signatures Obtained from eight SRAM Chips Under Temperature Variation Using the WRITE Approach	98
7.11	Intra-die Hamming Distance Values of Signatures Obtained from eight SRAM Chips Under Supply Voltage Variation Using the WRITE Approach	99
7.12	Summary of DRAM Experimental Results	101
8.1	Comparison of Results between the Proposed Methodology and the Equivalent SRAM-based Methodology	111
8.2	Comparison of Results between the Proposed Methodology and other DRAM-based Methodologies	113

List of Figures

1.1	IoT security (adapted from [3]).	3
2.1	Utilization of PUF for building secret keys.	7
2.2	Security properties of an ideal PUF (adapted from [4]).	7
2.3	PUF based authentication scheme.	9
2.4	The flow of active hardware metering scheme for counterfeit detection.	10
2.5	Utilizing PUF in a private key-based mechanism for unlocking the IP.	11
2.6	Structure and response bit generation mechanism of memory-based PUF.	13
3.1	DRAM authentication architecture: (a) The PUF consisting of a DRAM array with peripheral circuitry and a delay generator, (b) Circuit diagram of a DRAM cell with basic differential sense amplifier, equalizer, and read and write circuitry.	19
3.2	Simplified voltage waveform for Write-0 and Write-1 operations in DRAM.	20
3.3	Delay unit in DRAM authentication architecture.	21
3.4	Read-out signature of a randomly selected group of DRAM cells after a write operation performed at three different write duty cycles; (a) $Write_a > Write_b$, (b) $Write_b$ (the optimized write duty cycle ensuring equal probability of write success and failure), and (c) $Write_c < Write_b$.	22

4.1	Distribution of the normalized minimum Write-1 duty cycles of all 128 DRAM cells in 1000 chips (the normal distribution fit with the corresponding expected value, μ , are shown in red).	24
4.2	Fractional Hamming weight in a Write-1 operation performed at three different write duty cycles ($Write_a > Write_b > Write_c$) in DRAM.	26
4.3	Inter-die Hamming distance distribution of 1000 DRAM chips for a Write-1 operation performed at the selected write duty cycle.	27
4.4	Average bit-flips in the signatures obtained from 1000 DRAM chips under temperature variation.	28
4.5	Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from 1000 DRAM chips under temperature variation.	29
4.6	Average bit-flips under voltage variation.	29
4.7	Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from 1000 DRAM chips under supply voltage variation.	30
4.8	Average bit-flips in the signatures obtained from 1000 DRAM chips under the NBTI effect.	31
4.9	Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from 1000 DRAM chips under NBTI effect.	31
5.1	DRAM experimental setup (test equipment from Component Engineering lab at Rockwell Automation).	35
5.2	<i>HiLevel</i> ETS test system (adapted from [2])	36
5.3	Example of a PinList file (adapted from [5]).	38
5.4	Example test vectors for DRAM.	39
5.5	Stimulus formats (adapted from [1]).	41
5.6	Analysis window (adapted from [2]).	44
5.7	Analysis Graph mode (adapted from [2]).	45

5.8	Output air nozzle of a T2420 precision temperature forcing system (adapted from [6]).	49
6.1	Block diagram for DRAM (μ PD416-3).	52
6.2	Snapshot of the bit-pattern of a DRAM chip (10 words by 1 bit) after ten PowerUp-read attempts.	54
6.3	Snapshot of the bit-patterns of ten DRAM chips (30 words by 1 bit) after ten PowerUp-read attempts. These snapshots do not represent the full signatures.	55
6.4	Fractional Hamming weight values for the signatures obtained from ten DRAM chips using the PowerUp approach (X axis represents DRAM cell values and Y axis represents the fractional Hamming weight). . .	56
6.5	Inter-die Hamming distance distribution of signatures obtained from ten DRAM chips using the PowerUp approach.	58
6.6	Percentage of fractional Hamming distance variation of signatures ob- tained from ten DRAM chips under temperature variation using the PowerUp approach.	59
6.7	Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from ten DRAM chips under temperature variation using the PowerUp approach.	60
6.8	Percentage of fractional Hamming distance variation of signatures ob- tained from ten DRAM chips under supply voltage variation using the PowerUp approach.	62
6.9	Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from ten DRAM chips under supply voltage vari- ation using the PowerUp approach.	63
6.10	Timing diagram for an early-write cycle for a DRAM (μ PD416-3) chip.	64

6.11	Timing diagram for the initialization and randomization phases using the WRITE approach for extracting PUF signatures from a DRAM (μ PD416-3) chip.	64
6.12	Best write duty cycles for DRAM chips to ensure a 50% rate of success to failure in a Write-1 operation.	66
6.13	Bit-pattern of a randomly selected group of 250 cells in ten DRAM chips when a Write-1 operation is performed at different write duty cycles ranging from 9 to 14 ns. The distribution of unstable cells across the same duty cycle range is shown on right (X axis represents DRAM cell value and Y axis represents the duty cycle in ns. For the bar charts on right, X axis represents the number of unstable cells and Y axis represents the duty cycle in nanoseconds).	68
6.14	Snapshot of the bit-pattern of a DRAM chip (10 words by 1 bit) after ten Write-1-Read attempts.	69
6.15	Snapshots of the bit-patterns of ten DRAM chips after ten Write-1-Read attempts. These snapshots do not represent the full signatures.	70
6.16	Inter-die Hamming distance distribution of signatures obtained from ten DRAM chips using the WRITE approach.	72
6.17	Percentage of fractional Hamming distance variation of signatures obtained from ten DRAM chips under temperature variation using the WRITE approach.	74
6.18	Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from ten DRAM chips under temperature variation using the WRITE approach.	74
6.19	Percentage of fractional Hamming distance variation of signatures obtained from ten DRAM chips under supply voltage variation using the WRITE approach.	76

6.20	Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from ten DRAM chips under supply voltage variation using the WRITE approach.	77
7.1	Block diagram for SRAM (HT6116-70).	80
7.2	Snapshot of the bit-pattern of an SRAM chip (10 words by 8 bits) after each of ten PowerUp-Read attempts.	81
7.3	Snapshots of the bit-patterns of eight SRAM chips (30 words by 8 bits) after ten PowerUp-Read attempts. These snapshots do not represent the full signatures.	82
7.4	Fractional Hamming weight for signatures obtained from eight SRAM chips using the PowerUp approach (X axis represents SRAM cell values and Y axis represents the fractional Hamming weight).	83
7.5	Inter-die Hamming distance distribution of signatures obtained from eight SRAM chips using the PowerUp approach.	84
7.6	Percentage of fractional Hamming distance variation of signatures obtained from eight SRAM chips under temperature variation using the PowerUp approach.	85
7.7	Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from eight SRAM chips under temperature variation using the PowerUp approach.	86
7.8	Percentage of fractional Hamming distance variation of signatures obtained from eight SRAM chips under supply voltage variation using the PowerUp approach.	87
7.9	Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from eight SRAM chips under supply voltage variation using the PowerUp approach.	88
7.10	Modified block diagram for SRAM (HT6116-70).	89

7.11	Timing diagram for the Write Enable signal for SRAM (HT6116-70) without the modified write circuitry.	89
7.12	Timing diagram for the Write Enable signal for SRAM (HT6116-70) with the modified write circuitry.	90
7.13	Best write duty cycle for SRAM to ensure a 50% rate of success to failure in Write-1 operation.	91
7.14	Bit-pattern of a randomly selected group of 250 cells in eight SRAM chips when a Write-1 operation is performed at different write duty cycles ranging from 0 to 25 ns. The distribution of unstable cells across the same duty cycle range is shown on right (X axis represents SRAM cell value and Y axis represents the duty cycle in ns. For the bar charts on right, X axis represents the number of unstable cells and Y axis represents the duty cycle in nanoseconds).	92
7.15	Snapshot of the bit-pattern of an SRAM chip (10 words by 8 bits) after each Write-1-Read attempt.	93
7.16	Snapshots of the bit-patterns of eight SRAM chips (30 words by 8 bits) after ten Write-1-Read attempts. These snapshots do not represent the full signatures.	94
7.17	Inter-die Hamming distance distribution of signatures obtained from eight SRAM chips using the WRITE approach.	96
7.18	Percentage of fractional Hamming distance variation of signatures obtained from eight SRAM chips under temperature variation using the WRITE approach.	97
7.19	Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from eight SRAM chips under temperature variation using the WRITE approach.	98

7.20	Percentage of fractional Hamming distance variation of signatures obtained from eight SRAM chips under supply voltage variation using the WRITE approach.	99
7.21	Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from eight SRAM chips under supply voltage variation using the WRITE approach.	100
8.1	PUF based multi-key authentication scheme.	103

Acknowledgments

Personal Acknowledgments

This work would not be possible without the help and encouragement I received from several people. First and foremost, I would like to express my most sincere gratitude to my advisor, Professor Christos Papachristou, for his continuous patience, excellent leadership, valuable advice, and support to complete this work.

I would also like to express my appreciation to Dr. Francis Wolff for all his help and support, valuable advice, and insightful comments throughout this research work.

I extend my gratitude to the members of dissertation committee for their participation, invaluable advice, and thoughtful comments to increase the quality of this research work.

Besides, I would like to extend my thanks to my managers and colleagues at Rockwell Automation for their continuous support and encouragement. I would like to specifically thank Steve Tiber for all his help and support with the test equipment at the Component Engineering lab at Rockwell Automation. Also, many thanks to my friends in Cleveland who make my life in Ohio more enjoyable.

Most of all, I would like to thank my dear family whom have always been present throughout my life in spite of the distance. At last, but definitely not least, I would like to thank my dear husband, Pedram, for his love, support, patience and encouragement throughout my studies.

Organizational Acknowledgments

I wish to express my sincere appreciation to Rockwell Automation, Inc., for providing the test equipment at the Component Engineering lab in the Mayfield Heights facility for real memory chip experiments.

I would also like to extend my appreciation to Synopsys, Inc., for providing the tools (*HSPICE* and *Design Compiler*) for circuit simulations and synthesis.

A Robust Authentication Methodology Using Physically Unclonable Functions in DRAM Arrays

Abstract

by

MARYAMSADAT HASHEMIAN

The high availability of DRAM in either embedded or standalone form makes it a target for counterfeiting attacks. In this dissertation, we propose a robust and secure authentication methodology against counterfeiting. The authentication is performed by exploiting the intrinsic process variation in write reliability of DRAM cells.

Extensive Monte Carlo simulations performed in *HSPICE* show that the proposed methodology provides high uniqueness of 50.01% average inter-die Hamming distance and good robustness under temporal fluctuations in supply voltage, temperature, and ageing effect over a 10-year lifetime. Furthermore, this methodology incurs very low hardware overhead by utilizing the DRAM array already present in the design.

The proposed methodology has been validated on real DRAM chips with an experimental setup to test different operating conditions. Comparative analysis of results from this work and the existing works published in the literature show that the proposed methodology provides signatures with excellent uniqueness and randomness and higher robustness under varying operating conditions, while being less susceptible to side-channel attacks due to no dependency on memory power-up values.

To further evaluate the effectiveness of the proposed methodology, experiments are performed on real SRAM chips. A comparative analysis of results between SRAM and DRAM shows that DRAM provides higher uniqueness with slightly lower robustness under varying operating conditions. Overall, this work shows that DRAMs can be utilized to provide a robust authentication mechanism in Systems-on-a-Chip that do not have SRAMs or simply require a larger set of challenge-response pairs for authentication purposes without compromising the design footprint.

Chapter 1

Introduction

Over the years, dynamic random access memory (DRAM) has been used in a wide range of high volume electronics applications. DRAM technology has a very low cost per bit, and it offers the highest density RAM, due to the simple 1T1C cell structure, comprising an access transistor and a storage capacitor. DRAM is found either in stand-alone form or embedded in a system-on-a-chip (SoC). Unlike SRAM, standalone DRAM has a huge market in high volume applications, including servers, workstations, PCs, and game consoles.

In the past few years, the use of embedded DRAM (eDRAM) has become widespread as an alternative to embedded SRAM (eSRAM) to satisfy the high-performance and density needs in memory [7, 8, 9]. eDRAM is a DRAM embedded in the same multi-chip package used for mobile integrated processor graphics. Embedding DRAM onto the package adds cost because eDRAM requires additional fab process steps compared with eSRAM. However, when it comes to bandwidth-intense applications, eDRAM has proven to be beneficial for SoC as major area savings offset the process cost.

In this work, an authentication methodology is developed based on a DRAM-PUF to provide resilience against counterfeit attacks. The advantage of the proposed methodology is based on the fact that stand-alone DRAM or the eDRAM already

present in an SoC can be used for generating device-specific signatures without requiring any additional hardware.

Signature generation in DRAM can be accomplished by inducing write failures. The random manufacturing process variation of the cells' parameters across the chip cause some cells to be more vulnerable to failures. The cells' vulnerability patterns are then translated into device-specific signatures. The signatures provide high uniqueness from chip to chip and good robustness under varying operating conditions, making the proposed methodology ideal for authentication purposes.

What follows highlights the significance of having a robust DRAM-based authentication methodology. Major contributions of the thesis are summarized and the organization of the thesis is outlined at the end of the chapter.

1.1 Motivation

Since the inception of the Internet of Things (IoT) in the late 1990s, severe security threats associated with the use of smart devices have drawn increasing attention [10, 11]. Figure 1.1 shows a glimpse of the vulnerability of IoT concerning security threats.

IoT devices pose a unique and challenging scenario for hardware security because of their area-power cost constraints. Traditional software techniques and cryptographic methods are either inadequate or impractical due to the computational effort and permanent storage required to process and maintain the privacy of the secret key.

In this light, Physical Unclonable Function (PUF) comes in handy as an inexpensive and yet effective solution by proposing a radically different way of generating and processing secret keys without having to store the secret key in the hardware [12].

Over the past few years, stand-alone DRAMs have been a target for counterfeiting. Complex SoCs with multiple IP blocks are not exempt from counterfeiting either.

Figure 1.1: IoT security (adapted from [3]).

Verification and authentication play an important role in counterfeit detection.

SRAM-based PUF has been widely investigated as an authentication mechanism [13, 14]. However, little research has been conducted to utilize DRAM for authentication purposes. With the current market for stand-alone DRAM and the rapid growth of eDRAM in future technologies, it is critical to investigate DRAM for authentication purposes.

This work is one of the first works in which DRAM is utilized as a PUF. One of the most important advantages of DRAM PUF over SRAM PUF or other memory-based PUFs is its large input space. Because of a large number of bits available in a typical DRAM, a large set of challenge-response pairs (CRPs) can be generated. This characteristic of DRAM PUF makes it very valuable and unique among all other types of memory-based PUFs.

1.2 Thesis Contributions

This work is the first comprehensive evaluation of DRAM PUF. It develops an authentication methodology based on a DRAM-PUF with the objective to provide resilience

against counterfeit attacks. The advantage of this methodology is based on the fact that the stand-alone DRAM or the eDRAM already present in an SoC can be utilized for generating device specific signatures without requiring any additional hardware.

The authentication methodology proposed in this work is faster by exploiting the write duty cycle than the methods in [15, 16] while providing a much better Hamming distance. Unlike the method in [17], the proposed methodology does not require memory power-up values. The signatures can be simply generated from the regular DRAM used in the device, while it is fully functional for normal storage operations.

This work leverages on access time failures to generate unique signatures in DRAMs. The reliability of cells are evaluated by inducing write failures through precise reduction of write duty-cycle. The duty cycle is reduced to the point that some cells become more vulnerable under process variation and fail the write operation. The cells' vulnerability patterns are then converted into unique signatures and used for authentication purposes.

Extensive simulations are provided to evaluate the effectiveness of the methodology. The generated signatures have high entropy, excellent uniqueness and very good reproducibility under temperature variation. Unlike the previous works, this work also considers the impact of supply voltage variation and ageing effect on the reproducibility of signatures and show that these are very robust under both factors. Experiments on real memory chips (DRAMs and SRAMs) are also performed to validate the simulation results.

1.3 Thesis Outline

In Chapter 2, we provide an overview of PUFs, their security properties, and applications. Next, different variants of PUFs and their vulnerabilities to different attacks

are discussed. Finally, the current DRAM-based PUF technologies are reviewed to conclude this chapter.

Chapter 3 provides the design architecture as well as a detailed description of the proposed DRAM-based authentication methodology.

Chapter 4 describes the *HSPICE* simulation model for the proposed methodology. The simulation results on a variety of security measures including randomness, uniqueness, and robustness are also presented.

Chapter 5 provides an overview of the experimental setup and the test equipment used to extract the PUF signatures from real DRAM and SRAM chips. The test equipment includes high performance chip testers and a precision temperature forcing system.

Chapter 6 presents the experimental results obtained from DRAM chips. The experiments are performed using two different methodologies to extract PUF signatures; 1) the power-up methodology, and 2) the proposed wordline controlled-duty-cycle methodology presented in this work.

Chapter 7 presents the experimental results obtained from SRAM chips following the same methodologies used in Chapter 6.

Chapter 8 provides an analysis on different security measures discussed in the context of the proposed authentication methodology, followed by a comparative analysis of results obtained from DRAMs and SRAMs.

Finally, Chapter 9 concludes the dissertation with a general discussion highlighting the contributions of this research followed by recommendations for future research directions.

Chapter 2

Background

2.1 An Overview of PUFs

PUF is a function embodied in a physical structure. It utilizes the random process variation within a silicon device to map a response to a given challenge. PUF response is highly random over a sample of the same type of devices but is unique to each device, and more importantly, is highly repeatable. PUF represents the silicon fingerprint and can be used to build a secret key. The utilization of PUFs for building secret keys is demonstrated in Figure 2.1.

This chapter provides an overview of PUFs along with their security properties. Then a PUF based authentication scheme is described followed by an overview of different applications of PUFs. Next, different types of PUFs are presented with an assessment of their vulnerabilities to different types of attacks. Finally, the current DRAM-based PUF technologies are reviewed to conclude this chapter.

2.1.1 Security Properties of an Ideal PUF

Figure 2.2 illustrates the security properties of an ideal PUF. An ideal PUF is:

- ***Reproducible*** – PUF response to the same challenge can be reproduced over

Figure 2.1: Utilization of PUF for building secret keys.

Figure 2.2: Security properties of an ideal PUF (adapted from [4]).

time and a wide range of operating conditions

- **Unique** – PUF response to a challenge is distinguishable from the response generated by the same PUF on another device when the same challenge is applied
- **Unclonable** – PUF cannot be physically or mathematically cloned. Physical unclonability means that it is infeasible to construct a PUF with the same challenge–response behavior as another given PUF because exact control over the manufacturing process is infeasible. Mathematical unclonability means that

it should be very hard to compute an unknown response given the other known CRPs of the PUF. This is because a response is created by a complex interaction of the challenge with many or all of the random components. In other words, given the design of the PUF system, without knowing all of the physical properties of the random components, the CRPs are highly unpredictable. The combination of physical and mathematical unclonability makes PUF truly unclonable.

- ***One-way*** – PUF is a one-way function. It is easy to evaluate in one direction but hard to reverse in the other.
- ***Unpredictable*** – PUF response to an arbitrary challenge cannot be predicted from the known CRPs of the same PUF instance.
- ***Tamper-Evident*** – PUF is designed to reveal any interference with the contents. Any physical attempt to maliciously modify PUF will result in a malfunction in the chip.

2.1.2 PUF based Authentication Scheme

Today, PUFs are usually implemented in integrated circuits (ICs) and are typically used in applications with high security requirements. Figure 2.3 shows a typical PUF based authentication scheme between Alice and Bob. Alice is the trusted party and Bob is the receiver. Alice who has access to the authentic device collects a set of challenge-response pairs (c, r) generated from the PUF instance P and stores them in a database for subsequent communication with Alice in a public network. P is then delivered to Bob through the untrusted supply chain so that Bob can use P for subsequent communications with Alice in a public network.

To authenticate P , Alice randomly selects an unused challenge c_i and sends it to Bob. Bob applies c_i to P to generate a response r_i' and sends it back to Alice. Alice

Figure 2.3: PUF based authentication scheme.

validates r'_i against the database [18]. If the CRP matches, then Bob has an authentic P . It is assumed that only Alice and Bob can produce the correct CRPs. Because of the exponentially large CRP space, the binary channel used for interrogation of challenges and responses can be non-confidential.

An untrusted but reliable physical delivery channel for transportation of P is hypothesized in which an adversary can have read-only access during the manufacturing process or transit of P through the channel. To prevent the PUF from falling into the hands of an adversary who can use it directly to impersonate Bob, acknowledgment of its receipt by Bob through a private channel should be received within a reasonable time before P can be used for subsequent authentications through the unprotected public channel.

To avoid playback attacks, a unique challenge should be used for each round of authentication. Therefore, it is important that Alice stores a sufficiently large number of CRPs and periodically refreshes the CRP database [19].

Figure 2.4: The flow of active hardware metering scheme for counterfeit detection.

2.1.3 Applications of PUFs

PUFs have a wide range of application; from the traditional unique serial numbering, secret key generation, random number sequence generation, to more advanced cryptographic protocols (like Oblivious Transfer [20], Bit Commitment [20], Key Exchange [21]) and Active HW Metering which enables chip designers to lock and unlock the circuit functionality to gain post-fabrication control of their intellectual property (IP).

A typical flow of an active hardware metering scheme is shown in Figure 2.4. With the dominant horizontal semiconductor business model, the physical design of IP is at the disposal of the merchant foundry [22]. The designer has no control over the fabrication process, quantities of production and any added circuitry. To turn the situation around, the IP designer can actively track each fabricated chip by keeping them locked automatically upon fabrication until it is activated by a unique passkey provided by the designer.

To gain post-fabrication control, the designer embeds a lock and a PUF with Error

Figure 2.5: Utilizing PUF in a private key-based mechanism for unlocking the IP.

Correction Code (ECC) to improve its reliability in the circuit before the Graphic Database System (GDS) file of the circuit layout is generated for the foundry to produce the contracted number of ICs. The challenge supplied by the designer is applied to the fabricated chips and the responses generated from their embedded PUFs are collected by the foundry and sent back to the IC designer for authentication. For each successfully authenticated IC, the designer selects a response (to a known challenge) to compute a passkey for the foundry to activate the chip so that it can be tested in operational mode.

Active hardware metering is made feasible by using PUF as a unique and unclonable chip identifier. The locking mechanism needs to be designed in such a way that the passkey used to activate the IP can only be generated by its designer based on the response of the embedded PUF to a given test vector. The manufacturer cannot unlock the IP without the authorization of the designer even if he can measure the CRPs of the PUF.

Figure 2.5 shows an example of a private key-based mechanism to unlock the IP. PUF is interfaced to a Boosted Finite State Machine (BFSM) which is created by adding redundant states and transitions to an original FSM design. K , K' and K'' are respectively the original, additional and total number of states in the BFSM. The original states of the FSM are shaded, and the redundant states are unshaded.

When the chip is powered up, the PUF will generate an initial state code from the challenge provided by the designer. Because of the exponential number of the redundant states, it is highly possible to lock the IC into one of the nonfunctional states among the K'' states.

The BFSM is designed such that there is only one valid route from each redundant state to the reset state. For the example, the PUF response sets the BFSM in the nonfunctional initial state S_0 and the functional reset state S_r could only be reached by a passkey that triggers the transitions $x_1 \rightarrow x_2 \rightarrow x_3 \rightarrow x_4$. Therefore, without knowing the structure of BFSM or the passkey of the designer, the probability of correctly traversing from any nonfunctional redundant state to the functional reset state by random guess is very small.

2.1.4 Different Variants of PUFs

In the past few years, silicon-based PUFs have become an important authentication and anti-counterfeiting measure. The concept of silicon PUF was first introduced by Devadas in 2002 [23]. Since then, several silicon PUFs have emerged. There are two main classes of silicon PUFs: (a) the PUFs exploiting delay variations and (b) the PUFs exploiting the state of memory cells [24].

Ring oscillator (RO)-based PUF [25] and Arbiter PUF [23] are the most well-studied delay-based PUFs which use the random delay variations to produce a digital signature. These PUFs are not very suitable to authenticate integrated circuits as they are power inefficient and rely on dedicated circuitry solely added for unique signature generation and hence present large area overhead which might not be feasible for all designs.

Memory-based PUFs utilize the memory arrays already present on the hardware for unique signature generation. A typical memory-based PUF exploits the metastable states of cross-coupled inverters to generate random bits during reset. Fig-

Figure 2.6: Structure and response bit generation mechanism of memory-based PUF.

Figure 2.6 shows the structure and response bit generation mechanism of memory-based PUF. The response bit is determined by which of the two identically sized inverters in a memory cell addressed by the challenge bit reaches its trip point faster.

One example of memory-based PUF is the SRAM PUF by Intrinsic ID [14] which has been deployed in many FPGAs and microcontrollers for authentication purposes. Another example is memory failure-based PUF [26, 27] which exploits the random memory failures in SRAM cells to generate unique signatures.

2.1.5 Attacks on PUFs

PUF has successfully eliminated the need for a persistent presence of a secret key in on-chip non-volatile memory (NVM), which reduces the risk of backdoor attacks on crypto-systems with a “secure golden key”.

As the device needs to be powered on to apply the challenge before its response can be measured, PUF is inherently tamper-evident. Any invasive attack or physical manipulation will upset its CRP mapping and render the PUF unusable.

Many PUFs are not used standalone. While it may be difficult to hack the PUF directly, PUF can be attacked by side-channel leakage through components built around its input/output signal interface. Many research works have shown that cer-

tain PUF structures can also be mathematically modeled and cracked by Machine Learning algorithms. What follows describes two popular types of attacks on PUFs.

A. Machine Learning -based Modeling Attacks

The most popular attack on PUFs is Machine Learning (ML) based modeling attacks. This kind of attack targets strong PUFs with a large number of CRPs [12]. Modeling attacks are usually implemented by deriving a numerical simulation model of the PUF. An ML algorithm is then used to predict its output responses to unknown challenges by training the machine learner with a subset of known CRPs [28]. Those CRPs can either be collected from direct access to PUF or by eavesdropping the protocol.

A four XOR 64-stage Arbiter-based SLPUF can be successfully attacked in no more than 155 hours with reasonable input size [29]. Becker’s experimental results proved the power of advanced ML techniques that some strong PUFs can be accurately modeled even without direct access to their native challenges and responses. Unfortunately, there is no easy way to strengthen these PUFs against ML attacks without inflicting a higher computational burden on the authentication process.

B. Side-Channel Attacks

Side-channel attacks refer to a group of attack techniques that exploit the measurable parameters of the physical implementation of a cryptographic algorithm or protocol to extract the secret key. The side-channels may be power dissipation, timing, temperature, electro-magnetic emanations, optical signal emissions, acoustic signals or any combination of them [30].

Keeping the hardware security primitive as a black box to resist crypto-analysis has proven to be ineffective as some side-channel attacks can succeed even without knowing the circuitry and its internal operations.

Side-channel attacks can also augment ML when the latter becomes computation-

ally impractical to model more sophisticated enhanced strong PUF structures [31]. A hybrid attack [32] that combines power side-channel with conventional ML attacks was successfully mounted against XOR arbiter PUF and LW PUF of more than 64 stages with up to nine parallel arbiter chains.

Although it is harder to attack memory-based PUFs by ML-based modeling due to their independent bit cells, memory itself can be easily characterized through side-channel attacks with the high spatial density and availability of the full physical response upon power-up. Helfmeier et al [33] have successfully produced a physical clone to replicate the startup behavior of a two-Kilobyte SRAM in an Atmel micro-controller chip ATmega328P by mounting a semi-invasive side-channel attack from the backside of the device to evade all the on-die tamper detection countermeasures. The power-on state of the entire SRAM was fully characterized by observing the near-infrared photonic emissions of the circuit.

Non-invasive cloning attack is also feasible on volatile memory. The attack [34] exploits the fact that the content of volatile memory will not vanish immediately but decays slowly over time when the supply voltage is removed or decreased. The startup states of all memory elements can be read by powering up the memory to the nominal voltage after it has been powered off for a precise time.

2.2 Current DRAM-based PUF Technologies

Besides this work, only a few other investigations have been conducted on DRAM PUF. What follows provides a review of these research works.

A. Refresh OFF -based DRAM PUF [15]

This approach is based on initializing all DRAM cells to ‘1’. With the refresh cycle being disabled, some cells leak to ‘0’. Due to the intrinsic process variation in DRAM

cells, the discharge rate of the storage capacitor is different from cell to cell, resulting in random data loss which can be extracted as a unique digital identifier.

When retrieving the cell charge, timing is an important factor. If the storage cells are read too early, almost no change has occurred. If the storage cells are read too late, the charge has vanished, and no information can be extracted. Therefore, an optimal time window has to be found after every startup.

The major drawback of this method is that the time required to observe the decays (evaluate the PUF response) can extend to hours, making this methodology impractical as a PUF. Moreover, this work does not provide an analysis on security measures such as uniqueness and robustness which are essential metrics for evaluating PUF's behavior.

B. Power OFF -based DRAM PUF [16]

In this method, instead of turning the refresh cycle off, power is turned off. This accelerates the cell leakage, and therefore reduces the challenge time from hours to minutes. Although the time required to evaluate the PUF response is reduced, still this method is highly timing dependent and therefore is not very practical. Moreover, this method suffers from lack of robustness under environmental conditions.

C. PowerUp -based DRAM PUF [17]

This work presents an enrollment algorithm to produce unique 128-bit signatures from DRAM. Signatures are generated by reading the startup values of DRAM during power-up. Unlike the methods in [15, 16], this work provides a comprehensive evaluation of PUF in terms of randomness, uniqueness, and robustness (stability) under temporal fluctuations and ageing.

Although the proposed methodology provides great results in terms of randomness and uniqueness, it does not provide strong stability under temperature or voltage

variations. Moreover, due to dependency on power-up values, the proposed DRAM PUF can be vulnerable to side-channel attacks, and therefore might not be suitable for authentication purposes.

Chapter 3

Proposed DRAM Authentication Methodology

This chapter provides the design architecture followed by a description of the proposed authentication methodology realized in a DRAM array.

3.1 Design Architecture

The concept of this methodology can be explained with the help of the architecture shown in Figure 3.1. Authentication is performed through a PUF realized in a DRAM array. The PUF consists of a basic DRAM array along with peripheral circuitry and a delay generator which introduces a negligible area overhead. The core circuitry of a DRAM array includes a DRAM cell with a differential sense amplifier, equalizer, and read and write circuitry [35].

Figure 3.2 reviews the signal transitions in a standard DRAM cell during Write-0 and Write-1 operations. The word line signal (WL) is driven to a voltage higher than the supply voltage (VDD) to allow a full voltage level to be written to the storage capacitor through the access transistor. Before sensing, the equalization signal (EQ) is asserted to pre-charge the bit lines (BL/BL^*) to $VDD/2$.

Figure 3.1: DRAM authentication architecture: (a) The PUF consisting of a DRAM array with peripheral circuitry and a delay generator, (b) Circuit diagram of a DRAM cell with basic differential sense amplifier, equalizer, and read and write circuitry.

To begin an active row cycle, first, EQ is de-asserted. Next, WL is asserted to share the charge between the storage and bit line capacitors. The sense amplifier is then activated by driving the sensing signals, PR and PS , from $VDD/2$ to VDD and VSS respectively. After the assertion of the sensing signals, the bit lines are driven to full voltage levels. Finally, the column select line (CSL) turns on the output transistor and allows the fully driven voltage to reach the output. At the same time, the access transistor remains open to restore the data in the DRAM cell. There is a differential bidirectional data bus (D/D^*) which is shared by a column of sense amplifiers and is used during a write operation. The Write Enable signal (WEN) connects the data bus to the bit line pairs. In the case of a write operation, the data bus provides a larger current to overdrive the sense amplifier and the bit line voltage. The DRAM cell would then be overwritten by the data values asserted to the data bus.

Figure 3.2: Simplified voltage waveform for Write-0 and Write-1 operations in DRAM.

3.2 Authentication Methodology

Large dense structures like DRAMs are particularly susceptible to process variation. The existing inter-die and intra-die variations in the device parameters, cause a mismatch in the cells' strength. As a result, DRAM cells are not equally strong. Due to the random nature of process variation, some cells experience more variation and fail to operate. These failures can be exploited to generate unique signatures that can be used for DRAM authentication.

The failure mechanisms that can be observed in a DRAM cell include:

- **Data retention failure** – when a cell loses its value after some amount of time; less than the amount required by DRAM refresh
- **Access time failure** – caused by signal transitions in the address decoders that are too fast or too slow
- **Transition failures** – where a cell can be written from '0' to '1', but not from '1' to '0', or the other way around

Figure 3.3: Delay unit in DRAM authentication architecture.

The idea of exploiting failures has been earlier investigated to generate unique signatures in SRAM [26, 27]. In this research work, the access time failure-based approach has been exploited to generate unique signatures in DRAM. The reliability of cells has been evaluated by inducing a write failure through a precise reduction of the write duty cycle. A delay unit, consisting of a chain of inverters, a multiplexer, and an AND gate is used to shorten the write duty cycle [26]. Figure 3.3 shows the delay unit used in DRAM authentication architecture.

To write a value into a DRAM cell, first, WL is selected. Next, the sense amplifier is temporarily forced to the desired value, causing the BL to charge or discharge the storage capacitor accordingly.

In a normal write operation, the write duty cycle is selected, such that all DRAM cells can successfully perform the write operation under all process corners. In the proposed methodology, however, the write duty cycle is shortened intentionally, such that some cells become unstable under process variation and fail the write operation.

The concept of the proposed methodology can be further explained with the help of the illustration shown in Figure 3.4. This figure compares the readout signature of a randomly selected group of DRAM cells after a write operation is performed using three different duty-cycles; $Write_a > Write_b > Write_c$.

First DRAM cells are initialized with 0's using a normal write operation. Then a write operation is performed as shown to write 1's. Figure 3.4.a shows that most of the write attempts succeed under $Write_a$. This results in more 1's in the readout

Figure 3.4: Read-out signature of a randomly selected group of DRAM cells after a write operation performed at three different write duty cycles; (a) $Write_a > Write_b$, (b) $Write_b$ (the optimized write duty cycle ensuring equal probability of write success and failure), and (c) $Write_c < Write_b$.

signature. As duty-cycle decreases, more write attempts fail, which results in having more 0's in the signature, as shown in Figure 3.4.c. The ideal write duty-cycle for PUF is shown in Figure 3.4.b, where the ratio of write success to failure is one-to-one, which results in having a balanced number of 0's and 1's in the readout signature.

The methodology described in this chapter is utilized to extract unique signatures from memory chips at both simulation and experimental level. The following chapters present the observations made from *HSPICE* simulations [36], and experiments on real memory chips (DRAMs and SRAMs) using the test equipment at Rockwell Automation.

Chapter 4

Simulation Model and Results

This chapter describes the Monte Carlo simulations performed in *HSPICE*, and presents the results on the adjusted write duty cycle, as well as the security measures including randomness, uniqueness, and robustness. Different metrics such as min-entropy, Hamming distance and Hamming weight have been used to evaluate the quality of PUF. Finally, the results on hardware overhead are presented.

4.1 Simulation Model

The proposed DRAM authentication methodology has been implemented with a 128-cell DRAM architecture including a 16×8 embedded DRAM array, sense amplifiers, equalizers, and read/write circuitry designed for the 45 nm low power Predictive Technology Model (PTM) [37]. The synthesis for the peripherals including address decoder, I/O with buffers, and delay generator is performed in Synopsys *Design Compiler*.

Extensive Monte Carlo simulations were carried out using Synopsys *HSPICE* for 1000 chips to generate 128-bit signatures. To introduce process variation, 10% inter and 8% intra-die variation on threshold voltage (V_{th}) are considered. These are the typical process variation numbers for inter-die and intra-die variations.

Figure 4.1: Distribution of the normalized minimum Write-1 duty cycles of all 128 DRAM cells in 1000 chips (the normal distribution fit with the corresponding expected value, μ , are shown in red).

4.2 Simulation Results

4.2.1 Write Duty Cycle

Measurements are performed for each DRAM cell to identify the minimum write duty cycle required to perform a successful Write-1 operation. Figure 4.1 shows the distribution of the measurements for 128 DRAM cells in 1000 chips. The mean of the distribution is chosen as the write duty cycle for PUF to ensure an equal probability of Write-1 success and failure.

The delay generator in the proposed methodology can be used as a write duty cycle controller, to evaluate the vulnerability of cells during write access and to induce failures using an appropriate write duty cycle.

In the proposed methodology, a unique CRP can be generated following these three steps:

- **Step 1** – Choosing randomly selected cells as part of the input challenge
- **Step 2** – Performing a Write-1 operation at the reduced write duty cycle
- **Step 3** – Extracting the cell values as part of the output response

The choice of 128 cells was proven to be a good number of cells in terms of the simulation results shown later. The number of chips is also chosen to be 1000 which is a typical number of iterations in Monte Carlo simulations.

Given the size of DRAM, and therefore the huge number of CRPs, it is practically infeasible to exhaustively evaluate all the challenges within a realistic time. The probability of correctly predicting the response to a randomly chosen unknown challenge is very low even with the knowledge of many other CRPs.

4.2.2 Randomness

PUF responses (also known as signatures) need to be random. Randomness is a measure of unpredictability of the response to a given challenge despite prior knowledge of a large number of CRPs.

Randomness can be evaluated using statistical tests such as the NIST test [38], Shannon entropy, or min-entropy. In this work, the min-entropy estimation is used to measure the randomness of PUF signatures. The ideal value for min-entropy is 1, which indicates PUF signatures are highly random and therefore unpredictable.

To measure the randomness of signatures, the min-entropy of DRAM PUF [39, 40, 41] is estimated. For the proposed methodology, the min-entropy per cell is found to be 0.97 which is very close to the ideal min-entropy of 1.0.

It is also desirable for a PUF signature to have a fractional Hamming weight of 50% since this indicates that the PUF is unbiased, and the cells have no preference for a certain state ('0' or '1'). Hamming weight is the percentage of non-zero bits in a signature.

Figure 4.2 shows the fractional Hamming weight (tendency toward '1') for each cell in a Write-1 operation performed at three different write duty cycles; $Write_a$, $Write_b$, and $Write_c$, where $Write_a$ is longer than $Write_b$, and $Write_b$ is longer than $Write_c$. As it is shown, the middle plot performed at the selected write duty cycle,

Figure 4.2: Fractional Hamming weight in a Write-1 operation performed at three different write duty cycles ($Write_a > Write_b > Write_c$) in DRAM.

$Write_b$, has a 50.15% average fractional Hamming weight, indicating that the PUF is perfectly unbiased. However, the top plot performed at $Write_a$ has a higher average fractional Hamming weight, due to a longer write duty cycle which results in fewer write failures. Similarly, the bottom plot performed at $Write_c$ shows a lower average fractional Hamming weight, due to a shorter write duty cycle which results in more write failures.

4.2.3 Uniqueness

For Authentication purposes, PUF signatures need to be as unique as possible. Uniqueness is a measure of how dis-similar or uncorrelated the signatures are from chip to chip (where chip refers to a packaged die). The less correlated the signatures, the less vulnerable they are against ML attacks.

To quantify the uniqueness of signatures, the inter-die Hamming distance is computed. Hamming distance is equivalent to the number of bit positions at which two

Figure 4.3: Inter-die Hamming distance distribution of 1000 DRAM chips for a Write-1 operation performed at the selected write duty cycle.

bit strings (signatures) are different. An ideal PUF has an average inter-die Hamming distance of 50%, which means half of the bits prefer a different state. This makes predicting the PUF signature more difficult, given a collection of known signatures.

Figure 4.3 shows the distribution of inter-die Hamming distance of 1000 signatures generated by performing a Write-1 operation at the selected write duty cycle. The horizontal axis represents the percentage of bits differing between two signatures, and the vertical axis represents the number of pairwise comparisons corresponding to a Hamming distance. For 1000 signatures, 499,500 pairwise signature comparisons are performed. The average inter-die Hamming distance is found to be 50.01% which is very close to the ideal value of 50%, showing that the proposed PUF provides highly unique signatures.

4.2.4 Robustness

PUF signatures need to be robust. Robustness measures the reproducibility of signatures under varying operating conditions, such as temperature, supply voltage, or ageing. For a PUF to be considered robust, the signature obtained at non-ideal operating conditions should not differ significantly from the one obtained under normal

Figure 4.4: Average bit-flips in the signatures obtained from 1000 DRAM chips under temperature variation.

conditions.

The robustness of PUF signatures is estimated through computing the intra-die Hamming distance between the signatures from the same chip subject to varying operating conditions.

A. Robustness under Temperature Variation

Temperature variations affect PUF's behavior (signature). To estimate the robustness of PUF under temperature variation, the average intra-die Hamming distance among the signatures is estimated under varying temperature. Temperature is varied from 20°C to 50°C in 5°C increments. As Figure 4.4 shows, the highest average signature variation is 18.9 bit-flips which occurs at 50°C where the circuit performance is affected the most.

Figure 4.5 shows the distribution of average intra-die Hamming distance of the signatures obtained from 1000 chips under temperature variation. As it is shown, most of the chips (94%) have fewer than 18 bit-flips in their signatures, including 200 chips with not a single bit-flip, showing that the proposed PUF is stable even at varying temperatures.

Figure 4.5: Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from 1000 DRAM chips under temperature variation.

Figure 4.6: Average bit-flips under voltage variation.

B. Robustness under Voltage Variation

Voltage variations affect PUF's behavior (signature). To estimate the robustness of PUF under voltage variation, the average intra-die Hamming distance among the signatures is estimated under varying supply voltage. The voltage level is varied from 80% to 110% of the nominal voltage (1.1 V) in steps of 100 mV. As Figure 4.6 shows, the highest average signature variation is 14.9 bit-flips which occurs at 0.9 V where the circuit performance is affected the most.

Figure 4.7: Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from 1000 DRAM chips under supply voltage variation.

Figure 4.7 shows the distribution of average intra-die Hamming distance of the signatures obtained from 1000 chips under supply voltage variation. As it is shown, most of the chips (90%) have fewer than 25 bit-flips in their signatures, including 230 chips with not a single bit-flip, showing that the proposed PUF is stable even at varying voltage levels.

C. Robustness under Ageing Effect

Ageing effect, particularly Negative Bias Temperature Instability (NBTI), can also impact PUF's behavior (signature). Ageing can cause degradation of V_{th} in PMOS transistors. There are PMOS transistors in the sense amplifier circuitry of DRAM. Degradation of V_{th} in these transistors can affect the reproducibility of PUF signatures. To investigate the robustness of signatures under NBTI, the PMOS technology file is updated according to the expected V_{th} shift corresponding to 1, 3, 5, and 10 year lifetime of the product [42].

Simulation results in Figure 4.8 show that even the highest average signature variation under the NBTI effect is very low due to the small number of PMOS transistors

Figure 4.8: Average bit-flips in the signatures obtained from 1000 DRAM chips under the NBTI effect.

Figure 4.9: Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from 1000 DRAM chips under NBTI effect.

in DRAM array circuitry. The highest average signature variation is only 1.45 bit-flips which occurs after 10 years where the V_{th} of PMOS is at its peak.

Figure 4.9 shows the distribution of average intra-die Hamming distance of the signatures obtained from 1000 chips under NBTI effect. As it is shown, the majority of the chips (98.9%) have less than three bit-flips in their signatures, including 750 chips with not a single bit-flip, showing that the proposed PUF is perfectly stable under NBTI effect.

4.2.5 Hardware Overhead

For the proposed DRAM authentication methodology, a 128-cell DRAM architecture is designed, including sense amplifiers, equalizers, and read and write circuitry using Synopsys *HSPICE*. Synthesis for the peripherals, such as the 4×16 row address decoder, the 8-bit I/O with buffers, and the delay generator has been done in Synopsys *Design Compiler*.

For the proposed authentication methodology, since the DRAM utilized is already present in the design, the area overhead is only due to the delay generator. For the experimental DRAM, which is less than 1 KB, the area overhead is only 7%.

4.2.6 Summary

Table 4.1 summarizes the simulation results presented in this chapter. A comprehensive evaluation of DRAM PUF was presented in terms of uniqueness, entropy, and robustness under varying environmental conditions and ageing.

The authentication methodology proposed in this work incurs very low design overhead by utilizing the DRAM array already present in the design. Also, the authentication time takes only a few nanoseconds due to the nature of the proposed approach.

Using the Hamming distance metric, the number of bits differing between two random signatures is found to be 50.01%, showing that the signatures generated using the proposed approach are highly unique.

Furthermore, the proposed methodology provides a normalized min entropy of 0.97 which is very close to the ideal value of 1.0. This indicates that the signatures generated using the proposed approach are highly unpredictable.

Finally, simulation results show that the proposed methodology provides a good level of robustness under temperature and voltage variation, as well as ageing. This shows that the signatures generated using the proposed approach have a good level

<i>HSPICE</i> Simulation Results	
Hardware Overhead	7% (for a 128-cell DRAM Architecture)
Authentication Time	Nanoseconds
Uniqueness	50.01%
Normalized Min-entropy	0.97
Robustness under Temperature Variation	93.03% (20°C – 50°C)
Robustness under Voltage Variation	92.81% (0.9 V – 1.2 V)
Robustness under Ageing	99.20% (10 Years)

Table 4.1: Summary of Simulation Results

of reproducibility even under varying operating conditions.

Chapter 5

Experimental Setup

This chapter provides an overview of the test equipment that creates the backbone of the experimental setup used in the subsequent chapters. The test equipment is used to extract PUF signatures from real memory chips under varied environmental conditions. The experiments are described in detail in Chapters 6–7. A comparative analysis of results is also provided in Chapter 8.

To perform the experiments, the test equipment from the Component Engineering lab at Rockwell Automation is used. High-performance chip testers, also shown in Figure 5.1, are used to analyze and validate the variability behaviors of memory cells concerning the results from circuit simulations presented in Chapter 4. The testers are programmed to perform read and write operations. They also provide control on the timing of input/output signals, which enables adjusting the write duty-cycle for the proposed methodology. A temperature forcing system is also used to evaluate PUF stability under temperature variation by heating or cooling the memory chips in their test socket with temperature-controlled air while extracting signatures.

The experimental setup includes:

- *HiLevel* ETS770 tester with test rates up to 50 MHz [43]
- *HiLevel* Griffin tester with test rates up to 100 MHz [43]

Figure 5.1: DRAM experimental setup (test equipment from Component Engineering lab at Rockwell Automation).

- *Thermonics* T-2420 temperature forcing system [6]
- *TI* SN54S09 quadruple 2-input positive-AND gates [44]
- Ten *NEC* μ PD416-3 $16K \times 1$ -Bit Dynamic MOS RAM [45]
 - Double-poly-layer N channel silicon gate process
 - 128 refresh cycles
 - Minimum Read-Write cycle time (t_{RWC}) = 320 ns
- Eight *Holtek* HT6116-70 CMOS $2K \times 8$ -Bit Static RAM [46]
 - 0.8 μ m CMOS Process
 - Minimum Write pulse (t_{WP}) = 25 ns

Figure 5.2: *HiLevel* ETS test system (adapted from [2])

Before each round of measurements, a calibration test including a clock generator test is performed to make sure the tester is fully calibrated, and the clock failure is less than the maximum allowable deviation of 1%.

5.1 High-Performance Chip Tester

Two high-performance chip testers from *HiLevel Technology* are used to analyze the variability behaviors of memory cells. Figure 5.2 shows a *HiLevel* ETS test system. The test system operates on a Windows platform and creates or simulates the environment that the device under test (DUT) may be in during actual operation. The test system also provides the capability to perform functional testing to ensure that

the DUT, in this case memory chips, operates according to its truth table. The memory chip's Input is stimulated with all possible bit combinations necessary to toggle every internal node and to execute every logical or mathematical function that the part is capable of [2]. The sections that follow provide the main steps in preparation for a functional test [47].

5.1.1 DUT Board Preparation

The accuracy of test results relies heavily on the integrity of the DUT board. A balanced 50 Ohm impedance, proper bypass capacitors, and nearly equal signal paths, all contribute to high-quality DUT interfacing [2]. A wide variety of unusual symptoms appearing in test environments are found to be attributable to *VDD* fluctuations caused by unsuppressed transients, rather than by some fault of the tester [48]. To filter the transient frequencies, bypass capacitors (0.01 μ f) are connected between the device power supply pins and tester ground [2, 48, 49].

5.1.2 PinList Preparation

Once the pins are defined, a PinList is created using the ETS software. PinList is a table correlating the memory chip's pins and System Channels (tester pins) to reflect the wiring. PinList also provides information about pin group number, and type of pin (Input, Output, Bidirectional, and Split cycle I/O [50]). Figure 5.3 provides a PinList example. PinList is saved in ASCII format and imported in future testing efforts [2].

5.1.3 Initialization

Before pins are defined, the test system hardware is reset to a known state using Initialize. This clears all setups in the software, including the test vectors [2].

```

PinList for C:\Symphony\74F161.txt
;SysCh  Pin#  Name    Grp   Type (IOBS)
 10      7    CET     5     I
 11      6    P3      2     I
 12      5    P2      2     I
 13      4    P1      2     I
 14      3    P0      2     I
 15      2    CLK     3     I
 16      1    MR      6     I
 25      9    PE      4     I
 26     10    CET     5     I
 27     11    Q3      1     O
 28     12    Q2      1     O
 29     13    Q1      1     O
 30     14    Q0      1     O
 31     15    TC      1     O

$End

```

Figure 5.3: Example of a PinList file (adapted from [5]).

5.1.4 Test Vector Creation

Test vectors are patterns of ‘1’s and ‘0’s applied to and expected from the memory chip’s pins during one test cycle. Valid test vectors are created to properly exercise the memory chip using a thorough inputs truth table [51]. Once the functional test vectors are executed, the actual data that was captured from the output pins is compared against the expected response data, and if they do not match, a failure is indicated [2]. Figure 5.4 shows example test vectors for reading five words (1 bit each) in a DRAM chip. The data input (*DIN*) is ignored during read operations. All five test vectors indicate failures as L’s (0’s) were captured while H’s (1’s) were expected.

5.1.5 Pin and Group Assignments

Part of the pin definition effort requires entering pins from the pin list to the defined groups. System channel numbers are the reference for grouping pins, but they are

Vector	W												Last Trc	Comments
Address	R												Sequence	
(Decimal)	R	C	I									D O	716	
	A	A	T	A	A	A	A	A	A	A	I	U	(Dec)	
	S	S	E	0	1	2	3	4	5	6	N	T		
=====														
35	0	0	1	0	0	1	1	1	1	0	1	L	- 679	
Expected	-----H-													
49	0	0	1	0	1	0	1	1	1	0	1	L	- 665	
Expected	-----H-													
63	0	0	1	0	0	0	1	1	1	0	1	L	- 651	
Expected	-----H-													
77	0	0	1	0	1	1	0	1	1	0	1	L	- 637	
Expected	-----H-													
91	0	0	1	0	0	1	0	1	1	0	1	L	- 623	
Expected	-----H-													

Figure 5.4: Example test vectors for DRAM.

not very meaningful for working with the tests. To make testing easier, a memory chip's pin number is assigned to each tester channel, as well as a signal name [2].

5.1.6 Stimulus Format, Timing, and Logic Levels Definition

Stimulus refers to a data pattern that will be used for the memory chip's Input pins [2]. When stimulus data is forced out to the Input pins, it may need to be applied in a certain way. It is known, for example, that very often the data must be present at input pins before the clock edge occurs, allowing sufficient setup time. Stimulus formats help with shaping the stimulus data to conform to follow the needs of the chip [1]. Table 5.1 provides a brief description of the stimulus formats supported by the ETS software.

Good knowledge of the memory chip's requirements and timing diagrams is needed to select the right format for each pin group. Proper use of the stimulus formats is crucial for timing measurements [53]. For the PUF experiments, NRZ is used unless

Stimulus Format	Description
NRZ	Non-return to zero – Vector data-driven to the DUT remains at a specified logic level for a period of time equal to one entire test cycle. This is not limited to cycle boundaries and can begin anywhere in a test cycle according to the delay value specified by a timing generator value (Leading Edge).
RZ	Return to zero – As vector sequencing progresses, data driven to the DUT remains at logic “0” until a logic “1” is encountered in the vector set. The tester then drives logic “1” to the DUT using the timing specified for Leading Edge and Trailing Edge.
R1	Return to One – The opposite of RZ.
RI	Return to inhibit – Tester driver remains at a tri-state level unless a logic “1” or logic “0” appears in the vector set, in which case the correct logic level is driven to the DUT for the duration specified by the timing generators. The driver then returns to the tri-state until the next occurrence of a “1” or “0” [52].
RC	Return to Compliment – More accurately, Surround by Compliment. ”RC” is retained as the name because it complies well with the understanding of this format.

Table 5.1: Stimulus Formats Supported by ETS Software (adapted from [1])

control over both the Leading and Trailing edges of stimulus is required. Dynamic format such as RZ or R1 are used for clocks, resets, and enables. This provides control over Trailing edges for tests like Pulse Width [53]. Finally, NRZ is used for data and address inputs [2].

The effects of selecting different waveforms are illustrated in Figure 5.5. The vector number (addresses) appears below the box. The ”Data” is the vector data at each address for the pin being illustrated. In the example, the Leading edge delay is set to 10 ns, while the Trailing edge delay is set to 50 ns. The Trailing edge delay is disregarded in the NRZ stimulus format.

Figure 5.5: Stimulus formats (adapted from [1]).

Part of the pin setup effort requires defining correct timing and logic levels for the pins in each group. The Input pins require setting Leading, Trailing, and Inhibit, while the Outputs only require setting Compare Strobe. A timing generator is selected for each Delay. The same timing generator is used in more than one group. Any change in the timing will affect other groups using the same timing generator [2].

Besides timing, logic levels are also defined for the pins in each group. For the Inputs, the Low Logic and High Logic values are set, while for the Outputs only the Threshold value is set. Signals above the Threshold are seen as logic “1”, and the signals below Threshold are seen as logic “0”. For bidirectional pins (I/O), all three voltage levels are set.

5.1.7 Downloading Test Vectors

The ASCII test vectors are converted into a downloadable binary file for future testing [54]. When needed, test vectors are loaded from the vector file from disk into the tester’s vector memory [2].

5.1.8 DUT Power Setup

As part of the power setup, the desired values for the memory chip's power supply voltage and current limits are set. The possible power supplies installed are [2]:

- *Supply #1* – Always 0 to +6 V @ 2 A max. (internal)
- *Supply #2* – Always 0 to ± 16 V @ 1 A max. (internal)
- *Supply #3* – Always 0 to ± 16 V @ 1 A max. (internal)
- *Supply #4* – May be: 0 to 7 V @ 5.5 A, 0 to 15 V @ 3.3 A, 0 to 21 V @ 2.5 A, or 0 to 40 V @ 1.4 A (external)

Moreover, the power-up and power-down sequences are set for the power supplies. Also, the delay between power ON and the execution of the first test vector is adjusted.

5.1.9 Run Setup

With DUT board wired, pins defined and grouped, power set up, and test vectors loaded, next, the remaining parameters for controlling the test run are established. The Run Setup parameters are described in Table 5.2.

5.1.10 DUT Continuity Test

As part of the final last steps before running a test, the DUT board is installed and mounted, and a Continuity check is run to verify that all pins of the memory chip are connected. The DUT Continuity test is a DC test that ensures that all of the pins are making good contact with the tester pins and that none of the pins are shorted together, or to power or ground [2]. The Continuity measurement operates on the principle that each of the memory chip's pins include an internal protection diode. By forcing a voltage onto each pin, the expected diode action can be monitored, and it can be determined whether or not the pin is open, shorted or connected [2, 56, 57].

Parameter	Description
Test Rate	Test clock rate in MHz [55].
Last Vector	The last valid vector number, usually the total number of vectors downloaded minus one (the first vector is vector zero). When the test is running but no stop occurs, vector sequencing executes one vector per clock until the Last Vector is reached, at which time the vector sequencing jumps to vector zero and begins again until stopped.
Stop on	The vector number for the stop. It can be any vector between vector 3 and Last Vector. If Failures, ETS software will repeatedly execute the vectors until a failure occurs. If Vector or Failure, test runs to the Last Vector unless a failure occurs, in which case it stops at the first failure. If External, the test run will not stop until a TTL transition appears at the TRIGGER IN BNC connector on the ETS software. If None, the vectors are executed endlessly until halted.
Clock Source	A clock source can be either internal or external.
Sequencing	Sequential executes one vector per clock, starting with vector zero. Programmed can be selected if a pattern generator is used to perform loops and jumps. Memory Test should only be selected when using the Memory Test feature.
Scan Test	Scan test mode can be disabled or enabled. Must be in Sequential mode to use Scan.
Stop Mode	Tells the ETS software what to do when stopped. Halt means that vector sequencing stops, all pins are disconnected from the DUT and DUT power is off. It is safe to remove the DUT when Halted. Pause means that vector sequencing stops, but the current vector is held statically at the DUT pins and DUT power is on. It is not safe to remove the DUT when Paused!

Table 5.2: Run Setup Parameters (adapted from [2])

Analysis: C:\visual\nt\ets\74F161.TRN							Last Trace Sequence		Comments
Vector Address (Dec)	TQQQQ	PPPP	C	L	P	CC	EE	M	
	C3210	3210	K	E	PT	R			90 (Dec)
72	01000	0000	1	1	11	1	-	18	Count full. Start over.
73	01001	0000	1	1	11	1	-	17	
74	01010	0000	1	1	11	1	-	16	
75	01011	0000	1	1	11	1	-	15	
76	01100	0000	1	1	11	1	-	14	
77	01101	0000	1	1	11	1	-	13	
78	01110	0000	1	1	11	1	-	12	
79	11111	0000	1	1	11	1	-	11	
80	00000	0000	1	1	11	1	-	10	
81	00001	0000	1	1	11	1	-	9	
82	00010	0000	1	1	11	1	-	8	End.
83	00011	0000	1	1	11	1	-	7	
84	00100	0000	1	1	11	1	-	6	
85	00101	0000	1	1	11	1	-	5	
86	00110	0000	1	1	11	1	-	4	
87	00111	0000	1	1	11	1	-	3	
88	01000	0000	1	1	11	1	-	2	
89	01001	0000	1	1	11	1	-	1	
90	11010	0000	1	1	11	1	-	0	

Figure 5.6: Analysis window (adapted from [2]).

5.1.11 Functional Test Run and Analysis

Once DUT board is properly wired and mounted, the memory chip (DRAM or SRAM) is placed in the socket, power assigned, and the Run parameters set, the last step is to execute a run of the test vectors by simply clicking the RUN button in the ETS software. Upon completion, the results are shown in the Analysis window. The data captured from the memory chip is displayed along with the input states for each vector.

Figure 5.6 shows an example of the Analysis window. ETS software makes use of colors to determine pass and fail; the Output data shown is the actual data captured, and not necessarily the data expected. If a character is green, this means that it is exactly what was expected as the memory Output. In other words, the data captured from the memory Output pins matched the expected output data in the

Figure 5.7: Analysis Graph mode (adapted from [2]).

Vectors window. If the character is red, it means that the memory Output was not what was expected to be. In either case, Analysis displays the data that was present on the memory Outputs at the time specified as Compare in Pin Setup [2].

Sequence numbers keep a running count of the elapsed test rate clock cycles before the stop point. The stop point is always sequence 0, whether you stop on a vector or a failure. In the Sequential mode, total vectors match the total sequences, but in Programmed mode, there may be many more sequences than vectors [2].

The analysis results of a functional test run can be also be viewed in a graph form just as the vectors can. The Analysis graph mode is shown in Figure 5.7. Colors are used in the graph mode to indicate pass and fail in the same way as it is used in the static data mode (Analysis window). This tool is useful in looking at timing relationships as they pertain to failures. Passing outputs are green while failing pins are shown in red [2].

5.1.12 Calibration and Diagnostics

The accuracy and therefore the value of the tests can only be as good as the system used for testing [2]. ETS software has the tools and the power to ensure the integrity of the test system. The powerful diagnostic routines provided by the ETS software allows repetitive testing of the test system under the constraints of system calibration.

The Automatic Calibration of the test system also allows the ETS Diagnostics to test system performance at much tighter tolerances than would otherwise be possible, further ensuring the accuracy of the test system and the tests. For PUF experiments, the ETS test system is calibrated before each round of measurements and when Diagnostics fails.

A. Diagnostics

Diagnostic tools are built into ETS software and help with thoroughly verifying the operability of the hardware. Each of the tests checks the hardware on at least one board in the system [2]. Table 5.3 describes the diagnostic tests. Diagnostics initializes the tester. For the PUF experiments, Diagnostics is run regularly as a maintenance regimen.

Full Diagnostics is run in certain scenarios:

- When there is a hardware problem
- After replacing a component to fix the problem
- When software is upgraded
- Before running Full Calibration or NIST Calibration
- As a preventative measure regularly

Test	Description
System Interface	Tests the communication between the tester and the computer.
Vector Memory	Checks all RAM behind each pin of the tester.
Pattern Generator	Verifies proper sequencing of the vector address control, whether sequential or non-sequential.
Acquisition Memory	Tests the RAM used for capture seen in Analysis.
Format Control	Refers to the ability to generate stimulus in all formats.
Clock Generator	Checks the accuracy and stability of internal clocks.
Timing Generator	Verifies proper timing is possible with each delay.
PMU	Applies to DC parametrics only.
Power Supplies	Tests DUT power supplies for programmability.
Pin Interface	Checks the relay matrix used by the pin electronics.
Programmable Loads	Programmable loads, relays and circuits.

Table 5.3: Diagnostic Descriptions (adapted from [2])

B. Calibration

There are three different types of calibrations available in ETS software: Automatic Calibration, NIST (National Institute of Standards and Technology) Calibration, and Focused Calibration. The Automatic Calibration (or Full Calibration) is a hands-off routine that uses system constants for time and voltage to ensure that all system components comply with specifications and are traceable to the standards issued by NIST.

Before running calibration, memory chip needs to be removed and at least 15 minutes of warm-up needs to be allowed [2]. Calibration acts as a “Super Diagnostic” because it can find problems with compliance that Diagnostics cannot [58].

Full calibration is run in certain scenarios:

- When any board is replaced
- When software is upgraded
- Before running NIST Calibration as well as afterward
- As a preventative measure, typically every month

The NIST Calibration sets the internal reference sources for voltage and timing to meet NIST compliance. This is done using external instruments that have been calibrated to NIST standards [58].

NIST calibration is run in certain scenarios:

- Every six months
- When a system basic board is replaced
- When the backplane or a system power supply is replaced

The NIST Calibration procedure requires that both Diagnostics and Full Calibration pass before performing NIST Calibration. Full Calibration should be run again after completing the NIST Calibration [58].

Maximum performance can be achieved by using the Focused Calibration. This function is very similar to the Full Calibration, but it calibrates only the pins and timing generators. It also calibrates at only the logic levels defined. This calibration is very quick and can be run before each test to ensure the highest possible accuracy [2]. It is important to note that all Diagnostics must pass before running the calibration or the calibration can be expected to fail [58].

5.2 Precision Temperature Forcing System

For temperature testing, the T2420 Precision Temperature Forcing System (PTFS) from *Thermonics* is used to heat or cool the memory chips (SRAMs and DRAMs)

Figure 5.8: Output air nozzle of a T2420 precision temperature forcing system (adapted from [6]).

in their test socket with temperature-controlled air, while PUF signatures are being read from the chips using the *HiLevel* ETS test system.

Figure 5.8 shows the output air nozzle of a T2420 PTFS. PTFS uses directed temperature-controlled forced air to provide a controlled environment for temperature testing of devices. This enables the tester to perform tests at specific locations of the component: on a test socket, PCB or small assembly.

The T2420 PTFS has a temperature range of -90°C to 225°C and can transition air temperatures between $+125^{\circ}\text{C}$ and -55°C in as little as four seconds. Temperature resolution is 0.1°C and accuracy is $\pm 1.0^{\circ}\text{C}$.

The method of heating is forced air with inline air heaters, while the method of cooling is forced air with single-stage mechanical refrigeration and multi-stage self-cooling heat exchanger. The T2420 PTFS provides a high airflow rate of 200 to 960 SCFH (standard cubic feet per hour) or 1.6 to 7.6 liters per second [6].

5.2.1 Precision Temperature Control

An advanced temperature control algorithm provides the T2420 PTFS with the most rapid and precise temperature control system. Physical integration to the DUT is accomplished with the interface kit, which includes thermal caps and a shroud assembly. Coupled with the system's high airflow and cold boost feature, test temperatures are achieved very efficiently [6].

5.2.2 DUT Sensor

For the PUF experiments, the case temperature of the memory chip is controlled with the use of the DUT sensor. This feature allows controlling the temperature of the memory chip to within $\pm 1.0^{\circ}\text{C}$ of the desired temperature set-point. Also, the advanced temperature control algorithm assures the memory chip is quickly stabilized at the set temperature [6].

5.2.3 Integrated Thermal Test Head and Motorized Arm

The PTFS provides a strong support arm for adapting the thermal test head to the memory chip under test. The positive action quick-adjust arm has several degrees of freedom that enables it to be positioned in a wide range of horizontal and vertical positions. The combination of electro-mechanical and pneumatic action of this assembly ensures precise, stable and repeatable placement of the thermal shroud over the memory chip. Heated purge air is provided to keep the test interface free of frost or moisture when operating at cold temperatures [6].

Chapter 6

Experimental Results on DRAM

This chapter presents the experimental results on real DRAM chips. For DRAM, two sets of experiments were performed using two different approaches to extract the PUF signatures. The first set of experiments was based on extracting the signatures using the PowerUp approach, whereas the second set was based on extracting the signatures using the proposed methodology (the WRITE approach). Both sets of experiments include identifying the stable cells across the chips, extracting the signatures, and finally analyzing the signatures' randomness, uniqueness, and robustness under temperature and voltage variations.

6.1 DRAM Technology Overview

For DRAM experiments, the NEC μ PD416-3 DRAM chips are used. The μ PD416-3 is a 16,384 words by 1 bit Dynamic MOS RAM. It is designed for memory applications where very low cost and large bit storage are important design objectives [45]. The μ PD416-3 is fabricated using a double-poly-layer N -channel silicon gate process which affords high storage cell density and high performance. The use of dynamic circuitry throughout, including the sense amplifiers, assures minimal power dissipation [45].

Figure 6.1: Block diagram for DRAM (μ PD416-3).

Multiplexed address inputs permit the μ PD416-3 to be packaged in the standard 16-pin dual-in-line package. The 16-pin package provides the highest system bit densities. Noncritical clock timing requirements allow the use of the multiplexing technique while maintaining high performance [45].

Figure 6.1 shows the block diagram for the 16K μ PD416-3 chip used in the DRAM PUF experiments. The 14 address bits required to decode 1 of 16,384 bit locations are multiplexed onto the 7 address pins and then latched on to the chip with the use of the Row Address Strobe ($\overline{RAS}$), and the Column Address Strobe ($\overline{CAS}$). The 7-bit row address is first applied, and $\overline{RAS}$ is then brought low. After the $\overline{RAS}$ hold time has elapsed, the 7-bit column address is applied, and $\overline{CAS}$ is brought low. This multiplexing operation imposes no penalty on access time [45].

For a write operation, the input data is latched on the chip by the negative-going

edge of $\overline{WRITE}$ or $\overline{CAS}$ whichever occurs later. For a read or write cycle, the data output will contain the data in the selected cell after the access time. Data out will assume the high impedance state anytime that $\overline{CAS}$ goes high [45].

Refresh of the memory array is accomplished by performing a memory cycle at each of the 128-row addresses every 2 milliseconds or less. Because data out is not latched, $\overline{RAS}$ -only cycles can be used for simple refreshing operation [45]. To assure long term reliability, VBB should be applied first during power-up and removed last during power down.

6.2 The PowerUp Approach

In the first set of experiments, the PowerUp approach is used to extract the PUF signatures. The following sections describe:

- Identifying the stable cells in DRAM
- Extracting the PUF signatures by reading out the stable cells upon PowerUp
- Analyzing the signatures' uniqueness as well as robustness under voltage and temperature variation

6.2.1 Stable Cells

One of the key characteristics of PUF is reproducibility. PUF needs to generate the same signature on every PowerUp-read attempt. To assure PUF's reproducibility, experiments are conducted to identify the highly stable cells during power-up. The PowerUp-read attempts are repeated ten times per chip. A 10-min wait time is considered between the attempts. This is to ensure the chip under test cools down to room temperature and the read attempts are performed under the same starting conditions. The results are then compared to identify the stable cells for each chip.

Figure 6.2: Snapshot of the bit-pattern of a DRAM chip (10 words by 1 bit) after ten PowerUp-read attempts.

The cells with a reproducibility rate of 80% or more are considered stable, while the rest are considered unstable and are excluded from PUF.

Figure 6.2 shows the snapshot of the bit-pattern of a DRAM chip for ten PowerUp-read attempts. The white cells represent the cells storing ‘0’s and the black cells represent the cells storing ‘1’s. The bit-pattern on the right highlights the cells with a reproducibility rate of less than 80%. These unstable cells are shown in red and are excluded from PUF.

Figure 6.3 shows the bit-patterns for a larger snapshot of the ten DRAM chips after ten PowerUp-read attempts. Like figure 6.2, unstable cells are shown in red, while the cells storing stable ‘1’s and ‘0’s are shown in black and white accordingly.

Table 6.1 shows the percentage of unstable cells in the signatures obtained from the ten DRAM chips using the PowerUp approach. As the data shows, except for one chip with 12.26% unstable cells, the remaining of the chips can produce highly stable bit-patterns (signatures) with 8 out of 9 chips with 1% or less unstable cells.

For signature comparison, same length signatures are obtained from all ten DRAM chips. This is achieved by setting the highest percentage of unstable cells as the elimination target. For all chips, not only the unstable cells are eliminated. But additionally, randomly selected stable cells are also eliminated until the elimination

Figure 6.3: Snapshot of the bit-patterns of ten DRAM chips (30 words by 1 bit) after ten PowerUp-read attempts. These snapshots do not represent the full signatures.

Chip	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Unstable Cells (%)	0.61	0.91	1.01	0.73	0.87	12.26	0.14	2.01	0.18	0.38

Table 6.1: Percentage of Unstable Cells in the Signatures Obtained from Ten DRAM Chips Using the PowerUp Approach

target is met. For the PowerUp approach, the highest percentage of unstable cells is 12.26%, which leaves 14,375 stable cells for PUF signatures.

Figure 6.4: Fractional Hamming weight values for the signatures obtained from ten DRAM chips using the PowerUp approach (X axis represents DRAM cell values and Y axis represents the fractional Hamming weight).

6.2.2 Randomness

To measure the randomness (unpredictability) of signatures, the min-entropy is estimated. This value is found to be 0.047 which is far from the ideal value of 1.0. This indicates that the DRAM signatures extracted using the PowerUp approach are predictable and therefore highly vulnerable to ML attacks.

Besides randomness, fractional Hamming weight is also measured to identify the bias point of signatures. This measure indicates whether or not the cells in each chip are biased toward a certain logic value. Ideally, the signatures should have a fractional Hamming weight of 50%. This indicates that the cells have an equal probability of storing ‘0’ or ‘1’ upon power-up.

Figure 6.4 shows the fractional Hamming weight for the signatures obtained from

Chip	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Fractional Hamming Weight	0.54	0.49	0.47	0.5	0.02	0.2	0.49	0.45	0.46	0.49
Average	0.41									

Table 6.2: Fractional Hamming Weight Values for Signatures Obtained from Ten DRAM Chips Using the PowerUp Approach

the ten DRAM chips using the PowerUp approach. The average fractional hamming weight is shown in Red. As the data shows, except for two chips with an average weight of 0.2 and 0.02, the remaining of the chips have an average weight of around 0.5 which indicates that for majority of DRAM chips the cells have an equal tendency toward ‘0’ or ‘1’ upon power-up.

Table 6.2 summarizes the fractional Hamming weight values per chip. The average fractional Hamming weight across all ten DRAM chips is found to be 0.41 which is not very far from the ideal value of 0.5.

6.2.3 Uniqueness

To measure the uniqueness of signatures, the inter-die Hamming distance is computed by calculating the fractional Hamming distance between the signatures obtained from the ten DRAM chips using the PowerUp approach, considering all pairwise comparisons.

As Figure 6.5 shows, the average inter-die Hamming distance is found to be approximately 17% which is far from the ideal value of 50%. This indicates that the signatures obtained from DRAMs using the PowerUp approach are highly correlated and might not be suitable for authentication purposes. The Inter die Hamming distance values for all 45 pairwise signature comparisons are shown in Table 6.3.

Figure 6.5: Inter–die Hamming distance distribution of signatures obtained from ten DRAM chips using the PowerUp approach.

Signature Comparison	1,2	1,3	1,4	1,5	1,6	1,7	1,8	1,9	1,10	2,3
Inter-die HD (%)	5.99	7.43	4.16	52.08	35.66	5.84	11.31	8.06	5.42	2.92
Signature Comparison	2,4	2,5	2,6	2,7	2,8	2,9	2,10	3,4	3,5	3,6
Inter-die HD (%)	1.7	49.07	30.33	1.85	6.91	3.76	1.62	3.55	47.13	28.59
Signature Comparison	3,7	3,8	3,9	3,10	4,5	4,6	4,7	4,8	4,9	4,10
Inter-die HD (%)	2.41	6.76	3.83	2.19	50.02	31.29	1.61	7.81	4.4	1.79
Signature Comparison	5,6	5,7	5,8	5,9	5,10	6,7	6,8	6,9	6,10	7,8
Inter-die HD (%)	19.15	49.26	43.39	46.57	49.49	30.37	24.95	31.69	30.88	6.77
Signature Comparison	7,9	7,10	8,9	8,10	9,10					
Inter-die HD (%)	3.79	1.94	7.02	6.59	3.09					

Table 6.3: Inter–die Hamming distance Values for Pairwise Comparison of Signatures Obtained from ten DRAM Chips Using the PowerUp Approach

Figure 6.6: Percentage of fractional Hamming distance variation of signatures obtained from ten DRAM chips under temperature variation using the PowerUp approach.

6.2.4 Robustness

A. Robustness under Temperature Variation

To estimate the robustness of signatures under temperature variation, the average intra-die Hamming distance among the signatures is estimated by obtaining the signature for each chip at four different temperatures under nominal supply voltage and comparing it with that obtained at room temperature. Baseline measurements are performed with the temperature set to 25°C and supply voltage set to $VCC = 5$ V, $VDD = 12$ V, $VBB = -5$ V. Next, measurements are performed with the temperature varied from -25°C to 75°C in 25°C increments using the *Thermonics* T-2420.

Temperature plays a significant role in memory decay by affecting power leakage at the transistor level. Figure 6.6 demonstrates the significant impact temperature variation can have on bit stability. The highest level of instability across all chips occurs at -25°C and is approximately 34%. As temperature decreases, V_{th} increases which affect the rate of charge decay and causes bit-flip from ‘1’ to ‘0’.

Table 6.4 shows the intra-die Hamming distance values of signatures obtained

Temperature	-25°C	0°C	50°C	75°C	Intra-die HD_{avg}
Chip1	10.39	5.75	3.99	7.06	6.80
Chip2	49.33	6.06	0.28	6.08	15.44
Chip3	8.38	3.15	1.92	2.44	3.97
Chip4	50.55	20.32	1.52	7.94	20.08
Chip5	49.08	18.61	10.36	38.24	29.07
Chip6	30.18	17.79	13.88	29.45	22.82
Chip7	47.39	5.11	3.75	20.02	19.07
Chip8	43.34	6.09	2.27	3.89	13.90
Chip9	46.65	3.12	2.03	2.43	13.56
Chip10	5.87	3.76	1.09	2.12	3.21
					Total = 14.79%

Table 6.4: Intra-die Hamming distance Values of Signatures Obtained from ten DRAM Chips Under Temperature Variation Using the PowerUp Approach

Figure 6.7: Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from ten DRAM chips under temperature variation using the PowerUp approach.

from ten DRAM chips under temperature variation using the PowerUp approach. The average robustness of signatures is found to be approximately 15%.

Figure 6.7 shows the distribution of average intra-die Hamming distance values of signatures obtained from ten DRAM chips under temperature variation. As it is shown, in 60% of cases there is less than 10% bit-flips in the signatures under varying

temperatures.

B. Robustness under Voltage Variation

To estimate the robustness of signatures under supply voltage variation, the average intra-die Hamming distance among the signatures is estimated by obtaining the signature for each DRAM chip under varied voltage levels and comparing it with that obtained at nominal voltage levels. Baseline measurements are performed with voltage levels set to $VCC = 5$ V, $VDD = 12$ V, $VBB = -5$ V and temperature set to 25°C. Next measurements are performed with voltage levels varied by 10% up and 10% down using the *HILEVEL* Griffin tester.

Figure 6.8 shows the impact of supply voltage variation on bit stability. Like temperature, supply voltage variations can also have an impact on the bit stability. The reason underlies the physical structure of a DRAM cell, which consists of one capacitor and one transistor. The PowerUp value of a DRAM cell is dependent on the bias voltage of the capacitor, and very slight variations in the supply voltage can alter the voltage differential across the capacitor.

As Figure 6.8 shows, lower supply voltages affect the bit stability more than higher supply voltages. The average cell instability at -10% supply voltage variation is found to be approximately 18%.

Table 6.5 shows the intra-die Hamming distance values of signatures obtained from ten DRAM chips under supply voltage variation using the PowerUp approach. The average bit-flips in signatures is found to be approximately 11%.

Figure 6.9 shows the distribution of average intra-die Hamming distance of the signatures obtained from ten DRAM chips under supply voltage variation. As it is shown, in 75% of cases, there are fewer than 6% bit-flips under supply voltage variation.

Figure 6.8: Percentage of fractional Hamming distance variation of signatures obtained from ten DRAM chips under supply voltage variation using the PowerUp approach.

Supply Voltage Variation	-10%	+10%	Intra-die HD_{avg}
Chip1	3.7	0.45	2.07
Chip2	2.81	0.94	1.87
Chip3	2.47	1.11	1.79
Chip4	1.19	0.34	0.76
Chip5	16.04	5.41	10.72
Chip6	54.29	18.53	36.41
Chip7	49.37	1.66	25.51
Chip8	2.63	1.04	1.83
Chip9	3.98	0.12	2.05
Chip10	46.15	5.87	26.01
			Total = 10.90%

Table 6.5: Intra-die Hamming Distance Values of Signatures Obtained from ten DRAM Chips Under Supply Voltage Variation Using the PowerUp Approach

6.3 The WRITE Approach

For the second set of experiments, the tester is programmed such that the cell values are read right after a Write-1 is performed. The read takes place in the same clock cycle as the Write-1 and before the Refresh signal is activated. A Write-0 (initializa-

Figure 6.9: Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from ten DRAM chips under supply voltage variation using the PowerUp approach.

tion phase) is performed before the Write-1 (randomization phase) to set all DRAM cells to a base state.

The timing diagram for a Write cycle in the μ PD416-3 DRAM is shown in Figure 6.10. The minimum write pulse is 45 ns, and the Refresh period is 2 ms. For a Write operation, the DIN is latched on the chip by the negative-going edge of $\overline{WRITE}$ or $\overline{CAS}$, whichever occurs later. If $\overline{WRITE}$ is active before $\overline{CAS}$, this is an early-write cycle and $DOUT$ will remain in the high impedance state throughout the cycle. In this case, the effective write pulse is measured from the negative-going edge of $\overline{CAS}$ to the positive-going edge of $\overline{WRITE}$ as shown in Figure 6.11.

To extract PUF signatures, DRAM cells are initialized with ‘0’s using a wide effective write pulse that satisfies the minimum timings. Next, random failures are induced by writing ‘1’s using a shorter effective write pulse that violates the minimum timings. The timing diagram for the initialization and randomization phases is shown in Figure 6.11.

To shorten the effective write pulse, the negative-going edge of $\overline{CAS}$ is shifted to right so that DIN is latched later into the cycle. Under the shortened write duty

Figure 6.10: Timing diagram for an early-write cycle for a DRAM ($\mu\text{PD416-3}$) chip.

Figure 6.11: Timing diagram for the initialization and randomization phases using the WRITE approach for extracting PUF signatures from a DRAM ($\mu\text{PD416-3}$) chip.

cycle, some cells fail the Write-1 operation, while some others succeed resulting in a bit-pattern with random '0's and '1's across the DRAM.

The following sections describe:

- Finding the appropriate effective write pulse (duty cycle) for randomization
- Extracting PUF signatures by inducing write failures using the selected write pulse from the previous step followed by reading out the cell contents
- Excluding the unstable cells from PUF signatures

- Analyzing the signatures’ uniqueness as well as robustness under voltage and temperature variation

6.3.1 Write Duty Cycle

For each DRAM chip, the appropriate write duty cycle is selected to ensure a 50% rate of success to failure in writing ‘1’s. In an early-write, the write duty cycle (effective write pulse) is measured from the negative-going edge of $\overline{CAS}$ to the positive-going edge of $\overline{WRITE}$. The write duty cycle is shortened by moving the negative-going edge of $\overline{CAS}$ to right.

To find the best write duty cycle for each chip, the duty cycle is swept from 45 ns down to 0 ns in 0.1 ns steps. At each step, a Write-1 operation is performed followed by a read to extract the signature. Next, the fractional Hamming weight is calculated for the obtained signature. The fractional Hamming weight measurements are then plotted against the duty cycle range as shown in Figure 6.12.

When the write duty cycle is very short, most write attempts fail. Therefore the fractional Hamming weight is very low. As duty cycle gets wider, more write attempts succeed causing Hamming weight to increase. Finally, for a wide duty cycle, most write attempts succeed, which results in the fractional Hamming weight reaching close to its maximum value of 100%. The abrupt rise of the Hamming weight is mainly due to the small size of storage capacitors in DRAM cells, which cause slight variations in test parameters (in this case duty cycle) causing bit flips from 0 to 1.

For the proposed methodology, the best write duty cycle is where the fractional Hamming weight is 50%. These duty cycles are identified for all ten DRAM chips and are shown in Figure 6.12. The shortened duty cycles are used to perform Write-1 operations and extract the signatures.

Although, theoretically, the ideal write duty cycles have been identified, but in reality the write duty cycles that can be used for extracting PUF signatures are

Figure 6.12: Best write duty cycles for DRAM chips to ensure a 50% rate of success to failure in a Write-1 operation.

limited to the resolution of the *HILEVEL* Griffin tester. Although the resolution of the tester is 0.5 ns, timings are allowed to be set even at the level of 0.1 ns. The final write duty cycle for each chip is adjusted based on allowed timing resolution for the tester and are shown in Table 6.6.

Chip	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Write Duty Cycle (ns)	10.4	10.2	10.8	12.8	10.2	10.8	10.4	12.3	11.6	10.7

Table 6.6: Write Duty Cycles for DRAM Chips

6.3.2 Stable Cells

The physical variations between cells across the DRAM array cause cells to write ‘1’s at different write duty cycles due to different transistor switching times. Figure 6.13 shows the bit-patterns of a randomly selected group of DRAM cells in ten chips when Write-1 is performed at write duty cycles ranging from 0 to 45 ns (the minimum write pulse for μ PD416-3). The ‘X’ axis represents the 250 DRAM cells, and the ‘Y’ axis represents varying write duty cycles (only shown for the 9 – 14 ns range).

For short write duty cycles, all cells fail to write ‘1’, whereas for wide write duty cycles, all cells succeed. For write duty cycles in between, some cells may fail the Write-1 operation, whereas other cells may succeed. As the width of the write duty cycle increases, more cells succeed in writing ‘1’s. However, some cells may enter an instability zone where cell values flicker between ‘0’s and ‘1’s.

To ensure robustness, unstable cells in a write operation are identified and excluded from PUF. The bar charts on the right side of Figure 6.13 show the unstable cells for different write duty cycles for all ten DRAM chips. As it is shown, unstable cells are mostly distributed around the selected write duty cycles marked with blue arrows. This is where the cells are at their most unstable state as they transition from ‘0’ to ‘1’.

With DRAM cells initialized to ‘0’s using a wide write duty cycle, and a Write-1 operation performed using a controlled write duty cycle, a random pattern of ‘0’s and ‘1’s is produced by each chip. The fractional Hamming weight of each bit-pattern (signature) is 50% which indicates a perfect bias point for each chip.

Figure 6.13: Bit-pattern of a randomly selected group of 250 cells in ten DRAM chips when a Write-1 operation is performed at different write duty cycles ranging from 9 to 14 ns. The distribution of unstable cells across the same duty cycle range is shown on right (X axis represents DRAM cell value and Y axis represents the duty cycle in ns. For the bar charts on right, X axis represents the number of unstable cells and Y axis represents the duty cycle in nanoseconds).

For PUF to be reproducible, same PUF signature needs to be reproduced every time. To ensure PUF's reproducibility, the stable cells are identified for each chip by reading the content of the chip after a Write-1 operation. The Write-1-read attempt is repeated ten times with a 10-min wait time considered between the attempts.

Figure 6.14 shows a snapshot of the bit-pattern of a DRAM chip after ten Write-

Figure 6.14: Snapshot of the bit-pattern of a DRAM chip (10 words by 1 bit) after ten Write-1-Read attempts.

Chip	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Unstable Cells (%)	18.01	13.32	13.87	28.07	19.55	15.48	14.23	8.11	10.29	32.35

Table 6.7: Percentage of Unstable Cells in Signatures Obtained from ten DRAM Chips Using the WRITE Approach

1-read attempts. The white cells represent the cells storing ‘0’s and the black cells represent the cells storing ‘1’s. A cell is considered unstable if its probability of storing the same logic value (‘0’ or ‘1’) over ten attempts is below 80%. The unstable cells are highlighted in red and excluded from PUF. Figure 6.15 shows a larger snapshot of the bit-patterns obtained from the ten DRAM chips after ten write-1-read attempts are performed. As it is shown, the unstable cells are highlighted in red. These cells are excluded from PUF.

Table 6.7 shows the percentage of unstable cells across the DRAM chips. The average percentage of unstable cells is found to be 17.33%. For signature comparison using the Hamming distance metric, same length signatures are obtained from all chips. This is achieved by setting the maximum percentage of unstable cells as the elimination target. For all chips, not only the unstable cells are eliminated. But on top of that, randomly selected stable cells are also eliminated until the elimination

Figure 6.15: Snapshots of the bit-patterns of ten DRAM chips after ten Write-1-Read attempts. These snapshots do not represent the full signatures.

target is reached. For the WRITE approach, the highest percentage of unstable cells is 32.35%, which leaves 11,083 stable cells for PUF signatures.

6.3.3 Randomness

To evaluate the randomness (unpredictability) of signatures, the min-entropy per cell is computed. For the PUF signatures obtained from DRAMs using the WRITE approach, the min-entropy is found to be 0.9215 which is very close to the ideal value of 1.0 indicating a significantly high level of randomness and therefore high resilience against modeling attacks.

Fractional Hamming weight is also computed to find the bias point for every chip. Table 6.8 shows the fractional Hamming weight values for all ten DRAM chips. The

Chip	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Fractional Hamming Weight (%)	50.83	50.37	50.2	49.38	49.66	50.04	50.11	49.48	50.3	49.62
Average (%)	49.99									

Table 6.8: Fractional Hamming Weight for Signatures Obtained from ten DRAM Chips Using the WRITE Approach

average value is found to be 49.99% which is very close to the ideal value of 50% indicating that DRAM cells are not biased toward a certain logic value ('0' or '1').

6.3.4 Uniqueness

The uniqueness of PUF is analyzed by measuring the inter-die Hamming distance of the signatures obtained from the ten DRAM chips considering all pairwise comparisons. This measures the level of dissimilarity of the signatures from chip to chip. The more unique (dissimilar) the signatures, the closer the average inter-die Hamming distance to 50%. Figure 6.16 shows that the average inter-die Hamming distance of DRAM signatures obtained using the WRITE approach is found to be 50.21% which is very close to the ideal value of 50%. The Inter-die Hamming distance values for pairwise comparison of signatures are shown in Table 6.9.

Figure 6.16: Inter-die Hamming distance distribution of signatures obtained from ten DRAM chips using the WRITE approach.

Signature Comparison	1,2	1,3	1,4	1,5	1,6	1,7	1,8	1,9	1,10	2,3
Inter-die HD (%)	40.12	51.87	53.66	46.21	49.33	49.17	56.45	48.67	45.11	58.98
Signature Comparison	2,4	2,5	2,6	2,7	2,8	2,9	2,10	3,4	3,5	3,6
Inter-die HD (%)	50.34	53.76	55.14	56.91	47.11	47.36	44.22	48.19	51.01	49.68
Signature Comparison	3,7	3,8	3,9	3,10	4,5	4,6	4,7	4,8	4,9	4,10
Inter-die HD (%)	50.03	48.67	51.34	51.98	50.02	47.69	43.17	49.35	52.29	48.19
Signature Comparison	5,6	5,7	5,8	5,9	5,10	6,7	6,8	6,9	6,10	7,8
Inter-die HD (%)	49.56	48.75	52.99	50.52	53.1	51.83	49.37	51.22	43.1	50.91
Signature Comparison	7,9	7,10	8,9	8,10	9,10					
Inter-die HD (%)	53.9	51.71	60.61	44.25	51.81					

Table 6.9: Inter-die Hamming Distance Values for Pairwise Comparison of Signatures Obtained from ten DRAM Chips Using the WRITE Approach

Temperature	-25°C	0°C	50°C	75°C	Intra-die HD_{avg}
Chip1	12.11	7.65	3.15	8.77	7.92
Chip2	45.09	11.21	4.65	5.98	16.73
Chip3	10.73	5.22	3.19	3.51	5.66
Chip4	43.28	27.76	5.34	1.025	21.65
Chip5	52.13	21.89	10.18	30.73	28.73
Chip6	44.9	31.55	15.44	19.93	27.95
Chip7	43.11	10.04	4.32	15.43	18.28
Chip8	36.35	13.54	6.64	6.3	15.70
Chip9	46.71	14.95	4.11	17.61	20.84
Chip10	30.65	17.85	6.43	6.27	15.3
					Total = 17.88%

Table 6.10: Inter-die Hamming distance Values of Signatures Obtained from ten DRAM Chips Under Temperature Variation Using the WRITE Approach

6.3.5 Robustness

A. Robustness under Temperature Variation

PUF needs to be robust under temperature variation. To measure the robustness of signatures, the average intra-die Hamming distance among the signatures is estimated. Baseline measurements are performed with the temperature set to 25°C and supply voltage set to $VCC = 5$ V, $VDD = 12$ V, $VBB = -5$ V. Next, measurements are performed with the temperature varied from -25°C to 75°C in 25°C increments using the *Thermonics* T-2420.

Figure 6.17 shows the percentage of Fractional Hamming distance variation of signatures under varying temperatures using the WRITE approach. The inter-die Hamming distance values are also shown in Table 6.10.

The average of highest signature variation is 36.52% which occurs at -25°C where V_{th} is at its highest value. As the temperature decreases, V_{th} increases. As a result, the selected write duty cycle is not long enough to fully charge the storage capacitor, resulting in a bit-flip from ‘1’ to ‘0’. The average bit-flips of PUF signatures under temperature variation is found to be approximately 18%.

Figure 6.17: Percentage of fractional Hamming distance variation of signatures obtained from ten DRAM chips under temperature variation using the WRITE approach.

Figure 6.18: Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from ten DRAM chips under temperature variation using the WRITE approach.

Figure 6.18 shows the distribution of average intra-die Hamming distance of the signatures obtained from ten chips under temperature variation. As it is shown, 70% of chips have fewer than 20% bit-flips in their signatures under varying temperatures.

B. Robustness under Voltage Variation

PUF needs to be robust under supply voltage variation. To measure the robustness of signatures, the average intra-die Hamming distance among the signatures is estimated. Baseline measurements are performed with supply voltages set to $VCC = 5$ V, $VDD = 12$ V, $VBB = -5$ V and temperature set to 25°C. Next measurements are performed with supply voltages varied by 10% up and 10% down using the *HILEVEL* Griffin tester at 25°C.

Figure 6.19 shows the impact of supply voltage variation on bit stability. Like temperature, supply voltage variations can also have an impact on the bit stability. The reason underlies the physical structure of a DRAM cell, which consists of one capacitor and one transistor. The value of a DRAM cell is dependent on the bias voltage of the capacitor, and very slight variations in the supply voltage can alter the voltage differential across the capacitor. As Figure 6.19 shows, lower supply voltages affect the bit stability more than higher supply voltages and this is true for all ten DRAM chips. This is mainly due to lower circuit performance at lower voltages. The average instability at -10% supply voltage variation is found to be approximately 27%.

The intra-die Hamming distance values of signatures obtained under supply voltage variation are shown in Table 6.11. The average bit-flips in signatures under supply voltage variation is found to be approximately 18%.

Figure 6.20 shows the distribution of average intra-die Hamming distance of the signatures obtained from ten DRAM chips under supply voltage variation. As it is shown, 70% of cases have fewer than 20% bit-flips under supply voltage variation.

Figure 6.19: Percentage of fractional Hamming distance variation of signatures obtained from ten DRAM chips under supply voltage variation using the WRITE approach.

Supply Voltage Variation	-10%	+10%	Intra-die HD_{avg}
Chip1	10.3	3.98	7.14
Chip2	11.23	3.65	7.44
Chip3	17.18	6.04	11.61
Chip4	14.22	6.87	10.54
Chip5	21.61	7.15	14.38
Chip6	56.67	25.23	40.95
Chip7	48.78	10.25	29.51
Chip8	19.44	7.84	13.64
Chip9	25.34	8.74	17.04
Chip10	50.02	13.93	31.97
			Total = 18.42%

Table 6.11: Inter-die Hamming distance Values of Signatures Obtained from ten DRAM Chips Under Supply Voltage Variation Using the WRITE Approach

6.4 Summary

Table 6.12 summarizes the DRAM experimental results presented in this chapter. A comprehensive evaluation of DRAM PUF was presented in terms of uniqueness, randomness, and robustness under varying environmental conditions. For both method-

Figure 6.20: Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from ten DRAM chips under supply voltage variation using the WRITE approach.

ologies, it takes only a few nanoseconds to generate the signatures.

Using the Hamming distance metric, the uniqueness of signatures obtained from DRAMs using both the PowerUp and the WRITE methodologies was evaluated. Results show that in comparison with the PowerUp approach, the proposed methodology produces signatures with significantly higher inter-die Hamming distance values.

Furthermore, the results from the min-entropy estimation show that the proposed methodology provides signatures with excellent randomness which makes this methodology resilient to ML attacks.

Finally, results show that both methodologies provide a good level of robustness under temporal fluctuations with the PowerUp approach showing slightly higher reproducibility under both temperature and voltage variations.

Overall, the signatures obtained through the proposed methodology provide significantly better results in terms of uniqueness and randomness, while providing a good level reproducibility under temporal fluctuations. Moreover, due to no dependency to power-up values, the proposed methodology is less vulnerable to side-channel attacks. All these make the proposed approach more suitable for extracting unique and

DRAM Experimental Results

Methodology	PowerUp	WRITE
Authentication Time	Nanoseconds	Nanoseconds
Percentage of Stable Cells	98.09%	82.67%
Uniqueness	17.34%	50.21%
Min-entropy	0.047	0.92
Bias Point	41.44%	49.99%
Robustness under Temperature Variation	85.21% (-25°C to +75°C)	82.12% (-25°C to +75°C)
Robustness under Voltage Variation	86.86% (Nominal voltage $\pm 10\%$)	81.58% (Nominal voltage $\pm 10\%$)

Table 6.12: Summary of DRAM Experimental Results

robust signatures from DRAM.

Chapter 7

Experimental Results on SRAM

The effectiveness of the proposed methodology is further evaluated by performing experiments on real SRAM chips. This chapter presents the experimental results on SRAM. For SRAM, two sets of experiments are performed using two different approaches to extract the PUF signatures. The first set of experiments is based on extracting the signatures using the PowerUp approach, whereas the second set is based on extracting the signatures using the proposed methodology (the WRITE approach). Both sets of experiments include identifying the stable cells across the chips, extracting the PUF signatures, and finally analyzing the signatures' randomness, uniqueness, and robustness under temperature and voltage variation.

7.1 SRAM Technology Overview

While both SRAM and DRAM are fundamental RAM types, they have some key differences that allows them to best perform for different tasks. Compared to DRAM technology, SRAM has a higher cost per bit and is not as dense, therefore it cannot hold as much data as DRAM can. SRAM is volatile but, unlike DRAM, if the system is powered SRAM retains data values without the need to recharge the cells.

For SRAM experiments, the HT6116-70 SRAM chips are used. Figure 7.1 shows

Figure 7.1: Block diagram for SRAM (HT6116-70).

the block diagram for the 16K HT6116-70 SRAM. The SRAM is organized with 2,048 words of eight bits in length, and operates with a single 5 V power supply. The IC is built with a high-performance CMOS 0.8 μm process, and it contains the standard 6-transistor SRAM cells.

7.2 The PowerUp Approach

In the first set of experiments, the PowerUp approach is used to extract the PUF signatures. The following sections describe:

- Identifying the stable cells in SRAM
- Extracting the PUF signatures by reading out the stable cells upon PowerUp
- Analyzing the signatures' uniqueness as well as robustness under voltage and temperature variation

Figure 7.2: Snapshot of the bit-pattern of an SRAM chip (10 words by 8 bits) after each of ten PowerUp-Read attempts.

7.2.1 Stable Cells

PUF signatures need to be reproducible. The same signature has to be obtained every time the SRAM chip is powered up. To ensure reproducibility, the stable cells are identified by reading out the content of each chip upon power-up. The PowerUp-read attempts are repeated ten times for each chip. A 10-min wait time is considered in between the attempts. This is for the chip to cool down to room temperature (25°C) and to ensure that the starting condition is the same before each attempt is performed.

Figure 7.2 shows the snapshot of the bit-pattern of an SRAM chip after each PowerUp-read attempt. The white cells represent the cells storing ‘0’s and the black cells represent the cells storing ‘1’s. Cells are considered stable if they have a probability of 80% or more of storing the same logic value over the ten PowerUp-read attempts. The remaining of the cells are considered unstable. These cells are highlighted in red and excluded from PUF. Figure 7.3 shows the bit-pattern of a larger snapshot of the eight SRAM chips after ten PowerUp-read attempts with the stable and unstable cells identified.

Table 7.1 shows the percentage of unstable cells in the signatures obtained from eight SRAM chips after ten PowerUp-read attempt. As data shows, at the worst case, the percentage of unstable cells is only less than 1% indicating majority of cells are highly reproducible upon PowerUp and can be included in the PUF signatures.

For signature comparison, same length signatures are obtained from all eight

Figure 7.3: Snapshots of the bit-patterns of eight SRAM chips (30 words by 8 bits) after ten PowerUp-Read attempts. These snapshots do not represent the full signatures.

Chip	#1	#2	#3	#4	#5	#6	#7	#8
Unstable Cells (%)	0.79	0.76	0.73	0.53	0.68	0.91	0.43	0.71

Table 7.1: Percentage of Unstable Cells in Signatures Obtained from eight SRAM Chips Using the PowerUp Approach

SRAM chips. This is achieved by setting the highest percentage of unstable cells as the elimination target. For all chips, not only the unstable cells are eliminated. But additionally, randomly selected stable cells are also eliminated until the elimination target is met. For the PowerUp approach, the highest percentage of unstable cells is 0.91%, which leaves 16,234 stable cells for PUF signatures.

7.2.2 Randomness

To measure the randomness (unpredictability) of signatures, the min-entropy per cell is estimated. Ideally, PUF signatures should have a min-entropy close to one to ensure high resistance against modeling attacks. For the SRAM signatures obtained using the PowerUp approach, the min-entropy per cell is found to be 0.1939 which is far from the ideal value of 1.0.

Figure 7.4: Fractional Hamming weight for signatures obtained from eight SRAM chips using the PowerUp approach (X axis represents SRAM cell values and Y axis represents the fractional Hamming weight).

Chip	#1	#2	#3	#4	#5	#6	#7	#8
Fractional Hamming Weight	0.86	0.80	0.80	0.97	0.85	0.89	0.93	0.92
Average	0.88							

Table 7.2: Fractional Hamming Weight for Signatures Obtained from eight SRAM Chips Using the PowerUp Approach

The bias point of signatures is also estimated using the fractional Hamming weight. This measure indicates whether or not the cells prefer a certain state ('0' or '1'). Ideally, PUF signatures should have a fractional Hamming weight of 0.5. Figure 7.4 shows the fractional Hamming weights for all eight SRAM chips. The average fractional Hamming weight (the bias point) is shown in red.

Table 7.2 summarizes the average fractional Hamming weight values for all SRAM chips. This value is found to be 0.88 which is far from the ideal value of 0.5. This indicates that on average SRAM cells have a tendency toward '1' upon power-up.

Figure 7.5: Inter-die Hamming distance distribution of signatures obtained from eight SRAM chips using the PowerUp approach.

7.2.3 Uniqueness

To quantify the uniqueness of signatures, the inter-die Hamming distance is computed by calculating the fractional Hamming distance between the signatures obtained from the eight SRAM chips, considering all pairwise comparisons. This is a measure of how unique (or how dissimilar) the signatures are from chip to chip.

As Figure 7.5 shows, the average inter-die Hamming distance is found to be approximately 22%. The desirable value is 50% which means that half of the cells prefer a different state. The Inter-die Hamming distance values for all 28 pairwise signature comparisons are also summarized in Table 7.3.

7.2.4 Robustness

A. Robustness under Temperature Variation

To estimate the robustness of signatures under temperature variations, the average intra-die Hamming distance among the signatures is estimated by obtaining the signature for each chip at four different temperatures under the nominal supply voltage of 5 V and comparing that with the signature obtained at 25°C.

Signature Comparison	1,2	1,3	1,4	1,5	1,6	1,7	1,8	2,3	2,4	
Inter-die HD (%)	27.99	28.58	16.30	25.12	22.72	19.02	19.90	31.56	21.88	
Signature Comparison	2,5	2,6	2,7	2,8	3,4	3,5	3,6	3,7	3,8	
Inter-die HD (%)	29.37	27.21	23.89	24.77	21.62	28.50	27.19	23.61	24.16	
Signature Comparison	4,5	4,6	4,7	4,8	5,6	5,7	5,8	6,7	6,8	7,8
Inter-die HD (%)	17.49	14.38	9.68	10.55	23.76	20.07	20.71	17.22	17.67	13.74

Table 7.3: Inter-die Hamming distance Values for Pairwise Comparison of Signatures Obtained from eight SRAM Chips Using the PowerUp Approach

Figure 7.6: Percentage of fractional Hamming distance variation of signatures obtained from eight SRAM chips under temperature variation using the PowerUp approach.

Figure 7.6 shows the percentage of Fractional Hamming distance variation under varying temperatures. The intra-die Hamming distance values of signatures are also shown in Table 7.4.

Temperature	-25°C	0°C	50°C	75°C	Intra-die HD_{avg}
Chip1	27.83	21.52	11.51	13.73	18.65
Chip2	15.72	6.67	3.79	8.37	8.64
Chip3	5.67	3.69	2.53	6.20	3.96
Chip4	1.81	0.75	0.32	3.14	1.50
Chip5	18.00	12.53	3.16	7.37	8.59
Chip6	32.04	6.38	2.78	18.30	13.73
Chip7	26.39	7.48	1.97	5.38	10.30
Chip8	34.34	13.59	1.96	5.59	13.87
					Total = 12.44%

Table 7.4: Intra-die Hamming Distance Values of Signatures Obtained from eight SRAM Chips Under Temperature Variation Using the PowerUp Approach

Figure 7.7: Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from eight SRAM chips under temperature variation using the PowerUp approach.

Temperature is varied from -25°C to 75°C in 25°C increments. The average of highest signature variation is approximately 20% which occurs at -25°C where the V_{th} is at its highest value. As the temperature decreases, V_{th} increases. As a result, the selected write duty cycle is not long enough to fully charge the storage capacitor, resulting in a bit-flip from ‘1’ to ‘0’.

Figure 7.7 shows the distribution of average intra-die Hamming distance of the signatures obtained from eight chips under temperature variation. As it is shown, 62% of chips have fewer than 9% bit-flips in their signatures under varying temperatures.

Figure 7.8: Percentage of fractional Hamming distance variation of signatures obtained from eight SRAM chips under supply voltage variation using the PowerUp approach.

B. Robustness under Voltage Variation

To estimate the robustness of signatures under voltage variation, the average intra-die Hamming distance among the signatures is estimated by obtaining the signature for each chip at four different voltage levels at 25°C and comparing that with the signature obtained at the nominal supply voltage of 5 V under 25°C.

Figure 7.8 shows the percentage of fractional Hamming distance variation of the signatures obtained from eight SRAM chips under supply voltage variation. The intra-die Hamming distance values of signatures are also summarized in Table 7.5. The supply voltage is varied from 4 to 6 V in 0.5 V increments. The average intra-die Hamming distance is found to be 3.71%. The desirable value is zero which indicates there is no bit-flip under voltage variation. The highest average signature variation occurs at 4 V where the circuit performance is affected the most.

Figure 7.9 shows the distribution of average intra-die Hamming distance of the signatures obtained from eight SRAM chips under voltage variation using the PowerUp

Temperature	4.0 v	4.5 v	5.0 v	5.5 v	Intra-die HD_{avg}
Chip1	6.53	2.87	1.12	1.60	3.51
Chip2	6.48	4.35	2.95	3.44	4.30
Chip3	1.30	0.80	0.57	0.65	0.61
Chip4	0.65	0.52	0.44	0.49	0.52
Chip5	3.30	1.67	0.70	1.48	1.57
Chip6	26.24	16.54	1.48	6.53	12.70
Chip7	13.67	2.97	1.95	2.75	5.33
Chip8	1.75	1.06	0.73	0.94	1.12
					Total = 3.71%

Table 7.5: Intra-die Hamming Distance Values of Signatures Obtained from eight SRAM Chips Under Supply Voltage Variation Using the PowerUp Approach

Figure 7.9: Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from eight SRAM chips under supply voltage variation using the PowerUp approach.

approach. As it is shown, most of the chips (91%) have fewer than 7% bit-flips in their signatures under varying voltage levels.

7.3 The WRITE Approach

In the second set of experiments, a minor change is implemented in the write circuitry of SRAM in order to extract the PUF signatures using the WRITE approach. Figure 7.10 shows the SRAM block diagram with the modified write circuitry in blue.

Figure 7.10: Modified block diagram for SRAM (HT6116-70).

Figure 7.11: Timing diagram for the Write Enable signal for SRAM (HT6116-70) without the modified write circuitry.

The expected timing diagram for the Write Enable signal in the SRAM is shown in Figure 7.11. The minimum timings for the write pulse, setup time, and hold time are 25 ns, 20 ns, and 5 ns respectively.

Figure 7.12 shows the timing diagram of the Write Enable signal in the SRAM with the modified write circuitry. To extract PUF signatures, SRAM cells are initialized with '0's using a wide write pulse that satisfies the minimum timings. Next, random failures are induced by writing '1's using a shorter write pulse that violates

Figure 7.12: Timing diagram for the Write Enable signal for SRAM (HT6116-70) with the modified write circuitry.

the minimum timings. Write-0 provides the longer low pulse for the initialization phase and Write-1 provides the shorter low pulse for the randomization phase. The AND of the two pulses provides the Write Enable signal.

The following sections describe:

- Finding the appropriate write pulse for randomization
- Extracting PUF signatures by inducing write failures using the selected write pulse from the previous step followed by reading out the cell contents
- Excluding the unstable cells from PUF signatures
- Analyzing the signatures' uniqueness as well as robustness under voltage and temperature variation

7.3.1 Write Duty Cycle

For each SRAM chip, the appropriate write duty cycle is selected to ensure a 50% rate of success to failure in the Write-1 operation. Write duty cycle is measured from the negative going edge of $\overline{WE}$ to the positive going edge of $\overline{WE}$. Figure 7.13 shows the write duty cycle selection process for each SRAM chip. A Write-1 operation is performed using write duty cycles ranging from 0 to 25 ns with 0.5 ns increments

Figure 7.13: Best write duty cycle for SRAM to ensure a 50% rate of success to failure in Write-1 operation.

Chip	#1	#2	#3	#4	#5	#6	#7	#8
Write-1 Duty Cycle (ns)	12.69	10.85	7.82	10.96	9.37	9.19	12.89	10.87

Table 7.6: Write Duty Cycles for Signatures Obtained from eight SRAM Chips Using the WRITE Approach

(tester's resolution). For each write duty cycle, a Write-1 operation is performed, the content of SRAM is read, and the fractional Hamming weight is measured and plotted.

As Figure 7.13 shows, when the write duty cycle is very short, all SRAM cells fail to write '1'. As the write duty cycle gets wider, more cells succeed in writing '1'. And finally, for a wide write duty cycle, all SRAM cells succeed in writing '1'. For the PUF proposed in this work, the best write duty cycle is where the probability of write success to failure is 50-50. Table 7.6 summarizes the selected write duty cycles for all SRAM chips.

Figure 7.14: Bit-pattern of a randomly selected group of 250 cells in eight SRAM chips when a Write-1 operation is performed at different write duty cycles ranging from 0 to 25 ns. The distribution of unstable cells across the same duty cycle range is shown on right (X axis represents SRAM cell value and Y axis represents the duty cycle in ns. For the bar charts on right, X axis represents the number of unstable cells and Y axis represents the duty cycle in nanoseconds).

7.3.2 Stable Cells

Different memory cells may write ‘1’ at different write duty cycles depending on their variability which affects V_{th} and transistor switching time. Figure 7.14 shows a group of randomly selected cells in eight SRAM chips and their values after Write-1 operations are performed using write duty cycles ranging from 0 to 25 ns. The ‘X’ axis represents the 250 SRAM cells, and the ‘Y’ axis represents the varying write duty cycles. For short write duty cycles, all cells fail to write ‘1’, whereas for wide write duty cycles, all cells succeed (unless they have permanent defects). For duty

Figure 7.15: Snapshot of the bit-pattern of an SRAM chip (10 words by 8 bits) after each Write-1-Read attempt.

cycles in between, some cells may fail and some may succeed. As the width of the write duty cycle increases, more cells succeed the Write-1 operation. However, some cells may enter an instability zone where the cell values flicker between ‘0’s and ‘1’s.

To ensure robustness in PUF signatures, unstable cells are identified and excluded from PUF. The bar charts on the right side of Figure 7.14 show the unstable cells for different write duty cycles for all eight SRAM chips. As it is shown, the unstable cells are mostly distributed around the selected write duty cycle shown in blue where the cells are at their most unstable state as they transition from ‘0’ to ‘1’.

Finally, using the selected write duty cycle obtained from the described approach, a Write-1 operation is performed for each chip to get a random pattern of ‘0’s and ‘1’s with a fractional Hamming weight of 50%.

Reproducibility is one of the key characteristics of PUFs. The same signature has to be obtained every time the content of SRAM is read after a Write-1 operation is performed using the selected write duty cycle. To ensure reproducibility, the stable cells are identified by reading the content of the SRAM chip after the write attempt. This process is repeated ten times. A 10-min wait time is considered in between the attempts.

Figure 7.15 shows the snapshot of the bit-pattern of an SRAM chip after each Write-1-Read attempt. The white cells represent the cells storing ‘0’s and the black cells represent the cells storing ‘1’s. Cells are considered stable if they have a probabil-

Figure 7.16: Snapshots of the bit-patterns of eight SRAM chips (30 words by 8 bits) after ten Write-1-Read attempts. These snapshots do not represent the full signatures.

Chip	#1	#2	#3	#4	#5	#6	#7	#8
Unstable Cells (%)	13.31	6.45	11.29	2.42	6.05	8.87	1.21	11.29

Table 7.7: Percentage of Unstable Bits in Signatures Obtained from eight SRAM Chips Using the WRITE Approach

ity of 80% or higher of storing the same logic value over the ten attempts. In the end, there are some stable ‘0’s and some stable ‘1’s and some unstable cells highlighted in red. The unstable cells will not contribute in the PUF signature.

Figure 7.16 shows a larger snapshot of the bit-pattern of the eight SRAM chips after ten Write-1-Read attempts with the stable and unstable cells identified. Table 7.7 summarizes the percentage of unstable cells across the SRAM chips. The average percentage of unstable cells is found to be 7.61%.

For signature comparison, same length signatures are obtained from all eight chips. This is achieved by setting the highest percentage of unstable cells as the elimination target. For all chips, not only the unstable cells are eliminated. But additionally, randomly selected stable cells are also eliminated until the elimination target is reached. For the WRITE approach, the highest percentage of unstable cells is 13.31%, which leaves 14,593 stable cells for PUF signatures.

Chip	#1	#2	#3	#4	#5	#6	#7	#8
Fractional Hamming Weight	49.81	50.02	50.39	50.71	49.29	50.35	50.76	49.44
Average	50.09							

Table 7.8: Fractional Hamming Weight for Signatures Obtained from eight SRAM Chips Using the WRITE Approach

7.3.3 Randomness

To measure the randomness of signatures extracted from SRAMs using the proposed methodology, the min-entropy per cell is computed. This value is found to be 0.9856 which is very close to the ideal value of 1.0, indicating the signatures obtained using the WRITE methodology are highly unpredictable.

To estimate the bias point of signatures, fractional Hamming weight is computed. Table 7.8 shows the fractional Hamming weight values for all eight SRAM chips. The average value is found to be 50.09% which is very close to the ideal value of 50% indicating that the signatures have no preference for a certain state ('0' or '1').

7.3.4 Uniqueness

To quantify the uniqueness of signatures, the inter-die Hamming distance is computed by calculating the fractional Hamming distance between the signatures obtained from the eight SRAM chips, considering all pairwise comparisons. This is a measure of how unique (or how dissimilar) the signatures are from chip to chip. Figure 7.17 shows that for the signatures obtained using the WRITE approach, the average inter-die Hamming distance is found to be 50.4% which is very close to the ideal value of 50% indicating that the signatures are highly unique from chip to chip. Table 7.9 summarizes the inter-die Hamming distance values for pairwise signature comparisons.

Figure 7.17: Inter-die Hamming distance distribution of signatures obtained from eight SRAM chips using the WRITE approach.

Signature Comparison	1,2	1,3	1,4	1,5	1,6	1,7	1,8	2,3	2,4	
Inter-die HD (%)	51.23	45.61	51.62	51.59	50.04	52.44	43.25	54.44	45.23	
Signature Comparison	2,5	2,6	2,7	2,8	3,4	3,5	3,6	3,7	3,8	
Inter-die HD (%)	50.05	51.63	50.01	49.65	57.20	50.03	43.65	45.24	52.79	
Signature Comparison	4,5	4,6	4,7	4,8	5,6	5,7	5,8	6,7	6,8	7,8
Inter-die HD (%)	47.23	43.22	57.61	46.77	51.20	51.23	56.36	49.61	50.80	53.21

Table 7.9: Inter-die Hamming distance Values for Pairwise Comparison of Signatures Obtained from eight SRAM Chips Using the WRITE Approach

7.3.5 Robustness

A. Robustness under Temperature Variation

To estimate the robustness of signatures under temperature variation, the average intra-die Hamming distance among the signatures is estimated by obtaining the signature for each chip at four different temperatures under the nominal supply voltage

Figure 7.18: Percentage of fractional Hamming distance variation of signatures obtained from eight SRAM chips under temperature variation using the WRITE approach.

of 5 V and comparing that with the signature obtained at 25°C. Temperature is varied from -25°C to 75°C in 25°C increments.

Figure 7.18 shows the percentage of Fractional Hamming distance variation under varying temperatures. The intra-die Hamming distance values of signatures are summarized in Table 7.10.

The average of highest signature variation is 21.22% which occurs at -25°C where V_{th} is at its highest value. As temperature decreases, V_{th} increases. As a result, the selected write duty cycle is not long enough to fully charge the storage capacitor, resulting in a bit-flip from ‘1’ to ‘0’.

Figure 7.19 shows the distribution of average intra-die Hamming distance of the signatures obtained from eight chips under temperature variation. As it is shown, 44% of chips have fewer than 9% bit-flips in their signatures under varying temperatures.

Temperature	-25°C	0°C	50°C	75°C	Intra-die HD_{avg}
Chip1	31.76	17.04	10.09	13.36	18.06
Chip2	23.11	11.95	3.17	8.30	12.74
Chip3	11.00	3.66	1.78	3.40	2.72
Chip4	12.48	1.92	0.59	1.95	4.23
Chip5	15.70	10.51	2.00	7.88	9.19
Chip6	28.20	18.10	5.88	10.79	8.33
Chip7	20.64	10.11	3.01	5.56	9.83
Chip8	26.86	18.05	3.16	12.10	16.02
					Total = 10.14%

Table 7.10: Intra-die Hamming distance Values of Signatures Obtained from eight SRAM Chips Under Temperature Variation Using the WRITE Approach

Figure 7.19: Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from eight SRAM chips under temperature variation using the WRITE approach.

B. Robustness under Voltage Variation

To estimate the robustness of signatures under voltage variation, the average intra-die Hamming distance among the signatures is estimated by obtaining the signature for each chip at four different voltage levels at 25°C and comparing it with the signature obtained at the nominal voltage level of 5 V under 25°C. Voltage is varied from 4 to 6 V in 0.5 V increments.

Figure 7.20 shows the percentage of Fractional Hamming distance variation under varying voltages. The intra-die Hamming distance values are summarized in

Figure 7.20: Percentage of fractional Hamming distance variation of signatures obtained from eight SRAM chips under supply voltage variation using the WRITE approach.

Temperature	4.0 v	4.5 v	5.0 v	5.5 v	Intra-die HD_{avg}
Chip1	7.98	4.91	0.50	3.37	4.17
Chip2	5.99	4.29	1.00	3.55	3.71
Chip3	2.57	1.83	0.76	1.64	1.70
Chip4	1.84	1.31	0.53	0.95	1.16
Chip5	2.98	2.00	0.69	1.71	1.84
Chip6	28.88	12.00	3.72	8.09	13.17
Chip7	18.98	9.65	2.77	9.39	10.20
Chip8	3.49	2.67	1.01	2.56	2.43
					Total = 4.80%

Table 7.11: Intra-die Hamming Distance Values of Signatures Obtained from eight SRAM Chips Under Supply Voltage Variation Using the WRITE Approach

Table 7.11. For the signatures obtained under voltage variation using the WRITE approach, the average intra-die Hamming distance is found to be 4.80%. The desirable value is zero which means that there is no bit-flip under voltage variation. The highest average signature variation occurs at 4 V where the circuit performance is affected the most.

Figure 7.21 shows the distribution of average intra-die Hamming distance of the

Figure 7.21: Distribution of average intra-die Hamming distance (bit-flips) of the signatures obtained from eight SRAM chips under supply voltage variation using the WRITE approach.

signatures obtained under varying voltages. As it is shown, 91% of chips have fewer than 10% bit-flips in their signatures under voltage variation.

7.4 Summary

Table 7.12 summarizes the SRAM experimental results presented in this chapter. A comprehensive evaluation of SRAM PUF was presented in terms of uniqueness, randomness, and robustness under varying environmental conditions. For both methodologies, it takes only a few nanoseconds to generate the signatures.

Using the Hamming distance metric, the uniqueness of signatures obtained from SRAMs using both the PowerUp and the WRITE methodologies was evaluated. Results show that in comparison with the PowerUp approach, the proposed methodology produces signatures with significantly higher inter-die Hamming distance values.

Furthermore, the results from the min-entropy estimation show that the proposed methodology provides signatures with excellent randomness which makes this methodology resilient to modeling attacks.

Finally, results show that both methodologies provide a good level of robustness under temperature variation and excellent robustness under voltage variations.

SRAM Experimental Results

Methodology	PowerUp	WRITE
Authentication Time	Nanoseconds	Nanoseconds
Percentage of Stable Cells	99.31%	92.39%
Uniqueness	21.74%	50.40%
Min-entropy	0.1939	0.9856
Bias Point	87.88%	50.09%
Robustness under Temperature Variation	87.56% (-25°C to +75°C)	89.86% (-25°C to +75°C)
Robustness under Voltage Variation	96.29% (4 V to 6 V)	95.20% (4 V to 6 V)

Table 7.12: Summary of DRAM Experimental Results

Overall, the signatures obtained through the proposed methodology provide significantly better results in terms of uniqueness, randomness, and bias point, while providing high reproducibility under temporal fluctuations. Moreover, due to no dependency to power-up values, the proposed methodology is less vulnerable to side-channel attacks. All these make the proposed approach more suitable for extracting robust and unique signatures from SRAM.

Chapter 8

Analysis

This chapter describes a PUF based multi-key authentication scheme as an example application for the proposed authentication methodology. The second part of the chapter presents a comprehensive analysis on different PUF security measures including uniqueness, randomness, and robustness with respect to simulations and experimental results presented in Chapters 4, 6, and 7. The third and final part of the chapter provides a comparison of results between the proposed authentication methodology and the existing works published in the literature. A comparative analysis of the results between this work and the equivalent SRAM-based methodology is also provided.

8.1 PUF Based Multi-key Authentication Scheme

Today, PUFs are implemented in a variety of microprocessors and FPGAs, and are used in applications with high security requirements. PUFs are widely used for authentication purposes. In comparison to delay-based PUFs, memory-based PUFs are more suitable for authentication purposes. Memory-based PUFs are easier to implement and present negligible area overhead by utilizing the memory arrays already present in the design. They also don't need special customization as delay-based

Figure 8.1: PUF based multi-key authentication scheme.

PUFs do. Moreover, the independent nature of memory cells makes predicting the correct response bits harder as opposed to the mutually correlated response bits produced by delay-based PUFs. Overall, memory-based PUFs are more suitable for authentication.

As a low-cost authenticator, The DRAM PUF presented in this work has a major advantage among other implementations of memory-based PUF due to its large challenge-response space. The proposed PUF can be applied in more authentication protocols due to its easy and low-cost implementation, while providing strong authentication. The quality of authentication can be further increased using a multi-key PUF based authentication scheme. Due to the large number of bits available in DRAM array, multiple keys can be used for authentication. This increases the authentication quality and minimizes the risk of key denial especially due to ageing as different keys obtained from different parts of DRAM array might have been impacted differently due to NBTI or other ageing factors.

Figure 8.1 illustrates a multi-key PUF based authentication scheme between Alice and Bob. Alice who has access to the authentic device with an embedded DRAM PUF, collects a set of challenge-response pairs $(c, r_1, r_2, \dots, r_n)$ generated from the PUF instance P and stores them in a database. P is then delivered to Bob through

the untrusted supply chain. To authenticate P , Alice randomly selects an unused challenge c_i and sends it to Bob. Bob applies c_i to P to generate a number of responses $r_{i1}', r_{i2}', \dots, r_{in}'$ depending on the authentication strength required and sends the responses back to Alice. Alice validates the responses against the database. If the responses match, then Bob is in possession of an authentic P .

8.2 PUF Evaluation

This section provides a comprehensive evaluation of the common security properties of PUFs. The evaluation is performed with respect to the authentication methodology proposed in this work.

8.2.1 Cell Stability Evaluation

The proposed authentication methodology presents a process to identify highly stable cells within the large set of available memory cells in a DRAM array. This ensures PUF is highly robust across different operating conditions by excluding the unstable cells that can easily flip.

A stable cell is a cell that consistently generates the same logic value ('0' or '1') in the read attempts conducted at room temperature and the nominal supply voltage. An 80% consistency rate threshold has been considered to identify the stable cells. This takes into account the random noises and their impact on the value of the memory cells.

8.2.2 Randomness Evaluation

Randomness is one of the most important security properties of PUFs. Randomness is a measure of unpredictability of the PUF response to a given challenge despite prior knowledge of a large number of CRPs. In a perfectly random PUF, responses

(also known as signatures) are generated independent of each other. In the context of memory-based PUF, this means that the value of a memory cell cannot be predicted regardless of how many cell values are known.

Randomness of PUF can be estimated through statistical tests such as the NIST test [38], machine learning techniques, Shannon Entropy, or min-entropy. While in practice it is easier to evaluate Shannon entropy than other entropy estimations, it is known that Shannon entropy does not provide a good estimate of randomness quality from a cryptographic viewpoint. In this dissertation, min-entropy is used as the metric to estimate the randomness of PUF responses (signatures).

Min-entropy is a conservative entropy estimation to measure the level of uncertainty associated with PUF signatures. Min-entropy indicates how many bits of a PUF signature are uniformly random. This value should be large enough to guarantee resistance against attacks. An ideal PUF has a min-entropy of 1.0.

Consider m chips, $m = 1, 2, \dots, M$, with each chip having k cells, $k = 1, 2, \dots, K$, where k represents the cells contributing to a PUF signature. To estimate the min-entropy, the fractional Hamming weight of cell k denoted $HW(k)$ is determined over all chip signatures. $HW(k)$ provides an estimate of the probability of cell k to be ‘1’. Then P_{max} provides the most likely outcome of cell k as follows:

$$P_{max}(k) = \max\{HW(k); 1 - HW(k)\} \quad (8.1)$$

The min-entropy is then defined as the log of the most likely outcome [59], which in the concept of PUF corresponds to guessing a response correctly in one go. This is a very conservative entropy estimation, but a good one for measuring uncertainty about a cryptographic key. This procedure is repeated for all cells, and after averaging, it gives the total entropy per cell. This method should only be used if the cells are

independent which usually is assumed.

$$H_{min} = \frac{1}{K} \sum_{k=1}^K -\log P_{max}(k) \quad (8.2)$$

For the PUF experiments described in Chapters 6 – 7, the signatures extracted using the proposed methodology, provide min-entropies close to the ideal value of 1.0 which indicates signatures are highly unpredictable.

8.2.3 Uniqueness Evaluation

Uniqueness is a measure of how dissimilar (uncorrelated) the PUF signatures are across dies. In the context of memory-based PUF, uniqueness means that the response resulting from evaluating the same challenge on a different instance of PUF should be dissimilar. Uniqueness is a function of the inherent process variation of a manufacturing process.

To evaluate the uniqueness of PUF responses (signatures), the inter-die Hamming distance is computed by calculating the fractional Hamming distance between the signatures obtained from different chips, considering all pairwise comparisons. Assuming R_i and R_j are K -bit signatures obtained from chip i and chip j , the average inter-die Hamming distance for m chips is then defined as [60]:

$$inter-die\ HD_{avg} = 100\% \times \frac{2}{m(m-1)} \sum_{i=1}^{m-1} \sum_{j=i+1}^m \frac{inter-die\ HD(R_i, R_j)}{K} \quad (8.3)$$

Ideally, the Hamming distance between the PUF signatures is 50%, indicating there is no correlation between the signatures. This makes predicting the PUF behavior more difficult even knowing a collection of CRPs.

For the PUF experiments described in Chapters 6 – 7, the signatures extracted using the proposed methodology provide average inter-die Hamming distance values

close to 50% which indicates signatures are highly unique from chip to chip.

8.2.4 Robustness Evaluation

Besides randomness and uniqueness, robustness (also known as reproducibility or reliability) is another important security measure of PUFs. Ideal PUFs are robust even under temporal fluctuations. Robustness indicates how resilient PUF signatures are under non-ideal operating conditions, such as temperature variation, supply voltage variation, and ageing.

For a PUF to be robust, the signature obtained at a non-ideal operating condition should not differ significantly from the one obtained under normal conditions. To quantify the robustness of signatures, the intra-die Hamming distance between the signatures from the same chip subject to varying operating conditions is computed. To compute intra-die Hamming distance, an K -bit signature, R' , is extracted from each chip at a non-ideal operating condition. The signature is then compared to the signature, R , obtained from the same chip under normal conditions. Assuming N samples of R' are taken for each of the operating conditions, the average intra-die Hamming distance for chip i is estimated as the intra-die Hamming distance between R_i and R_i' over N samples and is defined as:

$$intra-die\ HD_{avg} = 100\% \times \frac{1}{N} \sum_{k=1}^N \frac{intra-die\ HD(R_i, R'_{i,k})}{K} \quad (8.4)$$

The total average intra-die Hamming distance is then computed by averaging all the average intra-die Hamming distance values over m chips. For high robustness, it is desirable to have a total average intra-die Hamming distance close to zero.

A. Robustness under Temperature Variation

Temperature variations can have a major impact on the robustness of PUF. The operational temperature affects the on-chip junction temperatures which in turn affects the delay of gates and wires, and therefore possibly causing a change in the PUF behavior.

To estimate the robustness of PUF signatures under temperature variation, the average intra-die Hamming distance among the signatures is estimated by obtaining the signature for each chip at different temperatures under nominal supply voltage and comparing it with that obtained at room temperature.

As temperature increases, device performance degrades. With slower device performance, the selected write duty cycle will not be long enough to fully charge the storage capacitor, resulting in a bit-flip from ‘1’ to ‘0’.

For the PUF experiments described in Chapters 6 – 7, the signatures extracted using the proposed methodology provide a good level of robustness under temperature fluctuations.

B. Robustness under Voltage Variation

Like temperature, variations in supply voltage can also have an impact on the robustness of PUF. Decreasing the supply voltage slows down the circuit and affects the reliability as different parts of the circuit suffer from a non-linear performance loss.

To estimate the robustness of PUF under voltage variation, the average intra-die Hamming distance among the signatures is estimated by obtaining the signature for each chip at different voltage levels under room temperature and comparing it with that obtained at the nominal voltage level.

For the PUF experiments described in Chapters 6 – 7, the signatures extracted using the proposed methodology provide a good level of robustness under supply voltage fluctuations.

C. Robustness under Ageing Effect

The main environmental factors causing changes in PUF response behavior are operational temperature and supply voltage. However, the degradation of electrical components over time can also impact PUF’s reliability. Several ageing causes have been identified such as electro-migration (EM) hot carrier injection (HCI), time-dependent dielectric breakdown (TDDB) and most prominently negative bias temperature instability (NBTI). NBTI is caused by the generation of trapped charges and can result in degradation of V_{th} in PMOS transistors which can in turn affect the reproducibility of PUF signatures.

For NBTI evaluation, the PMOS technology file was updated to reflect the expected shift in V_{th} corresponding to 1, 3, 5, and 10 years lifetime of the product. Simulation results described in Chapter 4 show that the signatures extracted using the proposed methodology provide excellent robustness under NBTI effect with less than 1% bit-flips in 10 years. For SRAMs however, the impact of NBTI is considered to be higher due to the existence of PMOS transistors in the SRAM cell structure.

8.2.5 Hardware Overhead Evaluation

Most PUFs rely on dedicated circuitry solely added for the purpose of unique signature generation and hence present large area overhead which might not be feasible in all designs. The authentication methodology presented in this work utilizes the memory array already present on the hardware for unique signature generation. Therefore, the area overhead is only due to the delay generator which is a small fixed circuit independent of the size of RAM. The area overhead becomes negligible for large off-the-shelf DRAMs with several Gigabytes of storage.

8.2.6 Vulnerability Evaluation

One of the advantages of the proposed authentication methodology over other implementations of PUF such as delay-based PUFs is that it is more resilient to modeling attacks due to the independent nature of the memory cells which makes predicting the correct response harder. Furthermore, an average inter-die Hamming distance value of close to 50% ensures low correlation between PUF signatures which strengthens the PUF even more against possible attacks.

Although no memory-based PUF is immune from side-channel attacks, DRAM PUF is evaluated to be less vulnerable compared to other PUF implementations due to the fact that storage capacitors are physically placed below transistors in DRAM cells. This makes probing extremely difficult when using Focused Ion Beam (FIB) techniques [17].

Also because the storage capacitors are small and therefore the observed voltage changes are very small, any probing will result in changing the PUF measurements, making the proposed authentication methodology naturally tamper-evident.

8.3 Comparisons

This section provides a comparative analysis of the simulations and experimental results presented in Chapters 4, 6, and 7.

A. The Proposed Methodology vs. The Equivalent SRAM-based Methodology

Table 8.1 compares the results from the proposed DRAM-based authentication methodology with the equivalent SRAM-based methodology. A comprehensive evaluation of security properties including uniqueness, randomness, and robustness under varying operating conditions have been performed under the same test conditions.

	This Work	Equivalent SRAM-based Authentication Methodology
Authentication Time	Nanoseconds	Nanoseconds
Percentage of Stable Cells	82.67%	92.39%
Uniqueness	50.21%	50.40%
Min-entropy	0.9215	0.9856
Bias Point	49.99%	50.09%
Robustness under Temperature Variation	82.12% (-25°C to +75°C)	89.86% (-25°C to +75°C)
Robustness under Voltage Variation	81.58% (Nominal voltage $\pm 10\%$)	95.2% (Nominal voltage $\pm 10\%$)
Robustness under Ageing	99.20% (10 Years)	More impacted by NBTI due to the PMOS transistors in SRAM cell structure
Vulnerability to Side-channel Attacks	Less vulnerable due to difficulty of probing	More vulnerable due to ease of probing

Table 8.1: Comparison of Results between the Proposed Methodology and the Equivalent SRAM-based Methodology

Experimental results from DRAMs and SRAMs show a higher percentage of unstable cells across DRAM. This is mainly due to the small size of storage capacitors in DRAM. A small voltage change can cause a bit-flip in a DRAM cell, whereas in an SRAM cell the same amount of voltage change might not impact the cell value. Despite the higher percentage of unstable cells, DRAMs still provide a significantly large set of CRPs due to their large dense structures. This characteristic of DRAM is very valuable and makes it stand out among other types of memory-based PUFs.

The results from both SRAMs and DRAMs show that the proposed methodology generates signatures with excellent randomness and uniqueness, and good robustness under temperature and voltage variations. In comparison to SRAMs, however, DRAMs are found to be slightly less robust when subjected to voltage variations. This is mainly due to small storage capacitors in DRAM cells. Very slight variations in the supply voltage can alter the voltage differential across the capacitor and cause a bit-flip. Similarly, in comparison to SRAMs, DRAMs are found to be slightly less

robust to temperature variations. This is due to the impact of temperature on V_{th} which affects the rate of charge decay and can cause a bit-flip.

Although no memory-based PUF is immune from side-channel attacks, DRAM-based PUFs are evaluated to be less vulnerable compared to other implementations. This is due to the fact that in a DRAM cell structure, the capacitor is physically placed below the transistor. This makes probing extremely difficult. Also because the capacitors are small and therefore the observed voltage changes are very small, any probing will change the PUF behavior making the proposed DRAM-based authentication methodology naturally tamper evident.

Finally, based on the *HSPICE* simulation results presented in Chapter 4, the proposed authentication methodology provides excellent robustness under ageing effect (NBTI) with less than 1% bit-flips in 10 years. For the SRAM-based methodology, however, the impact of NBTI is considered to be higher due to the existence of PMOS transistors in the SRAM cell structure.

B. The Proposed Methodology vs. Other DRAM-based Methodologies

Table 8.2 compares the results from this work against other DRAM-based methodologies published in the literature. Overall, this work provides a comprehensive evaluation of PUF signatures in terms of uniqueness, entropy, and robustness under variations in environmental conditions and ageing.

The methodology proposed in this work incurs very low design overhead by utilizing the DRAM array already present in the design. Also, the nature of the proposed methodology lends itself to be faster than the methods in [15, 16]. Furthermore, the proposed methodology produces a higher percentage of stable cells that can contribute in PUF signatures as compared to the method in [17].

The inter-die Hamming distance results show that the number of bits differing between two random signatures in the proposed methodology is 50.21% which is very

	This Work	Keller, et al. [15]	Liu, et al. [16]	Tehranipoor, et al. [17]
Authentication Time	Nanoseconds	Hours	Minutes	Nanoseconds
Percentage of Stable Cells	82.67%	NA	NA	74.5%
Uniqueness[1]	50.21%	NA	49.97%	49.37%
Min-entropy	0.9215	NA	0.71	0.9483
Bias Point	49.99%	NA	NA	53.62%
Robustness under Temperature Variation	82.12% (-25°C to +75°C)	NA	88% (unknown range)	56.93% (0°C, +80°C)
Robustness under Voltage Variation	81.58% (Nom. voltage $\pm 10\%$)	NA	NA	39.00% (Nom. voltage $\pm 10\%$)
Robustness under Ageing	99.20% (10 Years)	NA	NA	82.67% (1 Year)
Vulnerability to Side-channel Attacks	Less vulnerable due to no dependency on power-up values	Less vulnerable due to no dependency on power-up values	Less vulnerable due to no dependency on power-up values	More vulnerable due to dependency on power-up values

Table 8.2: Comparison of Results between the Proposed Methodology and other DRAM-based Methodologies

close to the ideal value of 50%, just like methods in [16, 17]. Moreover, the proposed methodology provides a normalized min-entropy of 0.92 which is very close to the ideal value of one as compared to 0.71 in method [16].

Using the fractional Hamming weight, the bias point of the signatures in the proposed methodology is found to be 49.99% which is very close to the ideal value of 50% as compared to 53.62% in [17]. Furthermore, results show that the proposed methodology is more robust under temperature and voltage variations compared to the method in [17]. Finally, unlike the method in [17] the proposed approach has no dependency on memory power-up values and therefore it is less prone to side-channel attacks.

Chapter 9

Conclusion

This chapter provides a summary of the dissertation, the concluding remarks, and recommendations on future research directions.

9.1 Summary

In this dissertation, a robust and secure authentication methodology was presented using PUFs in DRAM arrays. This novel DRAM-based authentication methodology leverages on word line duty-cycle-controlled write failures to produce device-specific signatures that can be used for authentication purposes.

HSPICE simulation results for 1000 chips with 10% inter- and 8% intra-die variation show that the proposed methodology provides excellent uniqueness of 50.01% inter-die Hamming distance. It also provides good reproducibility under varying temperatures and supply voltage. Furthermore, ageing analysis shows that under NBTI effect, signatures have only less than 1% bit-flips over a 10-year lifetime. Moreover, the proposed methodology incurs very low design overhead by utilizing the DRAM array already present in the design.

The simulation results were validated through experiments performed on real DRAM chips. The results show that the proposed methodology provides signatures

with excellent randomness and uniqueness. In comparison to other works published in the literature, the signatures provide higher robustness under temporal fluctuations. Another advantage of the proposed methodology over the existing DRAM-based methodologies is that it has no dependency to memory power-up values which makes it less vulnerable to side-channel attacks.

The effectiveness of the proposed methodology was further evaluated through experiments performed on real SRAM chips. Results show that in comparison to SRAM, the proposed methodology provides higher uniqueness, but slightly lower robustness under temporal fluctuations due to less tolerance to voltage changes which cause some cells to flip easier. While the proposed methodology may not exhibit the same levels of robustness under varying operating conditions as the SRAM counterpart, however, it offers an opportunity to provide authentication mechanisms by utilizing the existing DRAMs in SoCs that do not have SRAMs, or simply require a larger set of CRPs without compromising the physical footprint of the system.

9.2 Future Research Directions

Despite the many advantages of the proposed authentication methodology, there are still many areas to investigate and improve. What follows describes the possible extensions to the authentication methodology presented in this dissertation.

- *Validation of Simulation Results on Ageing:* In this dissertation, the impact of ageing effect (particularly NBTI) on PUF robustness was evaluated through *HSPICE* simulations presented in Chapter 4. As part of the future work, these simulations can be validated through experiments leveraging accelerated ageing techniques on real DRAM chips .
- *Evaluation of Robustness under Temperature and Voltage Variation:* In Chapters 4 and 6, robustness of PUF has been evaluated under one source of varia-

tion at a time (temperature or voltage variation). As part of the future work, robustness can be evaluated in presence of fluctuations in both of these.

- *Introducing other Types of Variation:* In addition to temperature and voltage, other sources and types of variation in operating conditions such as vibration and radiation can be introduced to further evaluate the robustness of PUF in real-world environments.
- *Improving the Stable Cell Selection Process:* In the experiments described in Chapter 6, the stable cell selection process is described. This process is based on identifying the cells that consistently pass or fail a Write-1 attempt that is performed using a duty-cycle-controlled write pulse. This exercise is conducted at room temperature and the nominal supply voltage with no variation present. To further improve this process, variations in temperature and voltage can also be introduced so that the cells that are truly stable are selected. This will improve the reproducibility of PUF signatures in presence of variation.
- *Other Possible Applications:* Another interesting topic as part of the future work is to extend the proposed authentication methodology to produce unique signatures in modern DRAMs as well as other forms of memory.

Bibliography

- [1] “What are the Stimulus Formats?, Q’nApps #s17.” <http://www.hilevel.com/Snotes.html>.
- [2] “Epoch Test Solution User Manual.” <http://www.hilevel.com>.
- [3] “Iot security. digital image. emnify news. 1 oct, 2017. web. 17 aug 2016.” <https://www.emnify.com/2016/08/17/iot-security-sms>.
- [4] B. C. Grubel, B. T. Bosworth, M. R. Kossey, H. Sun, A. B. Cooper, M. A. Foster, and A. C. Foster, “Silicon photonic physical unclonable function,” *Opt. Express*, vol. 25, pp. 12710–12721, May 2017.
- [5] “Can Symphony help me generate a list of pins and associated parameters?, Q’nApps #s1.” <http://www.hilevel.com/Snotes.html>.
- [6] “THERMONICS Precision Temperature Forcing Systems User Manual.” <https://www.axiomtest.com/documents/models/Ther%20T-2500%20Datasheet.pdf>.
- [7] F. Hamzaoglu, U. Arslan, N. Bisnik, S. Ghosh, M. B. Lal, N. Lindert, M. Meterelliyoz, R. B. Osborne, J. Park, S. Tomishima, Y. Wang, and K. Zhang, “A 1Gb 2GHz embedded DRAM in 22nm Tri-Gate CMOS technology,” in *2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*, pp. 230–231, Feb 2014.

- [8] J. Barth, D. Plass, E. Nelson, C. Hwang, G. Fredeman, M. Sperling, A. Mathews, T. Kirihaata, W. R. Reohr, K. Nair, and N. Cao, “A 45 nm soi embedded dram macro for the powerTM processor 32 mbyte on-chip l3 cache,” *IEEE Journal of Solid-State Circuits*, vol. 46, pp. 64–75, Jan 2011.
- [9] “SiliconMotion.” <http://www.siliconmotion.com/A6.1.DetailNews.php?sn=154>.
- [10] “Security in the internet of things, White Paper, Wind River, Jan 2015.” <https://www.windriver.com/whitepapers/security/security-in-the-internet-of-things>.
- [11] N. Dhanjani, *Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts*. O’Reilly Media, 2015.
- [12] C. Herder, M. Yu, F. Koushanfar, and S. Devadas, “Physical unclonable functions and applications: A tutorial,” *Proceedings of the IEEE*, vol. 102, pp. 1126–1141, Aug 2014.
- [13] “SmartFusion2 SoC FPGAs.” <http://www.microsemi.com/products/fpga-soc/socfpga/smartfusion2>.
- [14] “QuiddikeyR -Flex - Flexible key storage module based on Hardware Intrinsic SecurityTM.” <http://www.intrinsic-id.com/products/quiddikey\OT1\textendashflex/>.
- [15] C. Keller, F. Gürkaynak, H. Kaeslin, and N. Felber, “Dynamic memory-based physically unclonable function for the generation of unique identifiers and true random numbers,” in *2014 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 2740–2743, June 2014.

- [16] W. Liu, Z. Zhang, M. Li, and Z. Liu, “A trustworthy key generation prototype based on DDR3 PUF for wireless sensor networks,” in *2014 International Symposium on Computer, Consumer and Control*, pp. 706–709, June 2014.
- [17] F. Tehranipoor, N. Karimian, W. Yan, and J. A. Chandy, “DRAM-based intrinsic physically unclonable functions for system-level security and authentication,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 3, pp. 1085–1097, 2016.
- [18] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, “Design and implementation of puf-based ”unclonable” rfid ics for anti-counterfeiting and security applications,” in *2008 IEEE International Conference on RFID*, pp. 58–64, April 2008.
- [19] U. Rührmair, “Oblivious transfer based on physical unclonable functions,” in *Trust and Trustworthy Computing* (A. Acquisti, S. W. Smith, and A.-R. Sadeghi, eds.), (Berlin, Heidelberg), pp. 430–440, Springer Berlin Heidelberg, 2010.
- [20] M. van Dijk and U. Rührmair, “Physical unclonable functions in cryptographic protocols: Security proofs and impossibility results,” *IACR Cryptology ePrint Archive*, vol. 2012, p. 228, 2012.
- [21] M. E. Van Dijk, “System and method of reliable forward secret key sharing with physical random functions,” Jan. 26 2010. US Patent 7,653,197.
- [22] F. Koushanfar, “Provably secure active ic metering techniques for piracy avoidance and digital rights management,” *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 51–63, Feb 2012.
- [23] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, “Silicon physical random functions,” in *Proceedings of the 9th ACM Conference on Computer and Com-*

- munications Security*, CCS '02, (New York, NY, USA), p. 148–160, Association for Computing Machinery, 2002.
- [24] X. Wang and M. Tehranipoor, “Novel physical unclonable function with process and environmental variations,” in *2010 Design, Automation Test in Europe Conference Exhibition (DATE 2010)*, pp. 1065–1070, March 2010.
 - [25] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in *2007 44th ACM/IEEE Design Automation Conference*, pp. 9–14, June 2007.
 - [26] A. R. Krishna, S. Narasimhan, X. Wang, and S. Bhunia, “MECCA: a robust low-overhead PUF using embedded memory array,” in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 407–420, Springer, 2011.
 - [27] Y. Zheng, M. S. Hashemian, and S. Bhunia, “RESP: A robust physical unclonable function retrofitted into embedded SRAM array,” in *Proceedings of the 50th Annual Design Automation Conference*, pp. 1–9, 2013.
 - [28] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, “Modeling attacks on physical unclonable functions,” in *Proceedings of the 17th ACM conference on Computer and communications security*, pp. 237–249, 2010.
 - [29] G. T. Becker, “On the pitfalls of using arbiter-PUFs as building blocks,” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 8, pp. 1295–1307, 2015.
 - [30] B. Köpf and D. Basin, “An information-theoretic model for adaptive side-channel attacks,” in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 286–296, 2007.

- [31] X. Xu and W. Burleson, “Hybrid side-channel/machine-learning attacks on PUFs: A new threat?,” in *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 1–6, IEEE, 2014.
- [32] A. Mahmoud, U. Rührmair, M. Majzoobi, and F. Koushanfar, “Combined Modeling and Side Channel Attacks on Strong PUFs,” *IACR Cryptology ePrint Archive*, vol. 2013, p. 632, 2013.
- [33] C. Helfmeier, C. Boit, D. Nedospasov, and J.-P. Seifert, “Cloning physically unclonable functions,” in *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pp. 1–6, IEEE, 2013.
- [34] S. Zeitouni, Y. Oren, C. Wachsmann, P. Koeberl, and A.-R. Sadeghi, “Remanence decay side-channel: The PUF case,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1106–1116, 2015.
- [35] D. Wang and D. Modern, *memory systems: performance analysis and a high performance, power-constrained DRAM-scheduling algorithm*. PhD thesis, PhD thesis, 2005.
- [36] M. S. Hashemian, B. Singh, F. Wolff, D. Weyer, S. Clay, and C. Papachristou, “A robust authentication methodology using physically unclonable functions in DRAM arrays,” in *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 647–652, IEEE, 2015.
- [37] “Predictive technology model.” <http://www.eas.asu.edu/ptm/>.
- [38] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo, “Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications,” tech. rep., Gaithersburg, MD, USA, 2010.

- [39] M.-D. Yu, R. Sowell, A. Singh, D. M'Raihi, and S. Devadas, "Performance metrics and empirical results of a PUF cryptographic key generation ASIC," in *2012 IEEE International Symposium on Hardware-Oriented Security and Trust*, pp. 108–115, IEEE, 2012.
- [40] R. van den Berg *et al.*, "Entropy analysis of physical unclonable functions," *Ph. D. dissertation, Dept. of Math and Computer Science, Eindhoven University of Technology*, 2012.
- [41] R. van den Berg, B. Skoric, and V. van der Leest, "Bias-Based Modeling and Entropy Analysis of PUFs," in *Proceedings of the 3rd International Workshop on Trustworthy Embedded Devices*, TrustED '13, (New York, NY, USA), p. 13–20, Association for Computing Machinery, 2013.
- [42] H. Luo, Y. Wang, K. He, R. Luo, H. Yang, and Y. Xie, "Modeling of PMOS NBTI Effect Considering Temperature Variation," in *8th International Symposium on Quality Electronic Design (ISQED'07)*, pp. 139–144, March 2007.
- [43] "hilevel." <http://www.hilevel.com/products.html>.
- [44] "Andgate." <https://www.ti.com/products/SN54S09>.
- [45] "NEC μ PD416-3 16K $\times$ 1-Bit Dynamic MOS RAM." <http://www.ralphselectronics.com/productimages/SEMI-UPD416.PDF>.
- [46] "Holtek HT6116-70 CMOS 2K $\times$ 8-Bit SRAM Datasheet." <https://www.cl.cam.ac.uk/teaching/2004/Hardware/datasheets/ht6116.pdf>.
- [47] "What must be done to prepare for a functional test?, Q'nApps #s26." <http://www.hilevel.com/Snotes.html>.
- [48] "Bypass caps? Who needs 'em?, Q'nApps #s22." <http://www.hilevel.com/Snotes.html>.

- [49] “What about connecting Power and Ground?, Q’nApps #s20.” <http://www.hilevel.com/Snotes.html>.
- [50] “What is Split I/O?, Q’nApps #s42.” <http://www.hilevel.com/Snotes.html>.
- [51] “If I’m unlucky enough to have a chip but little else, how can I test it?, Q’nApps #s13.” <http://www.hilevel.com/Snotes.html>.
- [52] “How do I use the ”Inhibit Delay” in the Pin Setup?, Q’nApps #s23.” <http://www.hilevel.com/Snotes.html>.
- [53] “How can I define ACPMU tests?, Q’nApps #s55.” <http://www.hilevel.com/Snotes.html>.
- [54] “How do I transfer simulator vectors into Symphony?,Q’nApps #s2.” <http://www.hilevel.com/Snotes.html>.
- [55] “How does HiLevel define ”data” and ”clock” rate?, Q’nApps #s24.” <http://www.hilevel.com/Snotes.html>.
- [56] “Can I measure for pin-to-pin continuity?, Q’nApps #s45.” <http://www.hilevel.com/Snotes.html>.
- [57] “Can DUT Continuity be tested faster?, Q’nApps #s51.” <http://www.hilevel.com/Snotes.html>.
- [58] “When should I run calibration and diagnostics?, Q’nApps #s60.” <http://www.hilevel.com/Snotes.html>.
- [59] S. Katzenbeisser, Ü. Kocabaş, V. Rožić, A.-R. Sadeghi, I. Verbauwhede, and C. Wachsmann, “Pufs: Myth, fact or busted? a security evaluation of physically unclonable functions (pufs) cast in silicon,” in *Cryptographic Hardware and Embedded Systems – CHES 2012* (E. Prouff and P. Schaumont, eds.), (Berlin, Heidelberg), pp. 283–301, Springer Berlin Heidelberg, 2012.

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