

INVESTIGATION OF COTS NVM TECHNOLOGIES FROM A RELIABILITY AND SECURITY PERSPECTIVE

SUPRIYA CHAKRABORTY



**DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY DELHI**

JUNE 2023

©Indian Institute of Technology Delhi (IITD), New Delhi, 2023

INVESTIGATION OF COTS NVM TECHNOLOGIES FROM A RELIABILITY AND SECURITY PERSPECTIVE

by

Supriya Chakraborty

DEPARTMENT OF ELECTRICAL ENGINEERING

submitted

in fulfillment of the requirement of the degree of Doctor of Philosophy

to the



INDIAN INSTITUTE OF TECHNOLOGY DELHI

JUNE 2023

Dedicated to

*My Mother, Father, Sister, and my friend cum wife Swatilkeha Majumdar. They have always been
the pillars of my strength and inspiration.*

कर्मण्येवाधिकारस्ते मा फलेषु कदा चन ।
मा कर्मफलहेतुर्भूर्मा ते सङ्गो ऽस्वकर्मणि ॥ २-४७ ॥

karmaṇy evādhikāras te mā phaleṣu kadā cana ।
mā karmaphalahetur bhūr mā te saṅgo 'stv akarmaṇi ॥2-47॥

- *Shrimad Bhagwad Gita, Chapter 2, Verse 47*

বাংলা: আপনার নির্ধারিত দায়িত্ব পালনের অধিকার আপনার রয়েছে, তবে আপনি নিজের কর্মের ফলের অধিকারি নন। নিজেকে কখনই আপনার ক্রিয়াকলাপের ফলাফলের কারণ হিসাবে বিবেচনা করবেন না এবং নিষ্ক্রিয়তা সাথে সংযুক্ত থাকবেন না।

हिंदी: आपको अपने निर्धारित कर्तव्यों को निभाने का अधिकार है, लेकिन आप अपने कार्यों के फल के हकदार नहीं हैं। कभी भी अपने आप को अपनी गतिविधियों के परिणामों का कारण न समझें, न ही निष्क्रियता से जुड़े रहें।

English: You have a right to perform your prescribed duties, but you are not entitled to the fruits of your actions. Never consider yourself to be the cause of the results of your activities, nor be attached to inaction.

CERTIFICATE

This is to certify that the thesis entitled **“INVESTIGATION OF COTS NVM TECHNOLOGIES FROM A RELIABILITY AND SECURITY PERSPECTIVE”** being submitted by Mr. **Supriya Chakraborty** for the award of the degree of Doctor of Philosophy in the Department of Electrical Engineering, Indian Institute of Technology Delhi, is a record of bonafide work done by him under my supervision and guidance. The thesis has reached the standards fulfilling the requirements of the regulations related to the award of the degree. The matter embodied in this thesis has not been submitted for the award of any other degree or diploma.

Place: New Delhi
Date:

Dr. Manan Suri
Associate Professor
Department of Electrical Engineering
Indian Institute of Technology, Delhi
Hauz Khas, New Delhi- 110016, India

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest gratitude to my supervisor, **Prof. Manan Suri** for his invaluable advice, continuous support, and patience during my Ph.D. He was kind enough to take me under his supervision when I was in the midst of a professional crisis. This endeavor would not have been possible without his constant motivation, and enormous belief in me. His guidance helped me in all the time of research and writing of this thesis.

I want to extend my gratitude to the Ministry of Education, Government of India, and Department of Electrical Engineering, Indian Institute of Technology Delhi for the Ph.D. scholarship and for providing me with the laboratory resources to perform this research activity. The dissertation would not have been possible without their financial backing and research facilities.

I would like to thank my Student Review Committee (SRC) members Prof. Ratnamala Chatterjee, Prof. Anuj, Dhawan, and Dr. Vivek Venkatraman for their valuable feedback. I am also grateful to Dr. Saakshi Dhanekar for her valuable feedback during the research review process and for teaching me the course semiconductor material and device characterization which helped me during my research work. I would like to thank my thesis evaluation committee members for their constructive feedback, availability and time.

I would like to express my gratitude to all the group members/colleagues of NVM and Neuro-morphic hardware research group including Abhishek Gupta, Tinish Bhattacharya, Sai Sukruth Bezugam, Alok Deep, Tamoghno Das for knowledge-sharing technical and non-technical discussions.

I would also like to extend my deepest appreciation to all my friends and colleagues with special mention to Dr. Swatilekha Majumdar (now at IBM, Germany), Dr. Atul Thakur (now at Mediatek Inc., Bangalore), Dr. Rajib Ratan Ghosh (now at TU Eindhoven, The Netherlands), Rohit Sarwal (now at Synopsis, Noida), Manoj Kumar, Abhilash Garg (now at Synopsis, Noida), Dr. Roohie Kaushik ma'am, Dr. Shubham Sahay (now assistant professor, IIT kanpur) for providing me a surrogate family, and lifetime cherished memories. I will always be grateful to all of them for being their during my ups and downs throughout this period. I would also like to take this opportunity to thank, Dr. Usham Viviano Dias, Aashish T. R., all my hostel mates with special mention to

Dushyant Kumar, Satish Kumar Verma, Kalyan Dash, Amrish Kumar, Arun kumar Choudhary sir (Scientist, MNRE), Dr. Kamal Aggarwal with whom I used to have late night discussions. I would also like to thank all the mess staffs of Udaigiri House.

Last, but not the least, I would like to thank my mother, father, and my sister for showering continuous love, care, and support, without which none of the accomplishments would have been its worth. Words fail me while conveying my indebtedness to them. I am also indebted to my loving and caring wife for being my inspiration and motivation. Thank you for being my best friend. I would also like to express my deepest gratitude to my father-in-law and mother-in-law for being there when I needed them. Their continuous support and motivation always helped me to complete this journey smoothly.

Supriya Chakraborty

IIT Delhi, India

ABSTRACT

Emerging Non-Volatile Memory (NVM) technologies are significant contender for next generation memory applications including both standalone and embedded memory usage. In addition, there are significant advancements of the NVM technologies beyond storage applications. This includes in-memory computing, neuromorphic applications, security primitives, approximate computing, etc. Since emerging NVM technologies are used in main stream memory applications, it is high time to investigate their reliability aspects. With the advancement of modern electronic systems and integrated circuits, hardware security has become one of the crucial concerns. Hardware security threats may arise at any stage of the life cycle of the electronic systems/devices ranges from the device specifications to fabrication including recycling. In addition, data processing within the electronic system is also subject to various threats such as unauthorized access, side channel attack, fault injection, data corruption, DoS, etc.

In this dissertation we investigate two aspects of Commercial-Off-The-Shelf (COTS) NVM chips i) reliability, and ii) security. We show that the unique characteristics of NVM technologies can act as two sides of the same coin: i) one related to exploitation of vulnerabilities leading to threats and other ii) related to exploitation for building innovative hardware security primitives. The key contributions of this work include characterization of NVM chips for i) latency, ii) current consumption, and iii) endurance. Different soft techniques are experimentally validated on FPGA to enhance the performance of the chips beyond datasheet specifications. We significantly reduce the number of bit flips by $\sim 26\%$. The unique current consumption signature of the chips is further exploited for efficient NVM programming. The reliability aspect is investigated by exposing MRAM chips to the external magnetic field. Both static and dynamic stress analyses are performed while exposing the external magnetic field to the chip from different directions. We observed that exposure to external magnetic field results in increase in chip read and chip write current. Furthermore, the intrinsic properties of COTS NVM chips are exploited for hardware security applications including PUF, TRNG, and IC anti-counterfeiting. The proposed methodology leverages the latency and variability of COTS NVM chips for security primitives. The randomness

of the generated bitstream is evaluated using the industry standard NIST SP 800-22 statistical test suite, and all 15 tests are passed. The obtained results validate the reliability and robustness of the extracted TRNG. Utilization of the existing NVM chips and no requirement for additional specialized hardware makes the proposed technique highly advantageous and cost-effective. A dedicated dataset through experimental characterization is also developed for conventional and emerging NVM technologies to train the Machine Learning classifier to high accuracy for detecting IC origin.

सार

नॉन - वोलेटाइल मेमोरी (NVM) प्रौद्योगिकियां अगली पीढ़ी के लिए महत्वपूर्ण दावेदार हैं- स्टैंडअलोन और एम्बेडेड मेमोरी उपयोग दोनों सहित मेमोरी एप्लिकेशन। इसके साथ ही, भंडारण अनुप्रयोगों से परे NVM प्रौद्योगिकियों में महत्वपूर्ण प्रगति हुई है। इस में इन-मेमोरी कंप्यूटिंग, न्यूरोमॉर्फिक एप्लिकेशन, सुरक्षा आदिम, अनुमानित कॉम्प्यूटिंग, आदि। चूंकि उभरती NVM प्रौद्योगिकियों का उपयोग मेन स्ट्रीम मेमोरी अनुप्रयोगों में किया जाता है, यह उनके विश्वसनीयता पहलुओं की जांच करने के लिए उच्च समय है। आधुनिक इलेक्ट्रॉनिक प्रणाली और इंटीग्रेटेड सर्किट की उन्नति के साथ, हार्डवेयर सुरक्षा महत्वपूर्ण चिंताओं में से एक बन गई है। हार्डवेयर इलेक्ट्रॉनिक सिस्टम/उपकरणों के जीवन चक्र के किसी भी स्तर पर सुरक्षा संबंधी खतरे उत्पन्न हो सकते हैं। इसके अलावा, डेटा प्रसंस्करण के भीतर इलेक्ट्रॉनिक प्रणाली भी विभिन्न खतरों जैसे अनधिकृत पहुंच, साइड चैनल हमले, fault injection, डेटा भ्रष्टाचार, DoS इत्यादि के अधीन है।

इस निबंध में हम COTS NVM चिप्स के दो पहलुओं की जांच करते हैं i) विश्वसनीयता, और ii) सुरक्षा। हम दिखाते हैं कि NVM प्रौद्योगिकियों की अनूठी विशेषताएं कार्य कर सकती हैं एक ही सिक्के के दो पहलू के रूप में: i) एक खतरे की ओर ले जाने वाली कमजोरियों के शोषण से संबंधित है और अन्य ii) नवोन्मेषी हार्डवेयर सुरक्षा आदिमों के निर्माण से संबंधित। कुंजी इस कार्य के योगदान में i) latency, ii) current consumption, और iii) Endurance। डेटाशीट विनिर्देशों से परे चिप्स के प्रदर्शन को बढ़ाने के लिए विभिन्न सॉफ्ट तकनीकों को FPGA पर प्रयोगात्मक रूप से मान्य किया गया है। हम महत्वपूर्ण रूप से बिट फ्लिप की संख्या ~ 26% कम करते हैं। चिप्स का unique current consumption हस्ताक्षर आगे पूर्व है कुशल एनवीएम प्रोग्रामिंग के लिए उपयोग किया गया है। MRAM चिप्स को उजागर कर विश्वसनीयता पहलू की जांच के लिए बाहरी चुंबकीय क्षेत्र किया गया है। बाहरी चुंबकीय क्षेत्र को विभिन्न दिशाओं से चिप में उजागर करके स्थैतिक और गतिशील stress विश्लेषण दोनों का प्रदर्शन किया गया है। हमने देखा कि बाहरी चुंबकीय क्षेत्र के कारण चिप रीड और चिप राइट करंट में वृद्धि होती है। आगे, COTS NVM चिप्स के आंतरिक गुण हार्डवेयर सुरक्षा PUF, TRNG और आईसी विरोधी जालसाजी सहित अनुप्रयोगों के लिए उपयोग किए गए हैं। प्रस्तावित कार्यप्रणाली विलंबता का लाभ उठाती है और सुरक्षा आदिम के लिए COTS NVM चिप्स की परिवर्तनशीलता। उत्पन्न बिट स्ट्रीम की यादृच्छिकता का मूल्यांकन उद्योग मानक NIST SP 800-22 सांख्यिकीय परीक्षण सूट और सभी 15 परीक्षणों का उपयोग करके किया गया है। प्राप्त परिणाम निकाले गए TRNG की विश्वसनीयता और मजबूती को मान्य करते हैं। उती

मौजूदा NVM चिप्स का निर्माण और अतिरिक्त विशेष हार्डवेयर बनाने की कोई आवश्यकता नहीं है प्रस्तावित तकनीक अत्यधिक लाभप्रद और लागत प्रभावी है। पूर्व के माध्यम से एक समर्पित डेटासेट पारंपरिक और उभरती हुई एनवीएम प्रौद्योगिकियों के लिए परिधीय लक्षण वर्णन भी विकसित किया गया है। आईसी मूल का पता लगाने के लिए Machine Learning क्लासिफायर को उच्च सटीकता के लिए प्रशिक्षित किया गया है।

Contents

ACKNOWLEDGEMENTS	i
ABSTRACT	iii
LIST OF TABLES	xi
LIST OF FIGURES	xvii
ABBREVIATIONS	xviii
1 Introduction and Motivation	1
1.1 Introduction	1
1.2 Motivation	3
1.3 Thesis Contribution and Organization	6
Part : A. Reliability Investigation of COTS NVM Chips	
2 Background Concepts and Survey	8
2.1 Overview of Emerging NVM Technologies	8
2.1.1 NOR Flash	8
2.1.2 Conductive Bridging Random Access Memory	9
2.1.3 Resistive Random Access Memory	9
2.1.4 Ferroelectric Random Access Memory	10
2.1.5 Magnetoresistive Random Access Memory	11
2.2 Reliability Metrics	12
2.2.1 Variability	12

2.2.2	Endurance, Retention and Programming Error	12
2.3	Overview of COTS NVM Chip	13
2.4	Hardware Security Use Cases	13
2.4.1	Physically Unclonable Function	13
2.4.2	True Random Number Generator	17
2.4.3	IC Counterfeiting	18
2.4.4	Fault Injection Attack	19
2.5	Conclusion	19
3	Experimental Setup and Methodology	21
3.1	Experimental Setup	21
3.1.1	Experimental Setup for Magnetic Field Exposure to NVM Chips	22
3.2	Characterization Methodology	23
3.2.1	Latency Characterization	23
3.2.2	Current Characterization	24
3.2.3	Endurance Characterization	25
3.2.4	Temperature Effects Characterization	26
3.3	Conclusion	26
4	Performance Enhancement of Emerging NVM Technologies Using Soft Techniques	28
4.1	Advanced Performance Enhancement Soft-Techniques for Emerging Resistive Memory	28
4.1.1	Performance Enhancement Algorithms	28
4.2	Experimental Validation of NVM Performance Enhancement Using FNW Soft-Technique	31
4.2.1	Performance Enhancement Using FNW	33
4.3	Comparative Analysis Among Different Soft-Techniques for Performance Enhancement	37
4.3.1	Memory Overhead	39

4.3.2	Error Asymmetry	40
4.3.3	Cost Function	41
4.3.4	Overall Comparison	42
4.4	Current Characterization in NVM Technologies	44
4.4.1	Current Variation with Data Pattern	44
4.4.2	Current Variation with Aging	46
4.4.3	Current Optimized Coset Coding (CoCC)	46
4.4.4	Analysis and Experimental Validation of CoCC	50
4.4.5	Hardware Implementation	53
4.5	Conclusion	54
5	Investigation of NVM Chips Against Fault Injection Attack	55
5.1	Experimental Study of Adversarial Magnetic Field Exposure Attacks on Toggle MRAM Chips	55
5.1.1	Static Stress Analysis	56
5.1.2	Dynamic Stress Analysis	57
5.1.3	Results and Discussion	57
5.2	Conclusion	66
Part : B. Security Application of COTS NVM Chips		
6	Hardware Security Applications of NVM Technologies	67
6.1	High-Quality PUF Extraction using Switching-Time Variability	67
6.1.1	PUF Extraction Methodology	67
6.2	True Random Number Generation from Commodity NVM Chips	71
6.2.1	Methodology for TRNG Extraction	71
6.2.2	Random Bit Stream Generation	73
6.2.3	Randomness Analysis	76
6.2.4	Performance Analysis	77

6.2.5	Aging and Temperature Effects	79	
6.3	Exploiting Nanoelectronic Properties of Memory Chips for Prevention of IC-Counterfeiting	80	80
6.3.1	Characterization Results and Analysis	80	
6.3.2	Proposed Methodology of Detecting IC Manufacturer	82	
6.4	Conclusion	85	
7	Conclusion and Future Work	87	
7.1	Summary	87	
7.2	On-Going and Next Steps	88	
	BIBLIOGRAPHY	89	
A	Exploiting switching properties of non-volatile memory chips for data security applications	103	
A.1	Proposed cryptosystem architecture	103	
A.1.1	Procedure for extracting TRNG	104	
A.1.2	Methodology for data ciphering	106	
A.2	Experimental results and discussion	109	
A.3	Conclusions	114	
B	List of Publications from this Thesis	116	

List of Tables

2.1	Vulnerabilities in emerging NVM. Adapted from [64].	20
3.1	Specifications of characterization instruments used for this work.	27
4.1	Area and Power Overhead for Encoding and Decoding Scheme.	54
6.1	Comparative Analysis of Latency- and Mapping- based PUFs.	70
6.2	Analysis of obtained number of states and NIST SP 800-22 test result for Resistive NVM and NOR Flash.	74
6.3	Evaluation of Randomness for Resistive NVM Using NIST SP 800-22 Statistical Test Suite.	76
6.4	Evaluation of Randomness for NOR Flash Using NIST SP 800-22 Statistical Test Suite.	77
6.5	Comparative analysis of different off-the-shelf memory based TRNG.	79
6.6	Details of NVM chips used	82
6.7	Performance comparison of ML algorithms for IC prediction	84
6.8	Comparison of memory IC anti-counterfeiting techniques	85
A.1	Comparative analysis of generated random numbers from different NVM chips for 600K cycles. Vendor1 = CBRAM, Vendor2 = NOR Flash, and Vendor3 = ReRAM.	107
A.2	NIST Test Results for Different NVM technologies at Room Temperature (+25 °C). Vendor1 = CBRAM, Vendor2 = NOR Flash, and Vendor3 = ReRAM. . .	110
A.3	Comparative Study of COTS NVM chips based TRNG.	112
A.4	Comparison of Correlation Coefficient of Image Components for Original and Encrypted Image. Vendor1 = CBRAM, Vendor2 = NOR Flash, and Vendor3 = ReRAM.	115

List of Figures

1.1	Semiconductor component wise market growth prediction. (a) Source [14], and (b) Source [94].	2
1.2	Predicted growth trend of different memory technologies for upcoming years. Source [31]	2
1.3	Some key players for different emerging NVM technologies. Source [30]. . . .	3
1.4	Recent publications and citations trend obtained from the Web of Knowledge using the search keywords: keyword=(hardware security) OR keyword=(hardware vulnerability) OR keyword=(survey of hardware security) OR keyword=(hardware security circuits) OR keyword=(secure hardware system) OR keyword=(Attacks in CMOS technology) OR keyword=(non volatile memory attack OR keyword=(non volatile memory security) OR keyword=(emerging non volatile memory security) OR keyword=(attacks in emerging non volatile memory) for the years 2018-2022 (a) Publications, (b) Citations.	4
1.5	Different hardware security threats.	4
1.6	Application spectrum of emerging NVM technologies [32].	5
1.7	Overview of the contribution of the thesis.	6
2.1	Basic working principle of the NVM technologies used for the research activity.	9
2.2	(a) Current-Voltage characteristics of a bipolar switching device. The set transition from the high resistance state (HRS) to the low resistance state (LRS) occurs at positive voltage due to the formation of a filament shunting the top and bottom electrodes, while the reset transition from the LRS to the HRS under negative voltage indicates the disconnection of the voltage-induced filament. (b) Volatage-Polarization characteristics of FeRAM devices. Application of a voltage above the coercive voltage V_c leads to dipole reorientation with positive remnant polarization P_r . A negative voltage below $-V_c$ results in negative remnant polarization $-P_r$. (c) Resistance–Voltage characteristic of a spin transfer torque magnetic random access memory device. The parallel (P) and antiparallel (AP) states have low and high resistance, respectively, which can be attained at positive and negative voltage, respectively [56].	10
2.3	(a) Block diagram of internal architecture of NVM COTS chips, (b) Pin configuration of SPI NVM chips. Adapted from [98].	14

2.4	Block diagram of implementation of PUF. The response are mutually exclusive on applying similar challenges to different PUFs.	14
2.5	Fault injection attack in NVM technology.	19
3.1	Block diagram of our experimental setup for NVM characterization.	22
3.2	(a) Snapshot of our experimental setup for NVM characterization, (b) Custom designed PCB for NVM characterization test setup.	22
3.3	(a) Schematic diagram, (b) Image of the experimental hardware setup.	23
3.4	Block diagram of measuring program/erase latency in NVM technologies.	23
3.5	Block diagram of measuring current consumption during programming/read operations in NVM chip.	24
3.6	Temperature effect study setup (a) Vötsch temperature chamber (VCL 7003), (b) Zoomed display of temperature controller, (c)-(d) Temperature effect measurements setup at 85°C and -45°C. Courtesy: IC characterization Lab, IIT Delhi.	26
4.1	Nature of error distribution of (a) a page (64 bytes), and (b) a byte program for 200k cycles in CBRAM.	32
4.2	(a) Overlay of total page errors (Y1-axis, black marker) and page write-latency (Y2-axis, red marker), with cycling. (b) Distribution of type of bit-errors with byte address and cycling.	33
4.3	FNW Used: (a) Overlay of total page errors (Y1-axis, black marker) and page write-latency (Y2-axis, red marker), with cycling. (b) Distribution of type of bit-errors with byte address and cycling.	33
4.4	CBRAM chip, page write-current consumption for 500 consecutive random data-write cycles using FNW and no-FNW.	34
4.5	RBBER plot for FNW and no-FNW for 2×10^5 cycles of random data-write. Inset compares page write-latency for the two cases.	35
4.6	Ratio of Stuck at 0/Stuck at 1 errors for the FNW and no-FNW cases (random data write - 200k cycles).	36
4.7	Comparison of decrease in nature of bit errors by implementing FNW for error reduction.	37
4.8	Average page write latency distribution at different cycle number for different algorithms.	38

4.9	(a) Individual page write latency with linear fitting for different soft techniques. Slope of the fit denotes latency degradation parameter. (b) Distribution of latency degradation parameter for all algorithms.	38
4.10	Distribution of total bit-error count with cycling for (a) DCW, (b) FNW, (c) CC, and (d) CAFO.	39
4.11	RBER plot of DCW, FNW, CAFO, and CC for random data page write (200k cycles).	40
4.12	Distribution of ratio of Stuck at 0/Stuck at 1 errors for a) DCW, b) FNW, c) CC, and d) CAFO (random data write - 200k cycles) across a given page.	42
4.13	Comparison of cost reduction for all four algorithms and their cost-function versions, when CBRAM initial state is randomized between every two consecutive write cycles.	42
4.14	Comparison of cost reduction for all four algorithms and their cost-function versions, when CBRAM initial state is not randomized between two consecutive write cycles.	43
4.15	Radar plot of different soft techniques comparing trade off parameters for (a) 50k cycles, (c) 100k cycles, and (d) 200k cycles, random data write.	43
4.16	Variation of average page write current with increasing number of bits toggled for different NVM chips.	45
4.17	(a) Variation of page write current consumption with cycling in CBRAM. (b) Increasing pattern of write latency with cycling.	45
4.18	(a) Normalized current consumption for different order bit switching events during page write operation. For each type of bit switching, an alternating sequence of 250 data-write cycles and 250 reset cycles are used. Normalized mean current for all possible- (b) 28 combinations of 2-bit switching and, (c) 56 combinations of 3-bit switching events (each point = mean over 500 cycles are shown).	48
4.19	Normalized mean program current distribution for different bit switching events (page write). Each point shows the mean current and standard deviation over 3000 write cycles. All possible 256 combinations illustrate a combination invariant trend. Experiments were performed for initial all 1 page (blue) and initial all-zero page (red).	49
4.20	Flowchart of our proposed CoCC algorithm. (a) Encoding scheme (H_d = bit flip order with minimum current consumption, I_d = input current, a = coset base element address and has k bits, P_d = previously saved word, Y = encoded word, i = index). (b) Decoding scheme.	49

4.21	(a) Simulated probability distribution of occurrence of an encoding with a particular hamming distance at least once in a given cycle. (Coset base sizes= 8, 16, 32, 64, for 200k cycles). Simulated per-cycle probability distribution of encodings with (b) hamming distance = 1, (c) hamming distance = 2, and (d) hamming distance = 3 for coset base sizes = 8 and 64.	50
4.22	Experimental comparison of current with and without CoCC. CoCC was implemented for hamming distance = 2 and 3. (1 point = mean over 5000 cycles). . .	51
4.23	Circuit implementation of proposed CoCC algorithm. (a) Encoding scheme. Hamming distance between previously stored data, and the XOR-ed input data is computed using XOR gates and a full adder (FA). (b) Decoding scheme of the encoded data.	51
5.1	Applying magnetic field from different directions of the chip.	56
5.2	Variation of magnetic flux with distance for different dimension DC magnetic sources.	56
5.3	(a) Chip write and chip read current measurement of 1Mb MRAM chip, and (b) Statistics of chip write and chip read current for different capacity MRAM chips in ambient condition. Statistics for each memory capacity is calculated on 5-7 different chips by performing 20 read/write cycles in each chip.	58
5.4	Statistics of chip read current for different capacity MRAM chips: before-during- and after static stress test on applying $B_{external}$ from different directions (case1-5). (External magnetic field = ~ 700 Gauss at 2 cm).	59
5.5	Statistics of chip write and read current for different capacity MRAM chips: before-during- and after dynamic stress test on applying $B_{external} = \sim 700$ Gauss at 2 cm from different directions (case1-5). Solid filled legends indicate chip read current and open filled legends indicate chip write current.	60
5.6	Total data corruption occurred (%) during data storage for different capacity MRAM chips with increasing exposure time. The inset shows the sequence of applied magnetic field signal for case1. (External magnetic field = ~ 700 Gauss, distance = 2 cm.)	61
5.7	Total data corruption occurred (%) during static stress test (chip-to-chip variability) for different capacity MRAM chips with increasing exposure time. The inset shows the sequence of applied magnetic field signal with increasing exposure time. (External magnetic field = ~ 700 Gauss, distance = 2 cm). Difference in exposure time for different memory chips is applied as each capacity of MRAM chip requires different time interval for chip read operation.	63
5.8	Total data corruption occurred (%) during static stress test for different capacity MRAM chips with different exposure angles. (External magnetic field = ~ 700 Gauss, distance = 2 cm). Applied sequence of magnetic field signal is shown in inset of Figure 5.7.	64

5.9	Total data corruption occurred (%) during dynamic stress test (chip-to-chip variability) for different capacity MRAM chips with increasing exposure time. The inset shows the applied magnetic field signal with increasing exposure time. (External magnetic field = ~ 700 Gauss, distance = 2 cm). Difference in exposure time for different memory chips is applied as each capacity of MRAM chip requires different time intervals for chip write and read operation.	65
5.10	Total data corruption occurred (%) during dynamic stress test for different capacity MRAM chips with different exposure angles. (External magnetic field = ~ 700 Gauss, distance = 2 cm). Applied sequence of magnetic field signal is shown in inset of Figure 5.9.	65
6.1	Distribution of write latency for 256 byte virtual page for: (a) four different challenges applied over 100k cycles, and (b) single challenge applied over 25k cycles.	68
6.2	Proposed RRAM latency based PUF extraction strategy.	69
6.3	Distribution of inter-hamming distance of the proposed 24-bit PUF for 25k cycles for four different chips.	69
6.4	Distribution of intra-hamming distance of the proposed 24-bit PUF for 25k cycles.	70
6.5	(a) Repetition of Inter-hamming distance experiments for the proposed 24-bit PUF. (Multiple different CRPs performed at 5 different sets of page locations, on 4 different ICs for different switching event types). (b) Repetition of Intra-hamming distance experiments. (each red square in both (a) and (b) = 25k cycles. (Inset: Blue squares denote RRAM chip, yellow rectangles denote tentative page locations used for L1 and L2 in a particular iteration.)	71
6.6	Distribution of uniformity of '1's for 24-bit PUF.	72
6.7	Flow chart of the proposed generalised methodology to generate high-quality TRNs from different NVM technologies. $W_{modified}$ denotes the modified write or erase latency value for the NVM technology.	72
6.8	Distribution of generated bits for specific data write in resistive NVM (a) raw data, (b) flipped data, (c) XOR-ed data, and (d) quantized (output) data.	74
6.9	Probability density function of the generated random numbers for 650k cycles from (a) Resistive NVM and (b) NOR Flash. (Flatten the histogram, better is the quality.)	74
6.10	Distribution of the count of occurrences of distinct states (for 650k cycles) (a) before, and (b) after implementation of the post-processing for resistive NVM. (c) before, and (d) after implementation of the post-processing for NOR Flash.	75
6.11	Bitmap image (3224 $\times$ 3225) of the obtained stream of random bits from (a) Resistive NVM and (b) NOR Flash. Black and white colour corresponds to bit '0' and bit '1' respectively. Almost equal number of '1s' and '0s' are observed.	78

6.12	Analysis of aging and temperature effect of NVM devices on randomness of the generated TRNs from (a) Resistive NVM, (b) NOR Flash.	78
6.13	(a)-(d) Evolution of sector erase/page write latencies over cycling (50k cycles) for various NVM chips. Distinct evolution in latency values is observed for different NVM technologies and manufacturers.	81
6.14	Statistics of latency values obtained within a span of 50 cycles before and after 1k, 6k, 16k and 36k cycles. Each point = 2 chips with 5 random locations in each chip (1k samples).	82
6.15	Test confusion matrix for KNN classifier. TPR = True Positive Rates, FNR = False Negative Rates.	84
6.16	Spatial latency map of full chip including all addresses for (a) CBRAM, (b) RRAM and (c) NOR Flash. Random locations are selected in a fresh chip and are programmed/erased continuously to generate used locations artificially. Dotted circles show such used locations in the NVM chips. (d) Zoomed view of used and unused individual locations for a NOR Flash chip.	85
A.1	Block diagram of (a) proposed cryptosystem, and (b) implemented IP blocks in FPGA.	104
A.2	Flow chart of the proposed algorithm for generating TRNs from NVM.	104
A.3	Generation of random bits from CBRAM (a) before and (b) after post-processing technique for 1000 cycles.	105
A.4	Flowchart of image (a) encryption and (b) decryption using generated stream of random bits. The $\oplus$ is bit-wise Exclusive-OR (XOR) operation.	105
A.5	Evolution of page write and sector erase latency and the post-processed data with cycling of different NVM technologies. Vendor1 = CBRAM, Vendor2 = NOR Flash, and Vendor3 = ReRAM.	109
A.6	Analysis for image encryption and decryption.	113
A.7	Differential attack for 10 randomly selecting red channel pixels. Nearly similar values are obtained for other channels (green and blue) of the image. Vendor1 = CBRAM, Vendor2 = NOR Flash, and Vendor3 = ReRAM.	114
A.8	Key sensitivity analysis for 10 randomly selecting keys for encrypting red channel. Nearly similar values are obtained for other channels (green and blue) of the image. Vendor1 = CBRAM, Vendor2 = NOR Flash, and Vendor3 = ReRAM.	114

ABBREVIATIONS

ASIC	Application Specific Integrated Circuit
AXI	Advanced eXtensible Interface
BL	Bit Line
C2C	Chip-to-Chip
CAGR	Compound Annual Growth Rate
CAFO	Cost Aware Flip Optimization
CBRAM	Conductive Bridging Random Access Memory
CC	Coset Coding
CF	Conductive Filament
CG	Control Gate
CHE	Channel-Hot Electron
CMOS	Complementary Metal-Oxide Semiconductor
COCC	Current Optimized Coset Coding
COTS	Commercial-Off-The-Shelf
CRP	Challenge Response Pair
CS	Chip Select
D2D	Device-to-Device
DCW	Data Compare Write
DDR	Double Data Rate
DFN	Dual-Flat No-Leads
DoS	Denial-of-Service
DRAM	Dynamic Random Access Memory
FeRAM	Ferroelectric Random Access Memory
FG	Floating Gate
FI	Fault Injection
FL	Free Layer

FN	Fowler–Nordheim
FNW	Flip-N-Write
FPGA	Field Programming Gate Array
HD	Hamming Distance
HDL	Hardware Description Language
HRS	High Resistive State
I2C	Inter-Integrated Circuit
IC	Integrated Circuit
IoT	Internet of Things
IP	Intellectual Property
JTAG	Joint Test Action Group
LRS	Low Resistive State
MIM	Metal-Insulator-Metal
ML	Machine Learning
MOS	Metal-Oxide Semiconductor
MRAM	Magneto-resistive Random Access Memory
MTJ	Magnetic Tunnel Junction
NIST	National Institute of Standards and Technology
NN	Neural Network
NVM	Non-Volatile Memory
ONO	Oxide-Nitride-Oxide
OTP	One Time Padding
PCB	Printed Circuit Board
PCM	Phase Change Memory
PL	Pinned Layer
PRNG	Pseudo Random Number Generator
PUF	Physically Unclonable Functions
PV	Program-Verify
RBER	Raw-Bit Error Rate
ReRAM	Resistive Random Access Memory
RNG	Random Number Generator
RO	Ring Oscillator

RTN	Random Telegraphic Noise
SAF	Synthetic Anti-Ferromagnetic
SL	Source Line
SMU	Source Measurement Unit
SoC	System on Chip
SOIC	Small Outline Integrated Circuit
SOP	Small Outline Package
SPI	Serial Peripheral Interface
SRAM	Static Random Access Memory
STT	Spin-Transfer Torque
TCAM	Ternary Content Addressable Memory
TO	Tunnel Oxide
TRNG	True Random Number Generator
UART	Universal Asynchronous Receiver/Transmitter
USB	Universal Serial Bus
VFI	Voltage Fault Injection
WIP	Write-In-Progress
WL	Word Line
WvW	Write-Verify-Write