INVESTIGATION OF COTS NVM TECHNOLOGIES FROM A RELIABILITY AND SECURITY PERSPECTIVE

SUPRIYA CHAKRABORTY

DEPARTMENT OF ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY DELHI

JUNE 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 ऽस्त्वकर्मणि ॥ 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 हक़दार 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 Neuromorphic 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 कॉमपुटिंग, 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 फ़्लिप 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 गया है। 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

List of Tables

List of Figures

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