M Sazadur Rahman

Phone: +1 (352) 213 - 7297 Email: mohammad.rahman@ufl.edu

ABOUT ME

I earned my Ph.D. from the Department of Electrical and Computer Engineering, University of Florida on development and usage of CAD tools in hardware security. I developed mathematically secure intellectual property (IP) protection and authentication methods with quantifiable security metrics. I possess industrial experience on ASIC design flow of cutting-edge semiconductor technologies.

Research Interest

Cybersecurity, IC design, ML guided computer-aided design, VLSI, hardware and software security

EDUCATION

December 2022	**Ph.D. in Electrical and Computer Engineering** **University of Florida, Gainesville, FL, USA** **Advisor:** Prof. Mark Tehranipoor, Chair, ECE, UF **Thesis:** Hardware Security Assurance via Obfuscation and Authentication
August 2022	**Master of Science in Electrical and Computer Engineering** **University of Florida, Gainesville, FL, USA**
March 2009 – July 2014	**Bachelor of Science in Electrical and Electronic Engineering** **Bangladesh University of Engineering and Technology** **Advisor:** Prof. Nasim Ahmed Dewan **Thesis:** Ion Energy Distribution of Multi-frequency Capacitively Plasma

RESEARCH AND WORK EXPERIENCE

Jan 2023 -	**Security Assurance Architect** **Intel Product Assurance and Security Team, Intel Corporation, USA** Working for architectural security hardening of Intel IPs against unauthorized access, microarchitectural, telemetry, and power side-channel vulnerabilities
Spring 2018 – Fall 2022	**Graduate Research Assistant** Florida Institute for Cybersecurity Research, Gainesville, FL, USA Worked in IP protection and authentication team to develop quantifiable and AI assured countermeasures against semiconductor supply chain threats
Summer 2021	**Security Researcher Intern** **Intel Corporation** Developed automated threat models review tool utilizing CWE, CVE, and CAPEC lists from mitre.org for nine different adversary models
Spring 2020	**Hardware Security Intern** **Intel Corporation, Hillsboro, Oregon** Developed firmware for FIPS 140 -3 security certification of cryptographic hardware using NIST Cryptographic Algo. Verification Program (CAVP)
Sept 2014 – Dec 2017	**Senior ASIC Design Engineer** **PrimeSilicon Technologies Ltd. And Neural Semiconductor Ltd.** Worked as implementation and verification engineer for tape out of 14nm and 28nm custom silicon using commercial EDA tools

HONORS & AWARDS

1. 2022 IEEE/ACM DAC, DATE, and HOST PhD Forum Best doctoral dissertation competition finalist
2. 2022 IEEE VTS TTTC's E. J. McCluskey Best Doctoral Thesis Competition – Runner up
3. 2023 IEEE/ACM Design Automation and Test in Europe (DATE) Best Paper Award Nomination
4. 2023 IEEE/ACM DATE PhD Forum Best doctoral dissertation competition finalist
5. 2022-23 IEEE Hardware Oriented Security and test doctoral dissertation competition finalist

Research Projects

DOSC [1]	Developed dynamically obfuscated scan chain architecture to ensure IP protection against untrusted parties in the supply chain. Performed mathematical modeling of the proposed countermeasure along with comprehensive experimental validation.
O'Clock [2]	Developed an automated clock-gating-based logic locking to protect IPs in complex SoCs. O'Clock obstructs data/control flows and makes the underlying logic dysfunctional for incorrect keys by manipulating the activity factor of the clock tree.
ReTrustFSM [3]	Architected a register-transfer (RT) level FSM obfuscation technique at the earliest stage using explicit external secrecy via an external key, implicit external secrecy based on specific clock cycles, and internal secrecy through a concealed FSM.
Security Metrics [4]	We examine the quantitative and qualitative metrics for logic locking. Then, by establishing a bridge between metrics and the potential methods, we introduce a compound-style logic locking that can meet the criteria needed for logic locking.
EvoLUTe [5]	Introduced a fine-grained redaction methodology using reconfigurable components (look-up-tables). Examine both eFPGA-based and LUT-based design, demonstrating that a novel cone-based and fine-grained universal function modeling approach using LUTs can provide the same degree of resiliency at a much lower overhead.
LL-ATPG [6]	Developed algorithm for logic-locking aware test method applying a set of valet keys based on a target coverage to perform manufacturing test in an untrusted environment. LL-ATPG achieves high test coverage and minimizes test time overhead.
ActiWate [7]	ACtiWate is an automatic self-verification protocol that communicates with various peripherals within the SoC. ActiWate is architectured to be an IP/SoC-agnostic watermark for RISC-V and ARM-based SoCs with different components/peripherals.
CAPEC [14], PSWise [16], EM-SC [17]	Developed IP-level watermarking solutions using different design features and side-channel characteristics. CAPEC implements cellular automata guided FSM watermarking. PSWise and EM-SC extracts power and EM side-channel characteristics of the underlying IP as a signature to detect IP usage in an SoC out of contract.

TEACHING AND RELATED EXPERIENCES

Teaching Assistant	**Introduction to Hardware Security and Trust, Dept. of ECE, Spring, 2019** **Responsibilities:** preparing lecture slides, delivering lectures, designing homework assignments, project, and questions for exam, holding student hours, invigilating during exams, and grading exam copies and assignments [lecture video]
Course Content	Designed EEE458 (VLSI) Cadence sessional course outline for Dept. of EEE, BUET
Instructor	Security and Privacy in IoT Era, UF CPET Program [course outline]

PROFESSIONAL SERVICES

Reviewer	IEEE Transaction on Computer Aided Design, IEEE Transactions on Computers IEEE VLSI Test Symposium, IEEE International Test Conference ACM Transactions on Design Automation of Electronic Systems ACM Hardware and System Security, Springer Nature Computer Science ACM Journal on Emerging Technologies in Computing Systems ACM Design Automation Conference, IEEE Hardware Oriented Security and Trust
Instructor	Micro-electronics Security Training Center – M6. SoC Design, M5. Logic locking
Ph.D. Mentor	Mentored ten Ph.D. students for Ph.D. student mentorship program
Organizer	UF/FICS Hardware De-obfuscation Competition.
Instructor	IEEE Young professional workshop on RTL to GDS signoff of an ASIC chip, 2017

Technical Skills

- *Hardware Description Languages:* SystemVerilog (assertion), Verilog, VHDL
- *Scripting:* Tcl-tk, Perl, Linux/Unix Shell (bash, csh, tcsh, awk, grep, sed)
- *Programming Languages:* C, C++, Python, MATLAB, Assembly language
- *Hardware Verification:* JasperGold, SPV, IFV, Model checking, SAT solvers
- *Machine Learning:* TensorFlow, Keras packages
- *Design & Simulation Tools:* Synopsys Design Compiler, DFT Compiler, VCS, TetraMAX, Formality, IC Compiler-II, PrimeTime, IC validator, PrimeRail, PrimePower, Cadence Genus**,** NCSim, Conformal LEC**,** Innovus, Tempus**,** PVS, QRC, Voltus**,** Tessent EDT, Mentor Graphics - Calibre
- *FPGA Design:* Vivado, Quartus, ModelSim

SELECTED TALKS

a. "Protecting Intellectual Property Cores against Piracy using Dynamically Obfuscated Scan Chain Architecture", Trusted and Assured Microelectronics (TAME) Forum, Gainesville, FL, 2019.
b. "Protecting Obfuscated Circuits against Attacks that Utilize Test Infrastructure", FICS Research
c. 2021 Technology Demonstration Conference (TDC), Gainesville, FL 2021.
d. "SoC Security Tool Chain", ACM Design Automation Conference, San Francisco, CA, 2022.

PATENTS

a. Tehranipoor, Mark M., …, and M Sazadur Rahman, "Protecting Obfuscated Circuits against Attacks that Utilize Test Infrastructures", U.S. Patent No. 16/535,795 (Issued).
b. Tehranipoor, Mark M., …, and M Sazadur Rahman, "Integrated Circuit Obfuscation by Stripped Functionality Based Decoy Clock Gates" (under construction)

BOOK AND BOOK CHAPTERS

a. Farimah Farahmandi, **M Sazadur Rahman**, Sree Ranjendaran, Mark M Tehranipoor. "CAD for Hardware Security." Springer, April 2023.
b. Asadizanjani, Navid, Mir Tanjidur Rahman, and Mark Tehranipoor. "Physical Assurance" Cham Switzerland: Springer Nature Switzerland AG (2021) (Chapter 1).
c. Bhunia, Swarup, and Mark Tehranipoor, "Hardware security: a hands-on learning approach", Morgan Kaufmann, 2018 (Chapter 6).

CONFERENCE PUBLICATIONS AND JOURNALS

1. **M Sazadur Rahman**, et. al., "Security Assessment of Dynamically Obfuscated Scan Chain Against Oracle-guided Attacks", ACM TODAES, vol. 26.4 (2021), pages 1-27. [demonstration]
2. **M Sazadur Rahman**, et. al., "O'Clock: Lock the Clock via Clock-gating for SoC IP Protection", ACM Design Automation Conference (DAC), 2022. [presentation]
3. **M Sazadur Rahman**, et al., "ReTrustFSM: Towards Register Transfer Level Hardware Obfuscation - A Hybrid FSM Approach", IEEE Access 2023 (under review).
4. Rui Guo*, **M Sazadur Rahman***, et al., "EvoLUTe: Evaluation of Look-Up-Table-based Fine-Grained IP Redaction", ACM Design Automation and Test in Europe (DATE), 2023.
5. **M Sazadur Rahman**, et al. "LL-ATPG: Logic-Locking Aware Test Using Valet Keys in an Untrusted Environment." *2021 IEEE International Test Conference (ITC)*. IEEE, 2021. [presentation]
6. Zahin Ibnat, **M Sazadur Rahman**, et al., "ActiWate: Adaptive and Design-agnostic Active Watermarking for IP Ownership in Modern SoCs", 60th ACM Design Automation Conference (DAC).
7. M Tanjidur Rahman, Shahin Tajik, **M Sazadur Rahman**, et. al., "The Key is Left under the Mat: On the Inappropriate Security Assumption of Logic Locking Schemes", HOST 2020.
8. Md Rafid Muttaki, Shuvagata Shaha, **M Sazadur Rahman**, et al., "RTLock: IP Protection using Scan-Aware Logic Locking at RTL", ACM Design Automation and Test in Europe (DATE), 2023.
9. M Tanjidur Rahman, **M Sazadur Rahman**, et. al., "Defense-in-Depth: A Recipe for Logic Locking to Prevail", IEEE Integration 72, 39-57.
10. N. Nalla Anandakumar, **M Sazadur Rahman**, et al. "Rethinking Watermark: Providing Proof of IP Ownership in Modern SoCs." Cryptology ePrint Archive (2022)
11. Minyan Gao, **M Sazadur Rahman**, et. al., "iPROBE: Internal Shielding Approach for Protecting Against Front-side and Back-side Probing Attacks", IEEE Transactions on Computer Aided Design, 2023.

12. Mashahedur Rahman, **M Sazadur Rahman**, et. al., "CAPEC: A Cellular Automata Guided FSM-based IP Authentication Scheme", IEEE VTS 2023.
13. Upoma Das, **M Sazadur Rahman**, et. al., "PSWise: Power Side Channel Based IP Watermarking Using Clock Gates", 28th IEEE European Test Synopsium, 2023.
14. Upoma Das, **M Sazadur Rahman**, et. al., "Electromagnetic Side Channel-based IP Watermark Verification on SOC without Physical Access", 28th IEEE European Test Synopsium, 2023.
15. Rasheed Kibria, **M Sazadur Rahman**, et. al., "RTL-FSMx: Fast and Accurate Finite State Machine Extraction at the RTL for Security Applications", 2022 IEEE International Test Conference (ITC).
16. **M Sazadur Rahman**, et al., "Metrics-to-Methods: Decisive Reverse Engineering Metrics for Resilient Logic Locking", 60th ACM Design Automation Conference (DAC) (poster presentation).
17. **Rahman, M. Sazadur**, et al., "Insider Threat: Emerging Vulnerabilities in Semiconductor Supply Chain", IEEE Design and Test, 2023 (under construction)
18. **M Sazadur Rahman**, et al., "Stripped Functionality Based Decoy Clock-gating for SoC IP Protection", IEEE Transactions on Computer Aided Design, 2023 (under construction)
19. Ahmed Bulbul, **M Sazadur Rahman**, et. al., "A Graph based Security Estimation for Logic Locking", ACM Conference on Computer and Communications Security (CCS), 2023 (under construction).

Funding Proposal Writing Experiences

- *Automated Implementation of Secure Silicon (AISS):* This three-year term project aims to ease the burden of developing secure chips. AISS seeks to create a novel, automated chip design flow that will allow security mechanisms to scale consistently with the goals of a chip design. Funded by DARPA.
  Contribution: Helped writing drafts of the primary investigators describing the proposed solution.
- *Intellectual Property Protection:* This four-year project establishes trust among different entities in the semiconductor fabrication and test flow by eliminating the threat of reverse engineering attacks on obfuscated deigns and provides a mathematical proof of security. Funded by DARPA.
  Contribution: Helped developing research plan and proposal drafts for the primary investigators.
- *SoC IP Protection:* This project aims to offer register transfer (RT) level locking by obfuscating the finite state machine to obscure the IP cores at a higher level of abstraction at the preliminary stage of the design process. Submitted to Cisco.
  Contribution: Helped developing investigation plan and proposal drafts for primary investigators.

REFERENCES

Mark M. Tehranipoor, Ph.D., Fellow of IEEE/ACM
Chair, Dept. of Electrical and Computer Engineering, https://www.ece.ufl.edu/
Intel Charles E. Young Preeminence Endowed Chair Professor in Cybersecurity
Co-director, AFOSR/AFRL Center of Excellence, CYAN
Co-director, MEST Center, https://mestcenter.org
University of Florida, Gainesville, FL 32611
Email: tehranipoor@ece.ufl.edu
Phone: +1-(352)-292-2585

Domenic Forte, Ph.D.
Associate Professor, Dept. of Electrical and Computer Engineering
Associate Director, Florida Institute for National Security (FINS)
University of Florida, Gainesville, FL 32611
Email: dforte@ece.ufl.edu
Phone: +1-(352)-392-1525

Farimah Farahmandi, Ph.D.
Assistant Professor, Dept. of Electrical and Computer Engineering
Associate Director, Florida Institute for Cybersecurity (FICS) Research
Associate Director, Edaptive Computing Inc. (ECI) Transition Center (ECI-TC)
University of Florida, Gainesville, FL 32611
Email: farimah@ECE.UFL.EDU
Phone: +1-(352)-392-0910