

MICHAEL ZUZAK

Assistant Professor, Department of Computer Engineering ◇ Rochester Institute of Technology

mjzeec@rit.edu ◇ mzuzak.github.io ◇ (585) 475-2312

ACADEMIC APPOINTMENTS

Assistant Professor, Department of Computer Engineering
Rochester Institute of Technology

August 2022 - Present

- Research Interests: Hardware Security, Digital VLSI/CAD, Computer Architecture

EDUCATION

Ph.D., Electrical Engineering
University of Maryland, College Park

August 2017 - August 2022

- ARCS/MWC Named Graduate Scholar, Future Faculty Fellow
- Advisor: Prof. Ankur Srivastava
- Thesis: Designing Effective Logic Obfuscation: Exploring Beyond Gate-Level Boundaries

M.S., Electrical Engineering
University of Maryland, College Park

August 2014 - May 2016

- Advisor: Prof. Donald Yeung
- Thesis: Exploiting Multigrain Parallelism on Heterogeneous Processors

B.S., Electrical Engineering (Cum Laude)
University of Maryland, College Park

August 2010 - May 2014

- University of Maryland Honors College, University Honors Citation

RESEARCH EXPERIENCE

University of Maryland, College Park
Graduate Research Assistant with Prof. Ankur Srivastava

August 2017 - August 2022

- Research Area: Hardware Security - Protecting integrated circuits from hardware trojans, piracy, and reverse engineering

Naval Research Laboratory, Surface Electronic Warfare Systems Branch
Electronics Engineer (Full-Time)

August 2015 - June 2018

- Research Area: Digital Signal Processing - Wide-band, high-speed digital signal processing for digital RF memories
- Primary contributor of digital design and digital signal processing capabilities for currently fielded urgent operational needs (UON) system for U.S. Navy

University of Maryland, College Park
Graduate Researcher with Prof. Donald Yeung

August 2014 - May 2016

- Research Area: Computer Architecture - Novel execution models for heterogeneous systems

PROJECT SPONSORS AND GRANTS

Total as PI/Co-PI: \$521,466

- [G4] NSF: "EAGER: Towards Crowd-Sourced Artifact Curation for Cyberattacks through a Learner-Centered AI Co-Pilot," 06/01/2024 - 05/31/2026, **Role: Lead PI**
- [G3] Eaton Corporation: "Hardware Anomaly and Zero-Day Detection in Resource-Constrained Microcontrollers Using Software Property Enforcement," 06/29/2023 - 06/28/2024, **Role: Sole-PI**
- [G2] NSF: "CRII: SaTC: Design Space Modeling for Logic Obfuscation to Enable System-Wide Security during IC Manufacture and Test," 03/15/2023 - 03/14/2025, **Role: Sole-PI**
- [G1] KEEN: "Improving Student Understanding of Non-Ideal Transistors," **Role: Sole-PI**

PUBLICATIONS

Journals:

- [J7] I. McDaniel, **M. Zuzak**, and A. Srivastava, "Removal of SAT-Hard Instances in Logic Obfuscation Through Inference of Functionality," in *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 2024
- [J6] **M. Zuzak**, Y. Liu, and A. Srivastava, "Security-Aware Resource Binding to Enhance Logic Obfuscation," in *IEEE Trans. on Computer Aided Design of Integrated Circuits and Systems (TCAD)*, 2023
- [J5] **M. Zuzak**, Y. Liu, and A. Srivastava, "Evaluating the Security of Logic-Locked Probabilistic Circuits," in *IEEE Trans. on Computer Aided Design of Integrated Circuits and Systems (TCAD)*, 2021
- [J4] Y. Liu, **M. Zuzak**, Y. Xie, A. Chakraborty, A. Srivastava, "Robust and Attack Resilient Logic Locking with a High Application-Level Impact," in *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 2021
- [J3] **M. Zuzak**, Y. Liu, and A. Srivastava, "Trace Logic Locking: Improving the Parametric Space of Logic Locking," in *IEEE Trans. on Computer Aided Design of Integrated Circuits and Systems (TCAD)*, 2020
- [J2] A. Chakraborty, N. Jayasankaran, Y. Liu, J. Rajendran, O. Sinanoglu, A. Srivastava, Y. Xie, M. Yasin, and **M. Zuzak**, "Keynote: A Disquisition on Logic Locking," in *IEEE Trans. on Computer Aided Design of Integrated Circuits and Systems (TCAD)*, 2019
- [J1] D. Gerzhoy, X. Sun, **M. Zuzak**, and D. Yeung, "Exploiting Nested MIMD-SIMD Parallelism on Heterogeneous Microprocessors," in *ACM Transactions on Architecture and Code Optimization (TACO)*, 2019

Conferences:

- [C20] L. Lam, M. Melnyk, and **M. Zuzak**, "Low Overhead Logic Locking for System-Level Security: A Design Space Modeling Approach," in *Proceedings of the ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED)*, 2024 (**Accepted**)
- [C19] K. Nakano, **M. Zuzak**, C. Merkel, A. Loui "Trustworthy and Robust Machine Learning for Multimedia: Challenges and Perspectives," in *Proceedings of the IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*, 2024 (**Accepted**)
- [C18] Z. Cheng, H. Choi, S. Feng, J. Liang, G. Tao, D. Liu, **M. Zuzak**, and X. Zhang, "Fusion is Not Enough: Single Modal Attack on Fusion Models for 3D Object Detection," in *Proceedings of the International Conference on Learning Representations (ICLR)*, 2024
- [C17] K. Nakano, M. Nakazawa, and **M. Zuzak**, "Complementing Vehicle Trajectories Using Two Camera Viewpoints," in *Proceedings of the IEEE Conference on Consumer Electronics (ICCE)*, 2024
- [C16] H. Xu, D. Liu, C. Merkel, and **M. Zuzak**, "Exploiting Logic Locking for a Neural Trojan Attack on Machine Learning Accelerators," in *Proceedings of the Great Lakes Symposium on VLSI (GLSVLSI)*, 2023
- [C15] D. Xing, **M. Zuzak**, and A. Srivastava, "Low Overhead System-Level Obfuscation through Hardware Resource Sharing," in *Proceedings of the International Symposium on Quality Electronic Design (ISQED)*, 2023
- [C14] I. McDaniel, **M. Zuzak**, and A. Srivastava, "A Linear-Time Structural Attack on SAT-Hard Instances in Logic Obfuscation," in *Proceedings of the International Conference on Computer Design (ICCD)*, 2022
- [C13] **M. Zuzak**, Y. Liu, I. McDaniel, and A. Srivastava, "A Combined Logical and Physical Attack on Logic Obfuscation," in *Proceedings of the ACM/IEEE International Conference on Computer-Aided Design (ICCAD)*, 2022
- [C12] I. McDaniel, **M. Zuzak**, and A. Srivastava, "A Black-Box Sensitization Attack on SAT-Hard Instances in Logic Obfuscation," in *Proceedings of the IEEE International Conference on Computer Design (ICCD)*, 2022
- [C11] Y. Liu, **M. Zuzak**, D. Xing, I. McDaniel, P. Mittu, O. Ozbay, A. Akib, and A. Srivastava, "A Survey on Side-Channel-based Reverse Engineering Attacks on Deep Neural Networks," in *Proceedings of the IEEE International Conference on Artificial Intelligence Circuits and Systems (AICAS)*, 2022
- [C10] **M. Zuzak**, Y. Liu, and A. Srivastava, "A Resource Binding Approach to Logic Obfuscation," in *Proceedings of the Design Automation Conference (DAC)*, 2021 (**Best Paper Candidate**)
- [C9] B. Tan, S. Garg, R. Karri, Y. Liu, **M. Zuzak**, ..., W. Savage, "Independent Verification and Validation of Security-Aware EDA Tools and IP," in *Proceedings of the Design Automation Conference (DAC)*, 2021
- [C8] **M. Zuzak** and A. Srivastava, "ObfusGEM: Enhancing Processor Design Obfuscation Through Security-Aware On-Chip Memory and Data Path Design," in *Proceedings of the International Symposium on Memory Systems (MEMSYS)*, 2020
- [C7] A. Mondal, **M. Zuzak**, and A. Srivastava, "StatSAT: A Boolean Satisfiability Attack on Logic Locking for Probabilistic Circuits," in *Proceedings of the Design Automation Conference (DAC)*, 2020
- [C6] Y. Liu, **M. Zuzak** and A. Srivastava, "Strong Anti-SAT: Secure and Effective Logic Locking," in *Proceedings of the International Symposium on Quality Electronic Design (ISQED)*, 2020

- [C5] Y. Liu, A. Mondal, A. Chakraborty, **M. Zuzak**, N. Jacobson, D. Xing, and A. Srivastava, "A Survey on Neural Trojans," in Proceedings of the International Symposium on Quality Electronic Design (ISQED), 2020
- [C4] **M. Zuzak**, M. Fitelson, S. Montano, and A. Srivastava, "Provable Detection and Location of Hardware Trojans with Linear Hybrid Cellular Automata," in Proceedings of the Government Microcircuit Applications and Critical Technology Conference (GOMACTECH), 2020
- [C3] **M. Zuzak** and A. Srivastava, "Memory Locking: An Automated Approach to Processor Design Obfuscation," in Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2019
- [C2] Z. Yang, **M. Zuzak**, and A. Srivastava, "HMCTherm: A Cycle-accurate HMC Simulator Integrated with Detailed Power and Thermal Simulation," in Proceedings of the International Symposium on Memory Systems (MEMSYS), 2018
- [C1] **M. Zuzak** and D. Yeung, "Exploiting Multi-Loop Parallelism on Heterogeneous Microprocessors," in Proceedings of the International Workshop on Programmability and Architectures for Heterogeneous Multicores (MULTIPROG), 2017 (**Awarded Best Paper**)

Book Chapters:

- [B1] Y. Liu, A. Mondal, A. Chakraborty, **M. Zuzak**, N. Jacobson, D. Xing, and A. Srivastava, "Neural Trojans," in Encyclopedia of Cryptography, Security and Privacy, 2021

Technical Reports:

- [T3] **M. Zuzak**, "Designing Effective Logic Obfuscation: Exploring Beyond Gate-Level Boundaries" (**Ph.D. Thesis**)
- [T2] B. Tan, R. Karri, N. Limaye, A. Sengupta, ..., **M. Zuzak**, A. Srivastava, et al., "Benchmarking at the Frontier of Hardware Security: Lessons from Logic Locking," in arXiv preprint arXiv:2006.06806, 2021
- [T1] **M. Zuzak**, "Exploiting Nested Parallelism on Heterogeneous Processors" (**M.S. Thesis**)

INVITED TALKS/POSTER PRESENTATIONS

- [P8] **M. Zuzak**, "Designing Obfuscated ICs for System-Wide Security during IC Manufacture and Test," Great Lakes Security Day (GLSD), 2023
- [P7] **M. Zuzak**, "Hardware: The Foundation of Security," at Electrical and Computer Engineering Research Seminar, Rochester Institute of Technology (RIT), 2022
- [P6] **M. Zuzak**, "New Horizons in Hardware Security," at Rochester Institute of Technology (RIT), 2021
- [P5] **M. Zuzak**, "Designing Obfuscated Systems for Enhanced Hardware-Oriented Security," at SIGDA Design Automation Conference (DAC) PhD Forum, 2021
- [P4] **M. Zuzak**, "Securing Hardware in a Globalized Supply-Chain," at ARCS Scholar Reception, 2020
- [P3] **M. Zuzak**, "Building Functional ICs with Approximate Keys," at CSAW'19 Logic Locking Conquest Finals, 2019
- [P2] **M. Zuzak**, "Achieving Hardware Security: Design and Fabrication of Secure Integrated Circuits," at ARCS Scholar Reception, 2019
- [P1] **M. Zuzak** and A. Srivastava, "Memory Locking: An Automated Approach to Processor Design Obfuscation," in Design Automation Conference (DAC), 2019

OPEN-SOURCE SOFTWARE

CLAP Attack- A Combined Logical and Physical Attack on Logic Obfuscation

- The CLAP attack is an open-source attack on logic obfuscation utilizing both logical and physical leakage to reverse-engineer the key of an obfuscated circuit. The physical portion of the CLAP attack logically guides an electro-optical probe to extract key leakage through electro-optical frequency mapping (EOFM). The logical portion of the CLAP attack relies on the open-source SAT attack toolkit by Subramanyan et al.

ObfusGEM - A Cycle-Accurate Processor Design Obfuscation Simulator

- ObfusGEM is a simulation framework for the evaluation of processor design obfuscation. It implements an error injection framework inspired by the architectural error resilience community to close-the-loop between gate-level obfuscation and its application-level impact. We provide a library of existing hardware security techniques and configurations along with ObfusGEM to enable the design and evaluation of hardware security configurations for specific architectures or devices.

StatSAT - A Statistical Boolean Satisfiability Attack on Logic Locking

- StatSAT is an open-source SAT-based attack against probabilistic circuits that have been secured by logic locking.

HMCTherm - A Cycle-Accurate Simulator for the Hybrid Memory Cube with Built-In Thermal Analysis

- HMCTherm is a comprehensive simulation framework for a Stacked-Memory-on-CPU architecture. Given the architectural description of a multi-core CPU using hybrid memory cubes (HMC), HMCTherm can simulate the 3D thermal profile (both transient and static) of the HMCs for an arbitrary computing workload.

TEACHING

CMPE361: Introduction to Hardware Security

Fall 2023, 2024

Instructor

Rochester Institute of Technology

- Course proposed, developed, and introduced by Prof. Michael Zuzak

CMPE630/530: Digital Integrated Circuit Design

Spring 2023, 2024

Instructor

Rochester Institute of Technology

ENEE640: Digital CMOS VLSI Design

Spring 2021

Co-Instructor with Prof. Ankur Srivastava

University of Maryland, College Park

ENEE359F: Advanced Verilog Design

Spring 2015

Graduate Teaching Assistant

University of Maryland, College Park

ENEE359F: Advanced Verilog Design

Fall 2014

Graduate Teaching Assistant

University of Maryland, College Park

- Awarded Department of Electrical and Computer Engineering Distinguished Teaching Assistant Award

STUDENT ADVISING

Ph.D. Students:

- Robi Paul Summer 2023 - Present
- Katsuaki Nakano Summer 2024 - Present
- Maksym Melnyk January 2025 - Present

M.S. Students (Thesis):

- **Sydale John Ayi** Spring 2023 - Present
Thesis: NoC Obfuscation and Encoding for Hardware Trojan Mitigation
Awards: NSF Louis Stokes Alliance for Minority Participation (LSAMP) Scholar
- **Long Lam** Summer 2023 - Spring 2024
Thesis: Low Power Logic Locking using Design Space Modeling to Achieve System-Wide Security
Publications: L. Lam, M. Melnyk, and M. Zuzak, "Low Overhead Logic Locking for System-Level Security: A Design Space Modeling Approach," in Proceedings of the ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED), 2024
Awards: RIT Outstanding Undergraduate Scholar, 2024
RIT Computer Engineering Department BS/MS Delegate, 2024
- **Thomas Wojtal** Fall 2022 - Spring 2024
Thesis: Adjoining Gates: Mitigating Optical Side-Channel Attacks on Integrated Circuits through Security-Aware Placement
Awards: RIT Computer Engineering Department MS Delegate, 2024
- **Katsuaki Nakano** (Co-Advised with Prof. Minoru Nakazawa) Fall 2022 - Spring 2024
Thesis: Complementing Vehicle Trajectories Using Two Camera Viewpoints
Publications: K. Nakano, M. Nakazawa, and M. Zuzak, "Complementing Vehicle Trajectories Using Two Camera Viewpoints," in Proceedings of the IEEE Conference on Consumer Electronics (ICCE), 2024
Awards: Best Student Presentation Award, ICCE 2024

• **Jacob Thomas**

Spring 2023 - Fall 2023

Thesis: Software-Based Property Enforcement for Detecting Hardware Anomalies

M.S. Students (Project):

- Robert Reed
- Aaron Schulte
- Aubrey Tarmu
- Yuyang Wang
- Ryan Blow

Fall 2023 - Spring 2024
Spring 2023 - Spring 2024
Fall 2022 - Spring 2024
Fall 2022 - Spring 2024
Fall 2022 - Fall 2023

B.S. Students (Co-Op/Internship):

- Renaaron Ellis
- Maksym Melnyk

Spring 2024 - Present
Fall 2022 - Spring 2024

PROFESSIONAL SERVICE

Chair/Co-Chair:

- Co-Director Beyond9.8 Program with Franklin High School (Cybersecurity Component)
- Co-Chair for 2024 ACM Student Research Competition at ICCAD (SRC@ICCAD'24)
- Co-Chair for 2023 ACM Student Research Competition at ICCAD (SRC@ICCAD'23)

Technical Program Committee Member:

- IEEE/ACM Design Automation Conference (DAC) - 2024
- Hardware Oriented Security and Trust (HOST) - 2024
- Great Lakes Symposium on VLSI (GLSVLSI) - 2023, 2024
- IEEE International System-on-Chip Conference (SOCC) - 2023, 2024
- Workshop on Attacks and Solutions in Hardware Security (ASHES) - 2023, 2024

Special Session Organizer:

- "Machine Learning and Hardware Security: A Winning Combo!," at the Great Lakes Symposium on VLSI (GLSVLSI) –
Organizers: A. Rezaei, **M. Zuzak**, K. Shamsi, and P. Beerel

Session Chair/Co-Chair:

- Great Lakes Symposium on VLSI (GLSVLSI) - 2023

Grant Reviewer:

- NSF Panelist - 2024

Journal Reviewer:

- IEEE Transactions on Knowledge and Data Engineering (TKDE) - 2024
- IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems (TCAD) - 2020, 2021, 2023
- ACM Journal on Emerging Technologies in Computing Systems (JETC) - 2023
- Springer Journal of Cryptographic Engineering (JCEN) - 2023
- Springer Analog Integrated Circuits and Signal Processing - 2022

Conference Sub-Reviewer:

- Design, Automation and Test in Europe Conference (DATE) - 2024
- IEEE International Symposium on On-Line Testing and Robust System Design (IOLTS) - 2023
- IEEE/ACM International Symposium on Microarchitecture (MICRO) - 2021
- IEEE/ACM Design Automation Conference (DAC) - 2021
- IEEE International Symposium on Circuits and Systems (ISCAS) - 2020

Judge:

- ACM Student Research Competition at ICCAD (SRC@ICCAD) - 2022

HONORS AND AWARDS

- Voted Graduation Reader for RIT Computer Engineering Department
- KEEN New Faculty Mini-Fellowship 2023
- Best Paper Candidate at the Design Automation Conference (DAC) 2021
- Future Faculty Fellow for the Clark School of Engineering at the University of Maryland, College Park
- Department of Electrical and Computer Engineering Distinguished Teaching Assistant Award
- ARCS/MWC Named Graduate Scholar (2019-2021)
- Edison Memorial Graduate Fellowship, Naval Research Laboratory
- Clark School of Engineering Distinguished Graduate Fellowship
- CSAW 2019 Logic Locking Conquest Finalist
- Best Paper at MULTIPROG-2017
- On the Spot Award, Naval Research Laboratory
- Northrop Grumman Master's Fellowship
- NSF Student Travel Grant for ISVLSI 2019
- University of Maryland Dean's Scholarship
- Association of Old Crows' (AOC) Scholarship