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 August 2022 - Present
Rochester Institute of Technology

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

EDUCATION

Ph.D., Electrical Engineering August 2017 - August 2022
University of Maryland, College Park

- 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 August 2014 - May 2016
University of Maryland, College Park

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

B.S., Electrical Engineering *(Cum Laude)* August 2010 - May 2014
University of Maryland, College Park

- University of Maryland Honors College, University Honors Citation

RESEARCH EXPERIENCE

University of Maryland, College Park August 2017 - August 2022
Graduate Research Assistant with Prof. Ankur Srivastava

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

Naval Research Laboratory, Surface Electronic Warfare Systems Branch August 2015 - June 2018
Electronics Engineer (Full-Time)

- 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 August 2014 - May 2016
Graduate Researcher with Prof. Donald Yeung

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

EXTERNAL SPONSORED PROJECTS AND GRANTS

Total External Awards as PI/Co-PI: $520,466.00

[G3] NSF: "EAGER: Towards Crowd-Sourced Artifact Curation for Cyberattacks through a Learner-Centered AI Co-Pilot," 06/01/2024 - 05/31/2026, **Amount Awarded: $299,000.00**, **Role: Lead PI**, (Co-PI: J. Yang)

[G2] Eaton Corporation: "Hardware Anomaly and Zero-Day Detection in Resource-Constrained Microcontrollers Using Software Property Enforcement," 06/29/2023 - 06/28/2024, **Amount Awarded: $45,762.00**, **Role: Sole-PI**

[G1] NSF: "CRII: SaTC: Design Space Modeling for Logic Obfuscation to Enable System-Wide Security during IC Manufacture and Test," 03/15/2023 - 03/14/2026, **Amount Awarded: $174,705.00**, **Role: Sole-PI**

PUBLICATIONS

Note: RIT student co-authors are highlighted in the author list.

Journals:

[J8] T. Wojtal, R. Paul, and **M. Zuzak**, "Mitigating Electro-Optical Frequency Mapping Attacks on Logic-Locked Integrated Circuits," in Springer Journal of Hardware and Systems Security (JHASS), 2025

[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:

[C23] R. Ramos-Brito, Ramana Ranganatham, **M. Zuzak**, and T. Das, "An All Analog Temporal Power-Supply Trojan to Subvert ECG Biometric Authentication," in Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), 2025 **(Accepted)**

[C22] R. Paul and **M. Zuzak**, "Michscan: Black-Box Neural Network Integrity Checking at Runtime Through Power Analysis," in Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2025 **(Accepted)**

[C21] M. Melnyk, J. Thomas, M. Wandera, A. Chathoth, and **M. Zuzak**, "Hardware Anomaly Detection in Microcontrollers Through Watchdog-Assisted Property Enforcement," in Proceedings of the IEEE Conference on Consumer Electronics (ICCE), 2025 **(Best Presentation Award - M. Melnyk)**

[C20] A. Galimberti, R. Purkait, N. Islam, A. Ganguly, M. Indovina, **M. Zuzak**, SM Pudukotai Dinakarrao, D. Zoni, and W. Fornaciari, "ML-Assisted Attack Detection on NoC-Based Many-Cores Through On-Chip Traffic Monitoring," in Proceedings of the IEEE International Conference on Electronics Circuits and Systems (ICECS), 2024

[C19] 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

[C18] 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

[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 **(Best Presentation Award - K. Nakano)**

[C16] 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), 2023

[C15] 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

[C14] 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

[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, 2025

Technical Reports:

[T4] R. Fayyazi, S. Trueba, **M. Zuzak**, and S. Yang, "ProveRAG: Provenance-Driven Vulnerability Analysis with Automated Retrieval-Augmented LLMs," in arXiv preprint arXiv:2410.17406, 2024

[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

TEACHING

CMPE799: Generative AI in Cybersecurity (Independent Study) Fall 2024
Co-Instructor (with Prof. Jay Yang) *Rochester Institute of Technology*

CMPE361: Introduction to Hardware Security Fall 2023, 2024
Instructor *Rochester Institute of Technology*

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

Offering Semester	Developed by M. Zuzak	Course Enrollment	Surveys Submitted	Instructor Effectiveness	Course Effectiveness
Fall 2024	Yes	25	41 (22 Course, 19 Lab)	4.73 / 5.0	4.53 / 5.0
Fall 2023	Yes	17	17	4.94 / 5.0	4.76 / 5.0

CMPE630/530: Digital Integrated Circuit Design Spring 2023, 2024
Instructor *Rochester Institute of Technology*

Offering Semester	Developed by M. Zuzak	Course Enrollment	Surveys Submitted	Instructor Effectiveness	Course Effectiveness
Spring 2024	No	20	20	4.8 / 5.0	4.8 / 5.0
Spring 2023	No	21	21	4.86 / 5.0	4.67 / 5.0

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*

- Recognized with Department of Electrical and Computer Engineering Distinguished Teaching Assistant Award

STUDENT ADVISING

Ph.D. Students:

- **Maksym Melnyk** November 2024 - Present
- **Katsuaki Nakano** Summer 2024 - Present
- **Robi Paul** Summer 2023 - Present
- **James Liang (Co-Advisor)** Fall 2021 - Fall 2024

  Thesis: Toward Prototypical Vision Clustering

  First Employer: U.S. Naval Research Laboratory (NRL)

  Note: Due to unforeseen circumstances, my role as a Co-Adviser for James Liang was primarily focused on developing the methodology in [C16] for future collaboration and placement at NRL.

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

  Publication: 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

  Publication: T. Wojtal, R. Paul, and M. Zuzak, "Mitigating Electro-Optical Frequency Mapping Attacks on Logic-Locked Integrated Circuits," in Springer Journal of Hardware and Systems Security (JHASS), 2025

  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

  Publication: 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

  Publication: M. Melnyk, J. Thomas, M. Wandera, A. Chathoth, and M. Zuzak, "Hardware Anomaly Detection in Microcontrollers Through Watchdog-Assisted Property Enforcement," in Proceedings of the IEEE Conference on Consumer Electronics (ICCE), 2025

M.S. Students (Project):

• Trevor Kamen	Fall 2024 - Present
• Ethan Vuong	Fall 2024 - Present
• Quentin Ramos II	Spring 2024 - Present
• Thomas Bertola	Spring 2024 - Present
• Eric Falcone (Awarded RIT Outstanding Undergraduate Scholar, 2025)	Spring 2024 - Fall 2024
• Robert Reed	Fall 2023 - Spring 2024
• Aaron Schulte	Spring 2023 - Spring 2024
• Aubrey Tarmu	Fall 2022 - Spring 2024
• Yuyang Wang	Fall 2022 - Spring 2024
• Ryan Blow	Fall 2022 - Fall 2023

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

• Renaaron Ellis	Spring 2024 - Present
• Chris Nokes	Fall 2023 - Present
• Maksym Melnyk	Fall 2022 - Spring 2024

Ph.D. Committee Member:

• Ahmed Najeeb	Present
• Nithil Harris Manimaran	Present
• Antonio Joia Neto	Present
• Adam Caulfield	Graduated Fall 2024
• Purab Sutradhar	Graduated Spring 2024

PROFESSIONAL SERVICE

Chair/Co-Chair:

- 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)

Organizing Committee:

- Member of Student Scholar Program Committee at International Conference on Computer-Aided Design (ICCAD) - 2024

Technical Program Committee Member:

- IEEE/ACM Design Automation Conference (DAC) - 2024, 2025
- IEEE International Symposium on Hardware Oriented Security and Trust (HOST) - 2024, 2025
- New England Hardware Security (NEHWS) Day - 2025
- ACM 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 2023 Great Lakes Symposium on VLSI (GLSVLSI'23)
  - *Organizers:* A. Rezaei, **M. Zuzak**, K. Shamsi, and P. Beerel

Session Chair:

- Session Chair for "Microarchitecture Support for Security" at International Conference on Computer-Aided Design (ICCAD) - 2024
- Session Chair for "VLSI Circuits and Design I" at Great Lakes Symposium on VLSI (GLSVLSI) - 2023
- Session Chair for "Hardware Security II" at Great Lakes Symposium on VLSI (GLSVLSI) - 2023

Grant Reviewer:

- NSF Panelist - 2024

Journal Reviewer:

- IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems (TCAD) - 2020, 2021, 2023, 2024
- IEEE Transactions on Knowledge and Data Engineering (TKDE) - 2024
- Springer Journal of Hardware and Systems Security (JHASS) - 2024
- 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

Official Judge:

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

Professional Society Membership:

- International Society of Electrical Engineers (IEEE), Member 2019 - Present
- Association for Computing Machinery (ACM), Member 2020 - Present
- National Center for Faculty Development and Diversity (NCFDD), Member 2022 - Present
- American Society for Engineering Education (ASEE), Member 2023 - Present

HONORS AND AWARDS

- Voted Graduation Reader for RIT Computer Engineering Department (2024)
- 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