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, Electronic Design Automation, Computer Architecture, Side-Channel Analysis

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

PUBLICATIONS

Journals:

[J1] **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), 2022 **(Under Review)**

[J2] **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

[J3] 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

[J4] **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

[J5] 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

[J6] 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:

[C1] **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

[C2] 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

[C3] 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

[C4] **M. Zuzak**, Y. Liu, and A. Srivastava, "A Resource Binding Approach to Logic Obfuscation," in Design Automation Conference (DAC), 2021 **(Best Paper Candidate)**

[C5] B. Tan, S. Garg, R. Karri, Y. Liu, **M. Zuzak**, ..., W. Savage, "Independent Verification and Validation of Security-Aware EDA Tools and IP," in Design Automation Conference (DAC), 2021

[C6] **M. Zuzak** and A. Srivastava, "ObfusGEM: Enhancing Processor Design Obfuscation Through Security-Aware On-Chip Memory and Data Path Design," in Proceedings Intl. 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

[C8] Y. Liu, **M. Zuzak** and A. Srivastava, "Strong Anti-SAT: Secure and Effective Logic Locking," in Proceedings of International Symposium on Quality Electronic Design (ISQED), 2020

[C9] Y. Liu, A. Mondal, A. Chakraborty, **M. Zuzak**, N. Jacobson, D. Xing, and A. Srivastava, "A Survey on Neural Trojans," in Proceedings of International Symposium on Quality Electronic Design (ISQED), 2020

[C10] **M. Zuzak**, M. Fitelson, S. Montano, and A. Srivastava, "Provable Detection and Location of Hardware Trojans with Linear Hybrid Cellular Automata," in Proceedings of Government Microcircuit Applications and Critical Technology Conference (GOMACTECH), 2020

[C11] **M. Zuzak** and A. Srivastava, "Memory Locking: An Automated Approach to Processor Design Obfuscation," in Proceedings IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2019

[C12] Z. Yang, **M. Zuzak**, and A. Srivastava, "HMCTherm: A Cycle-accurate HMC Simulator Integrated with Detailed Power and Thermal Simulation," in Proceedings Intl. Symposium on Memory Systems (MEMSYS), 2018

[C13] **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:

[T1] **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

[T3] **M. Zuzak**, "Exploiting Nested Parallelism on Heterogeneous Processors" **(M.S. Thesis)**

POSTER PRESENTATIONS/INVITED TALKS

[P1] **M. Zuzak**, "New Horizons in Hardware Security," at Rochester Institute of Technology (RIT), 2021

[P2] **M. Zuzak**, "Designing Obfuscated Systems for Enhanced Hardware-Oriented Security," at SIGDA Design Automation Conference (DAC) PhD Forum, 2021

[P3] **M. Zuzak**, "Securing Hardware in a Globalized Supply-Chain," at ARCS Scholar Reception, 2020

[P4] **M. Zuzak**, "Building Functional ICs with Approximate Keys," at CSAW'19 Logic Locking Conquest Finals, 2019

[P5] **M. Zuzak**, "Achieving Hardware Security: Design and Fabrication of Secure Integrated Circuits," at ARCS Scholar Reception, 2019

[P6] **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 Satisfiablity 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 EXPERIENCE

University of Maryland, College Park Spring 2021
Co-Teacher with Prof. Ankur Srivastava

- Co-Teacher for joint Undergraduate/Graduate course titled Digital CMOS VLSI Design (ENEE640)

University of Maryland, College Park Fall 2014, Spring 2015
Graduate Teaching Assistant

- Teaching Assistant for Undergraduate/Graduate Advanced Verilog Design Course (ENEE359F) for 2 semesters
- Awarded Department of Electrical and Computer Engineering Distinguished Teaching Assistant Award

PROFESSIONAL SERVICE

Reviewer For:

- IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems (TCAD)
- ACM Journal on Emerging Technologies in Computing Systems (JETC)
- Springer Analog Integrated Circuits and Signal Processing
- 2021 IEEE/ACM International Symposium on Microarchitecture (MICRO)
- 2021 IEEE/ACM Design Automation Conference (DAC)
- 2020 IEEE International Symposium on Circuits and Systems (ISCAS)

HONORS AND AWARDS

- 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