Curriculum Vitae

Shahin Tajik
Assistant Professor
Department of Electrical and Computer Engineering
Worcester Polytechnic Institute
Office: Atwater Kent Laboratories 215
100 Institute Road, Worcester, MA 01609-2280
Phone: 508-831-5231
E-mail: stajik@wpi.edu
Web: https://wp.wpi.edu/stajik/

I. Background

A. Education

Technische Universität Berlin, Berlin, Germany	Ph.D., Electrical Engineering	2017
Technische Universität Berlin, Berlin, Germany	M.S., Electrical Engineering	2013
K. N. Toosi University of Technology, Tehran, Iran	B.S., Electrical Engineering	2010

B. Professional Experience

Assistant Professor	Worcester Polytechnic Institute, Worcester, MA	2021–Present
Assistant Research Professor	Worcester Polytechnic Institute, Worcester, MA	2020–2021
Assistant Research Professor	University of Florida, Gainesville, FL	2019–2020
Postdoctoral Fellow	University of Florida, Gainesville, FL	2018–2019
Postdoctoral Researcher	Technische Universität Berlin, Germany	2017–2018
Research Assistant	Technische Universität Berlin, Germany	2013–2017
Intern	Deutsche Telekom Innovation Laboratories, Germany	2013–2013
Student Assistant	Technische Universität Berlin, Germany	2012–2012
Student Assistant	Fraunhofer Heinrich Hertz Institute, Germany	2010–2011

C. Languages Spoken

- English (full professional proficiency)
- German (full professional proficiency)
- Persian (mother tongue)

II. Scholarship

A. Publications

Books

(B1) S. Tajik, "On the Physical Security of Physically Unclonable Functions," *Springer International Publishing*, 2018.

Book Chapters

(BC1) Y. Yao, P. Kiaei, R. Singh, S. Tajik, P. Schaumont, "Programmable RO (PRO): A Multipurpose Countermeasure against Side-channel and Fault Injection Attack," in Security of FPGA-Accelerated Cloud Computing Environments by Jakub Szefer and Russel Tessier, *in press, Springer*, 2023. **[peer-reviewed]**

(BC2) S. Tajik, F. Ganji, "Artificial Neural Networks and Fault Injection Attacks," in Security and Artificial Intelligence by Thomas Baeck, Lejla Batina, Ileana Buhan, Stjepan Picek, *Springer*, 2022. **[peer-reviewed]**

(BC3) F. Ganji, S. Tajik, “Physically Unclonable Functions and AI: Two Decades of Marriage,”, in Security and Artificial Intelligence by Thomas Baeck, Lejla Batina, Ileana Buhan, Stjepan Picek, *Springer*, 2022. **[peer-reviewed]**

Journal Papers

(J1) T. Mosavirik, S. Khalaj Monfared, M. Saadat Safa, S. Tajik, “Silicon Echoes: Non-Invasive Trojan and Tamper Detection using Frequency-Selective Impedance Analysis,” *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, 2023. **[peer-reviewed, impact factor: 2.18]**

(J2) T. Mosavirik, P. Schaumont, S. Tajik, “ImpedanceVerif: On-Chip Impedance Sensing for System-Level Tampering Detection,” *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, 2023. **[peer-reviewed, impact factor: 2.18]**

(J3) T. Krachenfels, J.-P. Seifert, S. Tajik, “Trojan Awakener: Detecting Dormant Malicious Hardware Using Laser Logic State Imaging (Extended Version),” *Journal of Cryptographic Engineering*, 2023. **[peer-reviewed, impact factor: 1.6]**

(J4) D. S. Koblah, R. Y. Acharya, D. Capecci, O. P. Dizon-Paradis, S. Tajik, F. Ganji, D. L. Woodard, D. Forte, “A Survey and Perspective on Artificial Intelligence for Security-Aware Electronic Design Automation,” *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 2023. **[peer-reviewed, impact factor: 1.447]**

(J5) T. Farheen, S. Roy, S. Tajik, D. Forte,“A Twofold Clock and Voltage-Based Detection Method for Laser Logic State Imaging Attack,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2022. **[peer-reviewed, impact factor: 2.775]**

(J6) T. Mosavirik, F. Ganji, P. Schaumont, S. Tajik, “ScatterVerif: Verification of Electronic Boards Using Reflection Response of Power Distribution Network,” *ACM Journal on Emerging Technologies in Computing Systems*, 2022. **[peer-reviewed, impact factor: 1.420]**

(J7) M. T. Rahman, N. F. Dipu, D. Mehta, S. Tajik, M. Tehranipoor, N. Asadizanjani, “CONCEALING-Gate: Optical Contactless Probing Resilient Design,” *ACM Journal on Emerging Technologies in Computing Systems*, 2021. **[peer-reviewed, impact factor: 1.420]**

(J8) F. Ganji, S. Tajik, P. Stauss, J.-P. Seifert, D. Forte, M. Tehranipoor, “Rock’n’roll PUFs: Crafting Provably Secure PUFs from Less Secure Ones (Extended Version),” *Journal of Cryptographic Engineering*, 2020. **[peer-reviewed, impact factor: 1.6]**

(J9) M. T. Rahman, M. S. Rahman, H. Wang, S. Tajik, W. Khalil, F. Farahmandi, D. Forte, N. Asadizanjani, M. Tehranipoor, “Defense-in-Depth: A Recipe for Logic Locking to Prevail,” *Integration, the VLSI Journal, Elsevier*, 2020. **[peer-reviewed, impact factor: 1.21]**

(J10) T. Hoque, K. Yang, R. Karam, S. Tajik, D. Forte, M. Tehranipoor, and S. Bhunia, “Hidden in Plaintext: An Obfuscation-based Countermeasure against FPGA Bitstream Tampering Attacks,” *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 2019. **[peer-reviewed, impact factor: 0.96]**

(J11) H. Lohrke, S. Tajik, Christian Boit and J.-P. Seifert, “Key Extraction Using Thermal Laser Stimulation: A Case Study on Xilinx Ultrascale FPGAs,” *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, 2018. **[peer-reviewed, impact factor: 2.18]**

(J12) F. Ganji, S. Tajik, F. Fässler, and J.-P. Seifert, “Having No Mathematical Model May Not Secure PUFs”, *Journal of Cryptographic Engineering*, 2017. **[peer-reviewed, impact factor: 1.6]**

(J13) S. Tajik, E. Dietz, S. Frohmann, H. Dittrich, D. Nedospasov, C. Helfmeier, J.-P. Seifert, C. Boit, H.-W. Hübers, “Photonic Side-Channel Analysis of Arbiter PUFs”, *Journal of Cryptology*, 2017. **[peer-reviewed, impact factor: 1.3]**

(J14) F. Ganji, S. Tajik, and J.-P. Seifert, “PAC Learning of Arbiter PUFs”, *Journal of Cryptographic Engineering*, 2016. **[peer-reviewed, impact factor: 1.6]**

Conference Papers

(C1) S. Khalaj Monfared, T. Mosavirik, S. Tajik, "LeakyOhm: Secret Bits Extraction using Impedance Analysis," *ACM Conference on Computer and Communications Security (CCS)*, 2023. **[conditionally accepted]**

(C2) S. Parvin, M. Goli, T. Krachenfels, S. Tajik, J.-P. Seifert, F. Sill Torres, R. Drechsler, "LAT-UP: Exposing Layout-Level Analog Hardware Trojans Using Contactless Optical Probing," *2023 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2023. **Best Student Paper Award**

(C3) M. Saadat Safa, T. Mosavirik, S. Tajik, "Counterfeit Chip Detection using Scattering Parameter Analysis," *26th International Symposium on Design and Diagnostics of Electronic Circuits and Systems*, 2023. **[peer-reviewed, acceptance rate: 34%]**

(C4) T. Farheen, S. Tajik, D. Forte "SPRED: Spatially Distributed Laser Fault Injection Resilient Design" *The 2023 International Symposium on Quality Electronic Design (ISQED)*, 2023.

(C5) S. Roy, S. Tajik, D. Forte "Polymorphic Sensor to Detect Laser Logic State Imaging Attack" *The 2023 International Symposium on Quality Electronic Design (ISQED)*, 2023.

(C6) D.S. Koblah, F. Ganji, D. Forte, S. Tajik, "Hardware Moving Target Defenses against Physical Attacks: Design Challenges and Opportunities," *9th ACM Workshop on Moving Target Defense*, 2022. **[invited paper]**

(C7) M. Choudhury, M. Gao, S. Tajik, D. Forte, "TAMED: Transitional Approaches for LFI Resilient State Machine Encoding," *IEEE International Test Conference (ITC)*, 2022. **[peer-reviewed]**

(C8) S. Tajik and P. Schaumont, "The Technological Arms Race in Hardware Security," *IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI)*, 2022. **[invited paper]**

(C9) S. Parvin, T. Krachenfels, S. Tajik, J.-P. Seifert, F. Sill Torres, R. Drechsler, "Toward Optical Probing Resistant Circuits: A Comparison of Logic Styles and Circuit Design Techniques," *Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2022. **[peer-reviewed, acceptance rate: 36.5%]**

(C10) S. Roy, T. Farheen, S. Tajik, D. Forte, "Self-timed Sensors for Detecting Static Optical Side Channel Attacks," *International Symposium on Quality Electronic Design (ISQED)*, 2022. **[peer-reviewed]**

(C11) T. Krachenfels, F. Ganji, A. Moradi, S. Tajik, J.-P. Seifert, "Real-World Snapshots vs. Theory: Questioning the t-Probing Security Model," *IEEE Symposium on Security and Privacy (SP) - Oakland*, 2021. **[peer-reviewed, impact factor: 3.82, acceptance rate: 12.0%]**

(C12) T. Krachenfels, T. Kiyan , S. Tajik, J.-P. Seifert, "Automatic Extraction of Secrets from the Transistor Jungle using Laser-Assisted Side-Channel Attacks," *USENIX Security Symposium (USENIX Security 21)*, 2021. **[peer-reviewed, impact factor: 2.79, acceptance rate: 18.6%]**

(C13) M. Choudhury, S. Tajik, D. Forte, "PATRON: A Pragmatic Approach for Encoding Laser Fault Injection Resistant FSMs," *Design, Automation and Test in Europe Conference and Exhibition (DATE)*, IEEE, 2021. **[peer-reviewed, acceptance rate: 24%]**

(C14) T. Krachenfels, J.-P. Seifert, S. Tajik, "Trojan Awakener: Detecting Dormant Malicious Hardware Using Laser Logic State Imaging," *Workshop on Attacks and Solutions in Hardware Security (ASHES)*, 2021. **[peer-reviewed]**

(C15) M. Choudhury, S. Tajik, D. Forte, "SPARSE: Spatially Aware LFI Resilient State Machine Encoding," *10th International Workshop on Hardware and Architectural Support for Security and Privacy (HASP)*, ACM, 2021. **[peer-reviewed]**

(C16) E. Amini, K. Bartels, C. Boit, M. Eggert, N. Herfurth, T. Kiyan, T. Krachenfels, J.-P Seifert, S. Tajik, "Special Session: Physical Attacks through the Chip Backside: Threats, Challenges, and Opportunities," *IEEE VLSI Test Symposium (VTS)*, 2021.

(C17) M. T. Rahman, S. Tajik, M.S. Rahman, M. Tehranipoor, N. Asadizanjani "The Key is Left under the Mat: On the Inappropriate Security Assumption of Logic Locking Schemes," *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2020. **[peer-reviewed]**

(C18) A. Stern, D. Mehta, S. Tajik, F. Farahmandi, M. Tehranipoor, "SPARTA: A Laser Probing Approach for Trojan Detection," *IEEE International Test Conference (ITC)*, 2020. **[peer-reviewed]**

(C19) A. Stern, D. Mehta, S. Tajik, U. Guin, F. Farahmandi, M. Tehranipoor, "SPARTA-COTS: A Laser Probing Approach for Sequential Trojan Detection in COTS Integrated Circuits," *IEEE International Conference on Physical Assurance and Inspection of Electronics (PAINE)*, 2020. **[peer-reviewed]**

(C20) A. Stern, J. Vosatka, S. Tajik, F. Farahmandi, M. Tehranipoor, "Trust Assessment for Electronic Components using Laser and Emission-based Microscopy," *IEEE Research and Applications of Photonics in Defense Conference (RAPID)*, 2020. **[peer-reviewed]**

(C21) F. Ganji, S. Amir, S. Tajik, D. Forte, J.-P. Seifert, "Pitfalls in Machine Learning-based Adversary Modeling for Hardware Systems," *Design, Automation and Test in Europe Conference and Exhibition (DATE)*, IEEE, 2020. **[peer-reviewed]**

(C22) M. Alam, S. Tajik, F. Ganji, M. Tehranipoor, D. Forte, "RAM-Jam: Remote Temperature and Voltage Fault Attack on FPGAs using Memory Collisions," *2019 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, 2019. **[peer-reviewed]**

(C23) F. Ganji, S. Tajik, P. Stauss, J.-P. Seifert, D. Forte, M. Tehranipoor, "Rock'n'roll PUFs: Crafting Provably Secure PUFs from Less Secure Ones," *International Workshop on Security Proofs for Embedded Systems (PROOFS)*, 2019. **[peer-reviewed]**

(C24) M. T. Rahman, Q. Shi, S. Tajik, H. Shen, D. L. Woodard, M. Tehranipoor, N. Asadizanjani, "Physical Inspection and Attacks: New Frontier in Hardware Security," *International Verification and Security Workshop (IVSW)*, IEEE, 2018. **[peer-reviewed]**

(C25) F. Ganji, S. Tajik, J.-P. Seifert, "A Fourier Analysis Based Attack against Physically Unclonable Functions," *International Conference on Financial Cryptography and Data Security (FC)*, 2018. **[peer-reviewed]**

(C26) S. Tajik, H. Lohrke, J.-P. Seifert, and C. Boit, "On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs," *ACM Conference on Computer and Communications Security (CCS)*, 2017. **[peer-reviewed]** ***[CCS 2017 Best Paper Award Nominee, CSAW'17 Applied Research Competition award]***

(C27) S. Tajik, J. Fietkau, H. Lohrke, J.-P. Seifert, C. Boit, "PUFMon: Security Monitoring of FPGAs using Physically Unclonable Functions," *IEEE International Symposium on On-Line Testing and Robust System Design (IOLTS)*, 2017.

(C28) H. Lohrke, H. Zöllner, P. Scholz, S. Tajik, C. Boit, and J.-P. Seifert, "Visible Light Techniques in the FinFET Era: Challenges, Threats and Opportunities", invited paper, *IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*, 2017.

(C29) H. Lohrke, S. Tajik, P. Scholz, J.-P. Seifert, C. Boit, "Automated Detection of Fault Sensitive Locations for Reconfiguration Attacks on Programmable Logic", *ASM International Symposium for Testing and Failure Analysis (ISTFA)*, 2016. **[peer-reviewed]**

(C30) H. Lohrke, S. Tajik, Christian Boit, and J.-P. Seifert, "No Place to Hide: Contactless Probing of Secret Data on FPGAs", *Conference on Cryptographic Hardware and Embedded Systems (CHES)*, 2016. **[peer-reviewed]**

(C31) F. Ganji, S. Tajik, Fabian Fässler, and J. -P. Seifert, "Strong Machine Learning Attack against PUFs with No Mathematical Model," *Conference on Cryptographic Hardware and Embedded Systems (CHES)*, 2016. **[peer-reviewed]** ***[CHES 2016 Best Paper Award Nominee, Invited to Journal of Cryptographic Engineering]***

(C32) C. Boit, S. Tajik, P. Scholz, E. Amini, A. Beyreuther, H. Lohrke, J.P. Seifert, "From IC Debug to Hardware Security Risk: The Power of Backside Access and Optical Interaction", invited paper, *IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*, 2016.

(C33) F. Ganji, S. Tajik, J.-P. Seifert, "Let Me Prove it to You: RO PUFs are Provably Learnable", *18th Annual International Conference on Information Security and Cryptology (ICISC)*, 2015 **[peer-reviewed]**

(C34) F. Ganji, J. Krämer, J. -P. Seifert, S. Tajik, "Lattice Basis Reduction Attack against Physically Unclonable Functions", *ACM Conference on Computer and Communications Security (CCS)*, 2015. **[peer-reviewed]**

(C35) S. Tajik, H. Lohrke, F. Ganji, J. -P. Seifert, and C. Boi, “Laser Fault Attack on Physically Unclonable Functions,” *Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, 2015. **[peer-reviewed]**

(C36) F. Ganji, S. Tajik, and J. -P. Seifert, “Why Attackers Win: On the Learnability of XOR Arbiter PUFs,” *International Conference on Trust and Trustworthy Computing (TRUST)*, 2015. **[peer-reviewed]**

(C37) S. Tajik, E. Dietz, J.-P. Seifert, D. Nedospasov, S. Frohmann, C. Helfmeier, H. Dittrich, and C. Boit, “Physical Characterization of Arbiter PUFs,” *Conference on Cryptographic Hardware and Embedded Systems (CHES)*, 2014. **[peer-reviewed]** ***[CHES 2014 Best Paper Award Nominee, Invited to Journal of Cryptology]***

(C38) S.Tajik, D. Nedospasov, C. Helfmeier, J.-P Seifert, C. Boit, “Emission Analysis of Hardware Implementations,” *EUROMICRO DSD*, 2014. **[peer-reviewed]**

(C39) C. Helfmeier, D. Nedospasov, S. Tajik, C. Boit, J.-P Seifert, “Physical Vulnerabilities of Physically Unclonable Functions,” *Design, Automation, and Test (DATE) in Europe*, 2014. **[peer-reviewed]**

(C40) M. Roshandel, A. Munjal, P. Moghadam, S. Tajik, and H. Ketabdar, “Multi-sensor Finger Ring for Authentication based on 3D Signatures”, *Human-Computer Interaction (HCI) International*, 2014. **[peer-reviewed]**

(C41) S. Tajik and A. Rostami, “MultiFlow: Enhancing IP Multicast over IEEE 802.11 WLAN,” *Wireless Days (WD), IFIP/IEEE*, 2013. **[peer-reviewed]**

B. Patents

(P1) F. Ganji, S. Tajik, J.-P. Seifert, D. Forte, M. Tehranipoor, “Hardness Amplification of Physical Unclonable Functions (PUFs),” US Patent App.# 16841873.

(P2) S. Tajik, T, Mosavirik, P. Schaumont, “Electronic Tampering Detection,” *pending.*

(P3) S. Tajik, T, Mosavirik, F. Ganji, P. Schaumont, “Method for Verifying Integrity and Authenticity of a Printed Circuit Board,” *pending.*

(P4) M. Tehranipoor, A. Stern, S. Tajik, F. Farahmandi, “Systems and methods for laser probing for hardware trojan detection,” US Patent App.# 17/196,035.

(P5) H. Ketabdar, B. Löhlein, M. Roshandel, M. Schlüssler, S. Tajik, “Method and System For Rating Measured Values Taken From a System,” Publication number: EP2854045B1.

(P6) Hamed Ketabdar, Bernhard Löhlein, Mehran Roshandel, Martin Schlüßler, Shahin Tajik, “System and method for computing of anomalies based on frequency driven transformation and computing of new features based on point anomaly density,” Publication Number: EP3457609A1.

C. Fellowships and Grants

- National Science Foundation (NSF), “Collaborative Research: SaTC: CORE: Small: ERADICATOR: Techniques for Laser Assisted Side-Channel Attack Monitor & Response,” $497,147, 7/22 - 5/25, S. Tajik (PI) and Domenic Forte (Co-PI, University of Florida), Personal share: 55%
- Electric Power Research Institute (EPRI), “Physical and Statistical Analysis of Hardware-Based Reference Signatures,” $171,629, 11/22 - 12/23, S. Tajik (PI), F. Ganji, and P. Schaumont (Co-PIs), Personal share: 40%
- Microchip Technology Inc., “IC Package Tamper Detection,” $10,000 12/22 - 12/23, S. Tajik (PI), Personal share: 100%
- Massachusetts Technology Collaborative (MassTech), “Toward a Globally Competitive Electronics Workforce Endowed with Next Generation Cybersecurity Techniques,” $2,000,000, 12/21 - 12/23, S. Tajik (PI), F. Ganji, B. Sunar, and P. Schaumont (Co-PIs)
- Cisco Systems Research, Silicon Valley Community Foundation, “PCBmeter: Remote PCB Verification using On-chip IP cores,” $79,477, 1/21 - 12/22, S. Tajik (PI) and P. Schaumont (Co-PI), Personal share: 90%

- National Science Foundation (NSF), “MRI: Acquisition of: High-Resolution Photon Emission/Laser Fault Injection Microscope with High-Performance Computers for Failure Analysis and Security Assessment of Electronic Systems,” $360,608, 8/21 - 9/24,F. Ganji (PI), S. Tajik, U. Guler, P. Schaumont, B. Sunar (Co-PIs)
- Electric Power Research Institute (EPRI), “Hardware Based Reference Signatures (HBRS) - Phase 2,” $109,422, 7/21 - 12/21, P. Schaumont (PI) and S. Tajik (Senior Personnel)

D. Professional presentations

Invited Talks

- “The Threat of Single Trace Laser-Assisted Side-Channel Attacks to Secure Designs,“ Special Seminar Series at Intel, 2022.
- “Debunking Common Myths About The Hardness of Optical Side-Channel Attacks,” Special Session at IEEE VLSI Test Symposium (VTS), 2021.
- “The Role of Photons in Hardware Security,” FICS Research Annual Conference on Cybersecurity, Gainesville, Florida, March 2019.
- “Semi-invasive Physical Attacks from IC Backside and Possible Countermeasures,” Advances in Integrated Circuit Reverse Engineering and Physical Attacks, DAC 2018, San Francisco, CA, USA, June 2018.
- “Threat Assessment of IC Reverse-Engineering through Optical Probing Attack,” Computer Science Colloquium, University of Bremen, Bremen, Germany, April 2018.
- “Threat Assessment of IC Reverse-Engineering through Optical Probing Attack,” Testmethoden und Zuverlässigkeit von Schaltungen und Systemen (TuZ 2018), Freiburg, Germany, March 2018.
- “On the Vulnerability of FPGAs to Optical Contactless Probing,” Fraunhofer Institute AISEC, Garching b. Munich, Germany, January 2018.
- “How Secure are Modern FPGAs,” Foundation of Secure Scaling Seminar, Schloss Dagstuhl, May 16-20, Germany, 2016.
- “Semi-Invasive Analysis of Physically Unclonable Functions,” Hardware Security Seminar, Schloss Dagstuhl, May 16-20, Germany, 2016.
- “Laser Fault Attack against Physically Unclonable Functions”, 23rd Crypto Day, ESCRYPT, Berlin, Germany, December 10-11, 2015.
- “Physical Characterization of Arbiter PUFs”, 20th Crypto Day, T-Labs, Berlin, Germany, June 26-27, 2014

Tutorials

- “Impedance Analysis: A Novel Physical Side-Channel for Defensive and Offensive Hardware Security,” PROACT Training School 2023, Vodice, Croatia, 2023.
- “Optical SCA through the Chip Backside: Threats, Challenges, and Opportunities,” Hardwear.io Webinar Series, 2021.
- “Security of PUFs: Lessons Learned after Two Decades of Research,” CHES 2019 Tutorial, Atlanta, Georgia, 2019.

E. Professional society memberships and offices

- 2008 - present: Institute of Electrical and Electronics Engineers (IEEE) member
- 2014 - present: International Association for Cryptologic Research (IACR) member
- 2021 - present: Association for Computing Machinery (ACM) member

F. Honors and Awards

- Co-author of Best Student Paper Award, IEEE Computer Society Annual Symposium on VLSI (ISVLSI) (ISVLSI) 2023.
- Best Hardware Demo Award, IEEE Symposium on Hardware Oriented Security and Trust (HOST) 2020.
- Schloss Dagstuhl - National Science Foundation (NSF) Support Grant for Junior Researchers, Awarded, 2019
- National Science Foundation (NSF) Travel Grant - Conference on Cryptographic Hardware and Embedded Systems (CHES), Awarded, 2019 and 2018
- Recognition of Ph.D. Degree with the Highest Distinction (Summa Cum Laude) - Technische Universität Berlin, 2017
- European Cyber Security Awareness Week (CSAW) Award, 2017
- Nominated for ACM Computer and Communications Security (CCS) Best Paper Award, 2017
- The International Association for Cryptologic Research (IACR) Travel Grants - Conference on Cryptographic Hardware and Embedded Systems (CHES), 2014, 2015, and 2016
- Runner-up papers for Conference on Cryptographic Hardware and Embedded Systems (CHES) 2014 and 2016

III. Teaching

A. Courses Taught at WPI

- Spring 2023: ECE 569 - Graduate Seminars (42 participants)
- Fall 2022 (A-Term): ECE 2049 - Embedded Computing in Engineering Design (69 participants, overall evaluation: 3.5)
- Fall 2021 (A-Term): ECE 2049 - Embedded Computing in Engineering Design (67 participants, overall evaluation: 3.5)
- Fall 2022: Guest Lecturer, 2 sessions at ECE 579C - Applied Cryptography and Physical Attacks
- Fall 2021: Guest Speaker, 1 session at the ECE 569 - Graduate Seminars

B. Previous Teaching Experiences

- Winter Semester 2017/18 (TU Berlin): Hardware Security (Lecture+Lab)
- Winter Semester 2016/17 (TU Berlin): Hardware Security (Lecture+Lab)
- Winter Semester 2015/16 (TU Berlin): Hardware Security (Lecture+Lab)
- Summer Semester 2015 (TU Berlin): Computer Security Seminar
- Fall 2019 (University of Florida): Guest Lecturer for 2 sessions at EEL (4930-5934) - Physical Inspection and Attacks on Electronics (PHIKS)
- Fall 2018 (University of Florida): Guest Lecturer for 2 sessions at EEL (4930-5934) - Physical Inspection and Attacks on Electronics (PHIKS)

C. Undergraduate projects (MQPs) advised and co-advised at WPI

- Kyle Mitard (C, D, A, B-Terms 2023), Vulnerability Analysis of security ICs against Laser Fault Injection
- Evan Wu (A, B, C, D-Terms 2022/23), Photon Emission and Laser-Assisted Side-Channel Analysis of Hardware Implementations
- Rachel Feldman (A, B, C-Terms 2022/23), Analysis of SRAM-based Physical Unclonable Functions

- Maxwell Westreich, (A, B, C-Terms 2021/22), PCB Verification using a Built-in FPGA Security Monitoring IP
- Isabell Estrada (A, B, C-Terms 2021/22), Chaos or Noise? Characterization of Meta-stable Behavior of Bistable Rings
- Victor Mercola (A, B, C-Terms 2021/22), Chaos or Noise? Characterization of Meta-stable Behavior of Bistable Rings

D. Graduate theses and dissertations advised at WPI

- Tahoura Mosavirik (Fall 2021 - present): Ph.D. thesis (RA)
- Maryam Sadat Safa (Fall 2022 - present): Ph.D. thesis (TA)
- Saleh Khalaj Monfared (Fall 2022 - present): Ph.D. thesis (TA)
- Victor Mercola (Fall 2022 - Spring 2023): M.S. thesis, co-advised with Prof. Ganji

E. Academic advising at WPI

- Fall 2021 - Present: 4 Graduate Advisees
- Fall 2021 - Present: 6 Undergraduate Advisees

F. Mentored External Ph.D. and Master Students

Ph.D. Students

- Thilo Krachenfels (TU Berlin, 2019 - present), co-advised with Prof. Jean-Pierre Seifert
- Muhtadi Choudhury (UF, 2020 - 2023), co-advised with Prof. Forte
- Tasnuva Farheen (UF, 2020 - present), co-advised with Prof. Forte
- Mir Tanjidur Rahman (UF, 2018 - 2020), co-advised with Prof. Asadizanjani
- Andrew Stern (UF, 2019-2020), co-advised with Prof. Tehranipoor
- Md Mahbub Alam (UF, 2019), co-advised with Prof. Forte
- Dhwani Mehta (UF, 2019), co-advised with Prof. Tehranipoor
- Mohammad Farmani (UF, 2018), co-advised with Prof. Tehranipoor
- Nidish Vashistha (UF, 2018), co-advised with Prof. Tehranipoor

Master Students

- Thilo Krachenfels (Master Thesis, TU Berlin, 2018)
- Pascal Stauss (Master Thesis, TU Berlin, 2018)
- Julian Fietkau (Master Thesis, TU Berlin, 2017)
- Fabian Fäßler (Master Project, TU Berlin, 2016)

IV. Services

A. Regional

- January 2022 - Present: Representing WPI in the Northeast Microelectronics Coalition (NEMC)
- August 2022 - Present: Leading the Secure Edge Computing R&D working group in the Northeast Microelectronics Coalition (NEMC) to prepare a hub proposal for CHIPS ACT's DoD Microelectronics Commons
- April 2023: Co-organizing the 2nd New England Hardware Security (NEHWS) Days
- April 2022: Co-organizing the 2nd New England Hardware Security (NEHWS) Days
- April 2021: Co-organizing the 1st New England Hardware Security (NEHWS) Days

B. Department and university

- Spring 2023: ECE Ad-hoc Undergraduate Curriculum Committee
- Spring 2023: ECE Visibility Committee
- Fall 2022: ECE Ad-hoc Undergraduate Curriculum Committee
- Fall 2022: ECE Visibility Committee
- Summer 2022: Ph.D. Thesis Defense Committee (Pantea Kiaei, July 28, 2022)
- Spring 2022: ECE Visibility Committee
- Spring 2022: Ph.D. Area Exam Committee (Pantea Kiaei, April 26, 2022)
- Spring 2022: M.S. Thesis Committee (Ramazan Kaan Eren, April 19, 2022)
- Fall 2021: ECE Visibility Committee
- Fall 2021: M.S. Thesis Committee (Jacob Grycel, May 3, 2021)

C. Profession

Program Committee (PC)

- Conference on Cryptographic Hardware and Embedded Systems (CHES 2019 and 2023)
- Great Lakes Symposium on VLSI (GLSVLSI 2022 and 2023)
- IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA 2022)
- Workshop on Artificial Intelligence in Hardware Security (AIHWS 2022, 2021, and 2020)
- Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2023, 2022, 2021, 2020, and 2019)
- IEEE International Symposium on Hardware Oriented Security and Trust (HOST 2020)
- Workshop on Attacks and Solutions in Hardware Security (ASHES 2022, 2020, 2019, and 2018)
- IEEE International Workshop on Physical Attacks and Inspection on Electronics (PAINE 2020, 2019, and 2019)
- ASM International Symposium for Testing and Failure Analysis (ISTFA 2019)

Journal Reviewer

- IEEE Transactions on Computers (TC)
- IEEE Transactions on Dependable and Secure Computing (TDSC)
- IEEE Transactions on Circuits and Systems (TCAS)

- IEEE Transactions on Very Large Scale Integration (TVLSI)
- IEEE Transactions on Information Forensics and Security (TIFS)
- IEEE Transactions on Emerging Topics in Computing (TETC)
- IEEE Transactions on Industrial Informatics (TII)
- IEEE Embedded Systems Letters (ESL)
- IEEE Journal on Emerging and Selected Topics in Circuits and Systems (JETCAS)
- ACM Journal on Emerging Technologies in Computing Systems (JETC)
- Journal of Cryptographic Engineering (JCEN)
- Journal of Hardware and Systems Security (HASS)
- Elsevier Journal of Microprocessors and Microsystems (MICPRO)

Conference Reviewer

- International Conference on Field-Programmable Logic and Applications (FPL 2020)
- Cryptographers' Track RSA (CT-RSA 2020)
- IEEE European Test Symposium (ETS 2018)
- Design Automation Conference (DAC 2018)
- IEEE International Symposium on Hardware Oriented Security and Trust (HOST 2014)