

Aydin Aysu

Associate Professor & Entrepreneur
North Carolina State University

Email: aaysu@ncsu.edu
Website: <https://research.ece.ncsu.edu/aaysu/>
Work Address: 890 Oval Dr, Raleigh, NC 27606

Education

Post-Doc , Department of ECE, The University of Texas at Austin	2016–2018
Ph.D. in Computer Engineering, Virginia Tech Thesis: <i>Resource-Constrained and Resource-Efficient Modern Cryptosystem Design</i>	2012–2016 Blacksburg, VA
M.Sc. in Electronics Engineering, Sabanci University Thesis: <i>A Baseline H.264 Video Encoder Hardware Design</i>	2008–2010 Istanbul, Turkey
B.Sc. in Microelectronics Engineering with Mathematics Minor, Sabanci University	2004–2008 Istanbul, Turkey

Summary

Associate Professor and entrepreneur, exemplifies exceptional managerial acumen in hardware and security by leading a research lab with **12 PhD** candidates (mentored over **40 researchers**), publishing **70+** peer-reviewed papers, founding MithrilAI Corp., securing over **\$5.8 million** in funding, and overseeing technical development with a multidisciplinary team.

Honors and Awards

Daugherty Endowment	My start-up company won an NCSU start-up Daugherty Award
Security Top Picks	HOST'20 paper selected as a top picks in 2018–2023 hardware and embedded security
University Faculty Scholar	NCSU outstanding academic achievement award for early- and mid-career faculty
NSF SBIR Phase-I	My start-up company won an National Science Foundation SBIR Phase-I award
Best Paper Nomination	TCHES 2022 paper has been nominated for best paper award based on review scores
Best Paper Recognition	Best paper recognition award at 2022 IEEE Hardware Security and Trust conference
Goodnight Innovators Award	NCSU early career faculty excellence award in STEM research and education
Publicity Paper Award	DAC 2022 paper was selected for the conference's publicity campaign
Google RSP Award	Google Research Scholar award for world-class research of early-career professors
Security Top Picks	HOST'18 paper selected as a top picks in 2015–2020 hardware and embedded security
NSF CAREER	NSF Faculty Early Career Development Award (2020)
Bennett Faculty Fellow	NC State University high achieving young faculty award
Best Paper Award	Best paper award at 2020 DATE conference
NSF CRII	NSF Research Initiation Initiative Award (2019)
Best Paper Award	Best paper award MSE Track at 2019 GLS-VLSI conference
Best Paper Runner-Up	Best student paper award nomination at 2019 Hardware Security and Trust conference
FRPD	NC State's 2019 Faculty Research and Professional Development Award
Best Paper Runner-Up	Best paper award nomination at 2018 IEEE Hardware Security and Trust conference
Top 50 Article (ESL)	Journal article listed in the top 50 popular publications of 2017 Embedded System Letters

Outstanding PhD Award	Awarded for the outstanding publications by Virginia Tech CESCA research center (2015)
Best Poster Award	Winner of Best Poster Award at Virginia Tech (CESCA Day 2014)
Best Presentation Award	Winner of Best Presentation Award at Virginia Tech (CESCA Day 2013)

Funding Awarded

NSF I/UCRC: Center for Advanced Electronics through Machine Learning, PI Detecting and Mitigating Fault Injection Attacks on AI/ML Chiplets	2025–2027
Semiconductor Research Corporation, Co-PI Securing On-Chip AI Accelerators Against Emerging Microarchitectural Attacks	2025–2028
Department of Energy, PI Center for Agile and Intelligent Power Systems: Cybersecurity Research, Development, and Workforce Training	2025–2027
National Science Foundation, PI Collaborative Research: SaTC: EDU: A Socially-Distant Cloud-Based Hardware Security Educational Platform	2024–2027
National Science Foundation, PI NSF-DFG: SaTC: CORE: Small: A Unified Hardware Design for the USA and German Post-Quantum Standards	2024–2027
National Science Foundation, Co-PI POSE: Phase I: An Open-Source Approach to Measure and Analyze Embedded Systems Security	2024–2025
Naval Surface Warfare Center, PI VerIP: Hardware Support for Securely Leveraging Untrusted Intellectual Property Cores	2023–2025
National Science Foundation, Senior Personnel SBIR Phase I: SaiFE: Trusted AI with Hardware Security Enforcement	2024–2025
National Security Agency, Co-PI GenCyberPack: Professional Development for Middle and High School Teachers on Cybersecurity	2023–2024
National Science Foundation, Sole PI SaTC: CORE: Small: An Automated Framework for Mitigating Single-Trace Side-Channel Leakage	2023–2026
Office of Naval Research, Sole PI Event Horizon: Hardware Security Emulators for Next-Generation Edge AI/ML	2022–2025
Google LLC, Sole PI Demonstrating and Mitigating Security Vulnerabilities of Edge Tensor Processing Units	2022–2023
Goodnight Early Career Innovator Award, Sole PI Early Career Award for Outstanding Research Contributions	2022–2025
National Science Foundation CCF, Sole PI SHF: Small: A New Approach for Hardware Design of High-Precision Discrete Gaussian Sampling	2022–2024
National Science Foundation PFI, Co-PI PFI-TT: Embedded Radio Frequency Identification (RFID) to secure the semiconductor supply chain	2022–2023
Office of Naval Research, co-PI Enabling Secure and Efficient Sharing of Accelerators in Expeditionary Systems	2021–2024
NSF I/UCRC: Center for Advanced Electronics through Machine Learning, PI ML-Based Security Analysis and Mitigation of Homomorphic Encryption Side-Channels	2020–2022
NCSU R. Ray Bennett Faculty Fellow Award, Sole PI High Achieving Untenured Young Faculty Award	2019–2020
National Science Foundation CAREER, Sole PI Physical Side-Channels Beyond Cryptography: Transforming the Side-Channel Framework for Deep Learning	2020–2025

NSF I/UCRC: Center for Advanced Electronics through Machine Learning, Co-PI FPGA Hardware Accelerator for Real Time Security	2020–2021
Semiconductor Research Corporation, PI Differential Power Analysis of Deep Neural Networks with Mitigations at the Architecture Level	2019–2022
National Science Foundation CRII, Sole PI CRII: SaTC: Secure Instruction Set Extensions for Lattice-Based Post-Quantum Cryptosystems	2019–2021
NSF I/UCRC: Center for Advanced Electronics through Machine Learning, PI Enabling Side-Channel Attacks on Post-Quantum Protocols through Machine Learning	2019–2020
NCSU Faculty Research & Professional Development, Sole PI ATOM-Crypt: A Tiny and Optimized Microcontroller Design for Emerging Lightweight Cryptography Standard	2019–2020
Equipment Donation, Sole PI Xilinx and Nvidia	2018–2019

Managerial Experience

MithrilAI Corp. Motto: Trusted AI Needs Trusted Hardware Early Stage Start-Up Developing Trusted AI Hardware	Founder & CEO <i>2023–Present</i> (Raleigh, NC)
- Founded and been leading a company that develops secure hardware for AI systems - Won an National Science Foundation SBIR Phase-I Award - Won Daugherty Endowment and North Carolina Matching Fund awards - Formed an advisory board, hired all administrators and engineers to run the company - Overseeing technical development of product teams	
North Carolina State University Departments: Assistant Professor at ECE between 2018-2024, now Associate Research Group: <i>HECTOR – Hardware Cybersecurity Research</i>	Associate Professor <i>2018–Present</i> (Raleigh, NC)
- Leading a research lab on hardware and embedded cybersecurity currently managing 12 PhD students - Teaching graduate/undergraduate courses on digital circuits and applied cryptography - Serving in the technical program committee at flagship security conferences and reviewing manuscripts for major journals - Graduated 1 post-doc, 4 PhD, 2 MS, and 20+ undergraduate researchers all hired to key industry and academic positions - Published 70+ peer-reviewed papers at leading venues and journals	

Research and Industry Experience

The University of Texas at Austin Advisors: Prof. Mohit Tiwari, Prof. Michael Orshansky Projects: <i>Secure Computer Architectures, Micro-Architectural Attacks, Side-Channels</i>	Post-Doctoral Research Fellow <i>2016–2018</i> (Austin, TX)
- Introduced new side-channel attacks and countermeasures for lattice-based post-quantum cryptosystems - Proposed a fresh re-keying scheme for PUFs (physical unclonable functions) and showed its feasibility - Demonstrated rowhammer and covert-channel attacks on micro-architectures and machine learning-based defenses - Authored 5 papers on hardware-based cybersecurity	
Virginia Tech, Secure Embedded Systems Lab Advisor: Prof. Patrick Schaumont Projects: <i>Post-Quantum Crypto., Physical Unclonable Functions, Anonymous Protocols</i>	Research Assistant <i>2012–2016</i> (Blacksburg, VA)
- Designed the world's smallest symmetric-key encryption units and cryptographic processors on FPGAs - Proposed novel authentication protocols and end-to-end cryptographic applications via PUF based systems - Optimized hash-based and lattice-based post-quantum cryptosystems for real-time/energy-harvesting applications - Published 14 papers in flagship international conferences and high-ranked journals	
Qualcomm Inc., Product Security Initiative Project: <i>Authentication with Physical Unclonable Functions</i>	Summer Research Intern <i>Jun–Aug 2014</i>

- Developed novel authentication protocols with PUFs for multi-vendor IoT Applications
- Prototyped protocols on RFID/NFC platforms with low-cost microcontrollers and FPGAs
- Granted 1 US patent based on this work

(San Diego, CA)

Vestek Research and Development Corp., Pixellence Design Team

Digital Design Engineer

Project: *Depth Estimation and Adjustment for 3DTV-Video Enhancement*

2010–2012

- Completed the full design and implementation flow from software description to commercial FPGA end-product (Istanbul, Turkey)
- Published 1 paper on systematic design methods for low-cost video enhancement hardware

Sabanci University, System-on-Chip Design & Test Lab

Research Assistant

Project: *Motion Estimation and Video Coding*

2008–2010

- Designed low-power and low-energy hardware components for H.264/MPEG-4 Video Coding (Istanbul, Turkey)
- Integrated a fully-functional H.264 video encoder
- Published 3 papers on low-power/low-energy VLSI design and integration

Teaching Experience

North Carolina State University, ECE/CS Department

Instructor

Graduate Course: *ECE/CS 592: Cryptographic Engineering and Hardware Security*

2018–present

- Developed a new graduate course on how to establish trust at the hardware root-of-trust (Raleigh, NC)
- Prepared course materials including all hands-on assignments and course projects
- **Best Paper Award:** Published a paper on designing such a course aiming next-generation cryptosystems

Undergraduate Course: *ECE 212: Fundamentals of Logic Design*

2019–present

- Taught an undergraduate course on the fundamentals of digital electronics to 700+ sophomores (Raleigh, NC)

The University of Texas at Austin, ECE Department

Guest Lecturer

Graduate Course: *EE 382: Security at the Hardware/Software Interface*

Fall 2017

- Gave a series of guest lectures on hardware-based cybersecurity: side-channel attacks and PUFs (Austin, TX)
- Prepared a course lab assignment based on the lectures and evaluated results
- Advised students on open-ended course projects

Sabanci University, EE Department

Teaching Assistant

Undergraduate Courses: *ENS 203: Electronic Circuits I, EE 310: Hardware Description*

2008–2010

Languages, EE 302: Digital Integrated Circuits

(Istanbul, Turkey)

- Performed teaching assistant activities at three undergraduate courses on electronics engineering
- Taught classes at recitations and led lab sessions
- Helped course material and exam preparations, graded coursework

Curriculum Development

ECE 592: Hardware Security and Cryptographic Engineering

Fall 2018–2024

Introduced a course on my research topics of hardware security that teaches how to establish trust in hardware. This is the first course ever focusing on quantum-secure cryptographic hardware design. The content include both theoretical basis and practical/hands-on experiments. Offered to senior undergraduate and graduate students. The course so far trained 67 students. Published a peer-reviewed paper on how to organize and effectively execute this course with hands-on experiments, which won the **best paper award** at GLS-VLSI 2019 conference.

The course received 4.3 score (averaged) from ClassEval. Below is an excerpt from a student's feedback: "*ECE 592 080 is an amazing course and it covered a wide range of topics pertaining to Hardware Security and Cryptography. The assignments were extremely well crafted and it has given the insights of what possible future hold for this rapidly rising field of security. Prof. Aysu has made this course even more interesting. He always makes the students push their horizons and achieve new levels of understanding. He always provides real time information about the topics and makes use delve into the subject even more.*"

ECE 212: Fundamentals of Logic Design

Spring 2019, Spring 2021–2024

This course focuses on digital circuit design fundamentals and is intended for sophomore undergraduates. The course has a diverse participant demographics and attracts students from electrical, mechanical, industrial, biomedical, and computer engineering. Adapted the course with new materials and also to an online context for remote learning during COVID-19. The course attracts around 150 students on average at each offering.

The course received 4.6 score (averaged) from ClassEval. Below is an excerpt from a student's feedback: *"Dr Aysu's teaching style made new concepts simple and easy to understand. Unlike other classes where I would simply memorize the process to find an answer, I felt like i genuinely understood the concepts I was working with and could apply them to real projects in the future. The homeworks were also well paced and did a good job of covering most aspects of what was covered in the previous week. All of this meant preparing for exams took little more than a bit of light review to be prepared. Perhaps most importantly for a professor however, Dr. Aysu has opened my eyes to a new career field that I wouldn't have ever considered otherwise. His genuine enthusiasm for the course matter and the insight he has brought to us about working in the career field has inspired me to look into finding work in the field of digital logic circuit design."*

Mentoring Activities

PhD Committee Chair

Anuj Dubey (2018–2023)
Emre Karabulut (2020–2024)
Furkan Aydin (2019–2024)
Priyank Kashyap (2022–2024)
Arsalan Malik (2022–present)
Ashley Kurian (2022–present)
Digvijay Anand (2022–present)
Rahul Magesh (2023–present)
Zinedine Hamoudi (2023–present)
Jinyu (Steve) Qui (2024–present)
Modini Ayyagari (2024–present)
Sharath Pendyala (2024–present)
Dasiy Kiptoo (2024–present)
Harshvadhan Mahir (2024–present)
John McFarland (2024–present)
Riddhi Khauta (2024–present)

PhD Committee Member

Terrence O'Connor (2018–2019)
Albert Gorski (2019–2020)
Luis Francisco (2020–2021)
Ge Li (2020–2022)
Billy Huggins (2021–2021)
Zachary Johnston (2021–present)
Archit Gajjar (2021–present)
Samin Yaseer Mahmud (2022–present)
Xijing Han (2022–2024)

MSc Committee Chair

Gregor Haas (2019–2021)
Aleesha Jiwani (2024–present)

MSc Committee Member

Paritosh Gaiwak (2019–2020)
Michael D'Argenio (2020–2021)

Post-Doctoral Advisor

Seetal Potluri (2019–present)

Undergraduate Advisor: NSF REU Berra Kara (2019)
Devin Whitmore (2019)
Sara Thornton (2019)
Zainab Alqatari (2019)
Timothy Boushell (2020)
Ashley Calhoun (2021)
Selena Jimenez (2021)
Erick Ortega (2021)
Michel Ibeto (2021)
Jullianna Eckard (2021)
John Wesley Cowand, IV (2022, 2023)
Bryan Wilson (2022)
Sky Kanoy (2023)
Niraj Patel (2023)
John Buchanan (2023, 2024)
Aydin Atasoy (2024)
Ethan Cornett (2024)

K-12 Advisor: Qubit x Qubit Esha Telang (2023)

Undergraduate Advisor: GEARS Qinhan Tan (2019)
Yitong Zhou (2020)

Publication List

Google Scholar profile: <https://scholar.google.com/citations?user=gkE2qn4AAAAJ&hl=en>

24 journal articles, **55** conference proceedings, **2** theses, and **1** patent.

Students and post-docs advised are marked with the * symbol.

Journal Articles

- [1] Qiu, Jinyi*, and **Aydin Aysu**. "SHIFT SNARE: Uncovering Secret Keys in FALCON via Single-Trace Analysis." IACR Transactions on Cryptographic Hardware and Embedded Systems – submitted.
- [2] Kurian, Ashley*, Anuj Dubey*, Ferhat Yaman*, and **Aydin Aysu**. "TPUExtract: An Exhaustive Hyperparameter Extraction Framework." IACR Transactions on Cryptographic Hardware and Embedded Systems 2025, no. 1 (2025): 78-103.
- [3] Martin, A., Kiptoo, D.J. *, Kanoy, D.S., Li, S., Du, C., Kumar, M., Pauls, A., Pathak, S., Bogdan, P., **Aydin Aysu** and Thuo, M. "Timed Physical Password or Authentication Keys." ACS Applied Materials & Interfaces 17, no. 25 (2025): 37257-37267.
- [4] Karabulut, Emre*, Arsalan Ali Malik*, Amro Awad, and **Aydin Aysu**. "THEMIS: Time, Heterogeneity, and Energy Minded Scheduling for Fair Multi-Tenant Use in FPGAs." IEEE Transactions on Computers (2025).
- [5] Gajjar, Archit, Priyank Kashyap*, **Aydin Aysu**, Paul Franzon, Yongjin Choi, Chris Cheng, Giacomo Pedretti, and Jim Ignowski. "RD-FAXID: Ransomware Detection with FPGA-Accelerated XGBoost." ACM Transactions on Reconfigurable Technology and Systems 17, no. 4 (2024): 1-33.
- [6] Karabulut, Emre*, and **Aydin Aysu**. "Masking FALCON's Floating-Point Multiplication in Hardware." IACR Transactions on Cryptographic Hardware and Embedded Systems 2024, no. 4 (2024): 483-508.
- [7] Malik, Arsalan Ali*, Emre Karabulut*, Amro Awad, and **Aydin Aysu**. "Enabling Secure and Efficient Sharing of Accelerators in Expeditionary Systems." Journal of Hardware and Systems Security (2024): 1-19.
- [8] Aydin, Furkan*, and **Aydin Aysu**. "Leaking secrets in homomorphic encryption with side-channel attacks." Journal of Cryptographic Engineering (2024): 1-11.

- [9] **Aysu, Aydin** and Scott Graham, "Introduction to the Special Issue on the Digital Threats of Hardware Security", ACM Digital Threats: Research and Practice Journal, *pre-published*, March 2023.
- [10] *Potluri, Seetal**, Shamik Kundu, Akash Kumar, Kanad Basu, **Aydin Aysu**. "SeqL+: Secure Scan-Obfuscation with Theoretical and Empirical Validation" IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD) 42, no 5. (2022): 1406-1410.
- [11] **Aysu, Aydin**, Xu Chen, W. Rhett Davis, Sung Kyu Lim, Paul Franzon, Madhavan Swaminathan, and Elyse Rosenbaum, "Better Performance, Higher Reliability, More Security: Research Highlights from the Center for Advanced Electronics through Machine Learning", Electronic Device Failure Analysis 24, no. 2, (2022)
- [12] *Dubey, Anuj**, Afzal Ahmad, Adeel Pasha, Rosario Cammarota, **Aydin Aysu**. "ModuloNET: Neural Networks Meet Modular Arithmetic for Efficient Hardware Masking" Transactions on Cryptographic Hardware and Embedded Systems (TCHES), no 1. (2022): 506-556 — **Nominated for Best Paper Award**
- [13] *Dubey, Anuj**, Rosario Cammarota, Vikram Suresh, and **Aydin Aysu**. "Guarding machine learning hardware against physical side-channel attacks." ACM Journal on Emerging Technologies in Computing Systems (JETC) 18, no. 3 (2022): 1-31.
- [14] *Karabulut, Emre**, Erdem Alkim, and **Aydin Aysu**. "Efficient, flexible, and constant-time gaussian sampling hardware for lattice cryptography." IEEE Transactions on Computers 71, no. 8 (2021): 1810-1823.
- [15] *Aydin, Furkan**, **Aydin Aysu**, Mohit Tiwari, Andreas Gerstlauer, and Michael Orshansky. "Horizontal Side-Channel Vulnerabilities of Post-Quantum Key Exchange and Encapsulation Protocols." ACM Transactions on Embedded Computing Systems (TECS) 20, no. 6 (2021): 1-22.
- [16] *Kashyap, Priyank**, *Furkan Aydin**, *Seetal Potluri**, Paul D. Franzon, and **Aydin Aysu**. "2Deep: Enhancing Side-Channel Attacks on Lattice-Based Key-Exchange via 2-D Deep Learning." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 40, no. 6 (2020): 1217-1229.
- [17] *Mert, Ahmet Can**, *Emre Karabulut**, Erdinç Öztürk, Erkan Savaş, and **Aydin Aysu**. "An extensive study of flexible design methods for the number theoretic transform." IEEE Transactions on Computers 71, no. 11 (2020): 2829-2843.
- [18] Ozcan, Erdem, and **Aydin Aysu**. "High-Level-Synthesis of Number-Theoretic Transform: A Case Study for Future Cryptosystems." IEEE Embedded Systems Letters (2019).
- [19] **Aysu, Aydin**, Ege Gulcan, Daisuke Moriyama, and Patrick Schaumont. "Compact and low-power ASIP design for lightweight PUF-based authentication protocols." IET Information Security 10, no. 5 (2016): 232-241.
- [20] **Aysu, Aydin**, and Patrick Schaumont. "Precomputation methods for hash-based signatures on energy-harvesting platforms." IEEE Transactions on Computers (TC) 65, no. 9 (2016): 2925-2931.
- [21] **Aysu, Aydin**, and Patrick Schaumont. "Hardware/software co-design of physical unclonable function based authentications on FPGAs." Elsevier Microprocessors and Microsystems (MICPRO) 39, no. 7 (2015): 589-597.
- [22] **Aysu, Aydin**, Bilgiday Yuce, and Patrick Schaumont. "The future of real-time security: Latency-optimized lattice-based digital signatures." ACM Transactions on Embedded Computing Systems (TECS) 14, no. 3 (2015): 43, 1-18.
- [23] **Aysu, Aydin**, Ege Gulcan, and Patrick Schaumont. "SIMON says: Break area records of block ciphers on FPGAs." IEEE Embedded Systems Letters (ESL) 6, no. 2 (2014): 37-40. *Top 50 Popular Article*
- [24] **Aysu, Aydin**, Gokhan Sayilar, and Ilker Hamzaoglu. "A low energy adaptive hardware for H. 264 multiple reference frame motion estimation." IEEE Transactions on Consumer Electronics (TCE) 57, no. 3 (2011): 1377-1383.

Peer-Reviewed Conference and Workshop Proceedings

- [25] *Malik, Arsalan Ali**, *Harshvadan Mihir**, and **Aydin Aysu**. "Craft: Characterizing and root-causing fault injection threats at pre-silicon." IEEE International Symposium on Hardware Oriented Security and Trust (HOST) – submitted.
- [26] O’Gara, Aidan, Gabriel Kulp, Will Hodgkins, James Petrie, Vincent Immler, **Aydin Aysu**, Kanad Basu, Shivam Bhasin, Stjepan Picek, and Ankur Srivastava. "Hardware-Enabled Mechanisms for Verifying Responsible AI Development." International Conference on Machine Learning (ICML) (2025) – accepted.

- [27] *Dubey, Anuj** and **Aydin Aysu**. "Stochastic Training for Side-Channel Resilient AI" In EdgeAI Foundation Summit, Austin, TX, 2025 – accepted.
- [28] *Magesh, Rahul**, *Sharath Pendyala**, *Modini Ayyagari**, **Aydin Aysu**. "A Comparison of Unified Multiplier Designs for the FALCON Post-Quantum Digital Signature" In Lightweight Cryptography for Security & Privacy (LightSec). 2025 – accepted.
- [29] Schmid, Martin, Giuseppe Manzoni, **Aydin Aysu** and Elif Bilge Kavun. "A Comparison of Unified Multiplier Designs for the FALCON Post-Quantum Digital Signature" In 2025 IEEE/ACM International Conference On Computer Aided Design (ICCAD), 2025 – accepted.
- [30] Lu, Chao, *Esha Telang**, **Aydin Aysu**, and Kanad Basu. "Quantum leak: Timing side-channel attacks on cloud-based quantum services." In Proceedings of the Great Lakes Symposium on VLSI 2025, pp. 252-257. 2025.
- [31] *Aydin, Furkan**, *Emre Karabulut**, and **Aydin Aysu**. "Pre-Silicon Side-Channel Analysis of AI/ML Systems." In 2024 IEEE Physical Assurance and Inspection of Electronics (PAINE), pp. 1-7. IEEE, 2024.
- [32] *Karabulut, Emre**, and **Aydin Aysu**. "A hardware-software co-design for the discrete gaussian sampling of falcon digital signature." In 2024 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 90-100. IEEE, 2024.
- [33] *Aydin, Furkan**, *Emre Karabulut**, and **Aydin Aysu**. "Pre-Silicon Vulnerability Assessment for AI/ML Hardware." In Proceedings of the Great Lakes Symposium on VLSI 2024, pp. 495-495. 2024.
- [34] *Dubey, Anuj**, and **Aydin Aysu**. "A Full-Stack Approach for Side-Channel Secure ML Hardware." In 2023 IEEE International Test Conference (ITC), pp. 186-195. IEEE, 2023.
- [35] Mert, Ahmet Can, Ferhat Yaman, *Emre Karabulut**, Erdinc Ozturk, Erkey Savas, and **Aydin Aysu**. "A Survey of Software Implementations for the Number Theoretic Transform." In International Conference on Embedded Computer Systems (SAMOS). 2023.
- [36] *Karabulut, Emre**, Amro Awad, and **Aydin Aysu**. "SS-AXI: Secure and Safe Access Control Mechanism for Multi-Tenant Cloud FPGAs", In 2023 IEEE International Symposium on Circuits and Systems (ISCAS), accepted, IEEE, 2023.
- [37] *Dubey, Anuj**, Rosario Cammarota, Avinash Varna, Raghavan Kumar, and **Aydin Aysu**. "Hardware-Software Co-design for Side-Channel Protected Neural Network Inference." In 2023 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 155-166. IEEE, 2023.
- [38] **Aysu, Aydin**. "Multi-Tenant Cloud FPGAs: Side-Channel Security and Safety." In Proceedings of the 2022 on Cloud Computing Security Workshop, pp. 7-8. 2022.
- [39] *Aydin, Furkan**, and **Aydin Aysu**. "Exposing Side-Channel Leakage of SEAL Homomorphic Encryption Library." In Proceedings of the 2022 Workshop on Attacks and Solutions in Hardware Security, pp. 95-100. 2022.
- [40] *Karabulut, Emre**, *Chandu Yuvarajappa**, *Mohammed Iliyas Shaik**, *Seetal Potluri**, Amro Awad, and **Aydin Aysu**. "PR Crisis: Analyzing and Fixing Partial Reconfiguration in Multi-Tenant Cloud FPGAs." In Proceedings of the 2022 Workshop on Attacks and Solutions in Hardware Security, pp. 101-106. 2022.
- [41] Sayadi, Hossein, Mehrdad Aliasgari, *Furkan Aydin**, *Seetal Potluri**, **Aydin Aysu**, Jack Edmonds, and Sara Tehranipoor. "Towards AI-Enabled Hardware Security: Challenges and Opportunities." In 2022 IEEE 28th International Symposium on On-Line Testing and Robust System Design (IOLTS), pp. 1-10. IEEE, 2022.
- [42] *Haas, Gregor** and **Aydin Aysu**. "Apple vs EMA: Electromagnetic Side-Channel Attacks on Apple CoreCrypto" Design Automation Conference (DAC), pp. 247-252. 2022 — **Won Publicity Paper Award**
- [43] *Calhoun, Ashley**, *Erick Ortega**, *Ferhat Yaman**, *Anuj Dubey**, and **Aydin Aysu**. "Hands-On Teaching of Hardware Security for Machine Learning." In Proceedings of the Great Lakes Symposium on VLSI 2022, pp. 455-461. 2022.
- [44] Gajjar, Archit, *Priyank Kashyap**, **Aydin Aysu**, Paul Franzon, Sumon Dey, and Chris Cheng. "FAXID: FPGA-Accelerated XGBoost Inference for Data Centers using HLS." In 2022 IEEE 30th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM), pp. 1-9. IEEE, 2022.

- [45] *Dubey, Anuj**, *Emre Karabulut**, Amro Awad, **Aydin Aysu**. “High-Fidelity Model Extraction Attacks via Remote Power Monitors” IEEE International Conference on Artificial Intelligence Circuits and Systems (AICAS), pp. 328-331. IEEE, 2022.
- [46] *Aydin, Furkan**, *Emre Karabulut**, *Seetal Potluri**, Erdem Alkim and **Aydin Aysu**. “RevEAL: Single-Trace Side-Channel Leakage of the SEAL Homomorphic Encryption Library.” Design, Automation & Test in Europe Conference & Exhibition (DATE), 2022 — Accepted
- [47] *Karabulut, Emre**, and **Aydin Aysu**. “Falcon Down: Breaking Falcon Post-Quantum Signature Scheme through Side-Channel Attacks.” In 2021 58th ACM/IEEE Design Automation Conference (DAC), pp. 691-696. IEEE, 2021.
- [48] *Karabulut, Emre**, Erdem Alkim, and **Aydin Aysu**. “Single-Trace Side-Channel Attacks on ω -Small Polynomial Sampling.” Hardware Oriented Security and Trust (HOST), 2021
- [49] *Haas, Gregor**, *Seetal Potluri**, **Aydin Aysu**. “iTimed: Cache Attacks on the Apple A10 Fusion SoC.” Hardware Oriented Security and Trust (HOST), 2021 – **Best Paper Recognition Award**
- [50] Chen, Zhaohui, *Emre Karabulut**, **Aydin Aysu**, Yuan Ma, and Jiwu Jing. “An Efficient Non-Profiled Side-Channel Attack on the CRYSTALS-Dilithium Post-Quantum Signature.” In 2021 IEEE 39th International Conference on Computer Design (ICCD), pp. 583-590. IEEE, 2021.
- [51] *Potluri, Seetal**, **Aydin Aysu** “Stealing Neural Network Models through the Scan Chain: A New Threat for ML Hardware.” In 2020 IEEE/ACM International Conference On Computer Aided Design (ICCAD), 2021
- [52] *Mert, Ahmet Can**, *Emre Karabulut**, Erdinç Öztürk, Erkan Savaş, Michela Becchi, and **Aydin Aysu**. “A flexible and scalable NTT Hardware: applications from homomorphically encrypted deep learning to post-quantum cryptography.” In 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 346-351. IEEE, 2020. — **Best Paper Award**
- [53] *Dubey, Anuj**, Rosario Cammarota, and **Aydin Aysu**. “BoMaNet: boolean masking of an entire neural network.” In 2020 IEEE/ACM International Conference On Computer Aided Design (ICCAD), pp. 1-9. IEEE, 2020.
- [54] Regazzoni, Francesco, Shivam Bhasin, Amir Ali Pour, Ihab Alshaer, *Furkan Aydin**, **Aydin Aysu**, Vincent Beroulle et al. “Machine Learning and Hardware security: Challenges and Opportunities.” In 2020 IEEE/ACM International Conference On Computer Aided Design (ICCAD), pp. 1-6. IEEE, 2020.
- [55] *Karabulut, Emre**, and **Aydin Aysu**. “RANTT: A RISC-V Architecture Extension for the Number Theoretic Transform.” In 2020 30th International Conference on Field-Programmable Logic and Applications (FPL), pp. 26-32. IEEE, 2020.
- [56] *Aydin, Furkan**, *Priyank Kashyap**, *Seetal Potluri**, Paul Franzon, and **Aydin Aysu**. “DeePar-SCA: Breaking Parallel Architectures of Lattice Cryptography via Learning Based Side-Channel Attacks.” In International Conference on Embedded Computer Systems, pp. 262-280. Springer, Cham, 2020.
- [57] *Potluri, Seetal**, **Aydin Aysu**, and Akash Kumar. “SeqI: Secure scan-locking for ip protection.” In 2020 21st International Symposium on Quality Electronic Design (ISQED), pp. 7-13. IEEE, 2020.
- [58] *Tan, Qinhan**, *Seetal Potluri**, and **Aydin Aysu**. “Efficacy of Satisfiability-Based Attacks in the Presence of Circuit Reverse-Engineering Errors.” In 2020 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1-5. IEEE, 2020.
- [59] *Dubey, Anuj**, Rosario Cammarota, and **Aydin Aysu**. “Maskednet: The first hardware inference engine aiming power side-channel protection.” In 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 197-208. IEEE, 2020.
- [60] **Aydin Aysu**. “Teaching the Next-Generation of Cryptographic Hardware Design to the Next-Generation of Engineers” ACM Great Lakes Symposium on VLSI (GLSVLSI), pp. 237-242. ACM, 2019 — **Best Paper Award**
- [61] Wei, Shijia, **Aysu, Aydin**, Michael Orshansky, Andreas Gerstlauer, and Mohit Tiwari. “Using Power-Anomalies to Counter Evasive Micro-Architectural Attacks in Embedded Systems.” International Symposium on Hardware Oriented Security and Trust (HOST), pp. 111-120, 2019 — **Nominated for Best Paper Award**
- [62] **Aysu, Aydin**, Youssef Tobah, Michael Orshansky, Andreas Gerstlauer, Mohit Tiwari. “Horizontal side-channel vulnerabilities of post-quantum key exchange protocols.” In 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 81-88. IEEE, 2018 — **Nominated for Best Paper Award — Won Top Picks in Hardware and Embedded Security 2015--2020**

- [63] Xi, Xiaodan, **Aydin Aysu**, Michael Orshansky. "Fresh re-keying with strong PUFs: A new approach to side-channel security." In 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 118-125. IEEE, 2018.
- [64] **Aysu, Aydin**, Michael Orshansky, and Mohit Tiwari. "Binary Ring-LWE hardware with power side-channel countermeasures." In 2018 Design, Automation Test in Europe Conference Exhibition (DATE), pp. 1253-1258. IEEE, 2018.
- [65] **Aysu, Aydin**, Ye Wang, Patrick Schaumont, and Michael Orshansky. "A new maskless debiasing method for lightweight physical unclonable functions." In Hardware Oriented Security and Trust (HOST), 2017 IEEE International Symposium on, pp. 134-139. IEEE, 2017.
- [66] Huth, Christopher, **Aydin Aysu**, Jorge Guajardo, Paul Duplys, and Tim Güneysu. "Secure and private, yet lightweight, authentication for the IoT via PUF and CBKA." In International Conference on Information Security and Cryptology (ICISC), pp. 28-48. Springer, Cham, 2016.
- [67] **Aysu, Aydin**, Shravya Gaddam, Harsha Mandadi, Carol Pinto, Luke Wegryn, and Patrick Schaumont. "A design method for remote integrity checking of complex PCBs." In Design, Automation & Test in Europe Conference & Exhibition (DATE), 2016, pp. 1517-1522. IEEE, 2016.
- [68] **Aysu, Aydin**, Ege Gulcan, Daisuke Moriyama, Patrick Schaumont, and Moti Yung. "End-to-end design of a PUF-based privacy preserving authentication protocol." In International Workshop on Cryptographic Hardware and Embedded Systems (CHES), pp. 556-576. Springer, Berlin, Heidelberg, 2015.
- [69] Gulcan, Ege, **Aydin Aysu**, and Patrick Schaumont. "BitCryptor: Bit-serialized flexible crypto engine for lightweight applications." In International Conference in Cryptology in India (IndoCrypt), pp. 329-346. Springer, Cham, 2015.
- [70] Gulcan, Ege, **Aydin Aysu**, and Patrick Schaumont. "A flexible and compact hardware architecture for the SIMON block cipher." In International Workshop on Lightweight Cryptography for Security and Privacy (LightSec), pp. 34-50. Springer, Cham, 2014.
- [71] Ghalaty, Nahid Farhady, **Aydin Aysu**, and Patrick Schaumont. "Analyzing and eliminating the causes of fault sensitivity analysis." In Proceedings of the conference on Design, Automation & Test in Europe (DATE), pp. 204-209. European Design and Automation Association, 2014.
- [72] Hamzaoglu, Ilker, **Aydin Aysu**, and Onur Can Ulusel. "A low power adaptive H. 264 video encoder hardware." In Consumer Electronics-Berlin (ICCE-Berlin), 2014 IEEE Fourth International Conference on, pp. 395-399. IEEE, 2014.
- [73] **Aysu, Aydin**, and Patrick Schaumont. "PASC: Physically authenticated stable-clocked soc platform on low-cost FPGAs." In Reconfigurable Computing and FPGAs (ReConFig), 2013 International Conference on, pp. 1-6. IEEE, 2013.
- [74] Schaumont, Patrick, and **Aydin Aysu**. "Three design dimensions of secure embedded systems." In International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE), pp. 1-20. Springer, Berlin, Heidelberg, 2013.
- [75] **Aysu, Aydin**, Nahid Farhady Ghalaty, Zane Franklin, Moein Pahlavan Yali, and Patrick Schaumont. "Digital fingerprints for low-cost platforms using MEMS sensors." In Proceedings of the Workshop on Embedded Systems Security (WESS), p. 2: 1-6. ACM, 2013.
- [76] **Aysu, Aydin**, Cameron Patterson, and Patrick Schaumont. "Low-cost and area-efficient FPGA implementations of lattice-based cryptography." In Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on, pp. 81-86. IEEE, 2013.
- [77] **Aysu, Aydin**, Murat Sayinta, and Cevahir Cigla. "Low cost FPGA design and implementation of a stereo matching system for 3D-TV applications." In Very Large Scale Integration (VLSI-SoC), 2013 IFIP/IEEE 21st International Conference on, pp. 204-209. IEEE, 2013.
- [78] Hamzaoglu, Ilker, **Aydin Aysu**, and Onur Can Ulusel. "A reconfigurable H. 264 video encoder hardware." In Signal Processing and Communications Applications (SIU), 2011 IEEE 19th Conference on, pp. 984-987. IEEE, 2011.

- [79] Akin, Abdulkadir, **Aydin Aysu**, Onur Can Ulusel, and Erkey Savaş. "Efficient hardware implementations of high throughput SHA-3 candidates keccak, luffa and blue midnight wish for single-and multi-message hashing." In Proceedings of the 3rd International Conference on Security of Information and Networks (SIN), pp. 168-177. ACM, 2010.

Patent

- [80] **Aysu, Aydin**, Dubey Anuj. "SIDE-CHANNEL AWARE TRAINING FOR COMMERCIAL MACHINE LEARNING ACCELERATORS" 18/950,948, submitted, Nov 24.
- [81] Guo, Xu, **Aydin Aysu**. "Security protocols for unified near field communication infrastructures." United States patent US 9497573 B2, Granted 2016, Nov 15.

Theses

- [82] **Aydin Aysu**. "Resource-constrained and resource-efficient modern cryptosystem design." Doctoral Dissertation, Virginia Polytechnic Institute and State University, 2016.
- [83] **Aydin Aysu**. "A baseline H.264 video encoder hardware design" Master Thesis, Sabanci University, 2010.

News Coverage of Research

TCHES 2025: TPUXtract: An Exhaustive Hyperparameter Extraction Framework.

2025

My TCHES 2025 research paper has been publicized through NC State news release and has subsequently been featured at The Register, Gizmodo, London Tribune, and Dark Reading among other places. We were interviewed by the cybersecurity news site Gizmodo and Dark Reading, and the interview was published online along with the news coverage.

DATE 2022: RevEAL: Single-Trace Side-Channel Leakage of the SEAL Homomorphic Encryption Library.

2022

My DATE 2022 research paper has been publicized through NC State news release and has subsequently been featured at Hacker News, CSO Online, and The Digital Hacker among other places. I was interviewed by the cybersecurity news site Dark Reading and the interview was published online along with the news coverage.

HOST 2021: iTimed: Cache Attacks on the Apple A10 Fusion SoC.

2021

My HOST 2021 research paper has been publicized through NC State news release and has subsequently been featured at several news agencies including The Register and WRAL TechWire. I was interviewed by CBS Raleigh and the interview was published on live TV (CBS 17) as part of Wake County News.

HOST 2020: MaskedNET: The First Hardware Inference Engine Aiming Power Side-Channel Protection.

2020

My HOST 2020 research paper has been featured at the IEEE Spectrum magazine. I was interviewed by Jeremy Hsu and the interview along with a summary of the paper has been printed at the magazine volume and published online.

GLS-VLSI 2019: Teaching the Next-Generation of Cryptographic Hardware Design.

2019

My special topics graduate course focusing on post-quantum cryptography and my paper about the course has been publicized through NC State news release and has subsequently been featured at the ACM Communications magazine. I was also interviewed for this published piece on "Future-proofing Security for the Coming Quantum Era" by ACM.

HOST 2019: Horizontal Side-channel Vulnerabilities of Post-Quantum Key-Exchange Protocols.

2019

My HOST 2019 research paper has been publicized through NC State news release and has subsequently been featured at several news agencies such as NSF's Science360, The Engineer, Military Embedded Systems, and Science Daily, among others. The news has been translated into German, Chinese, and Turkish. The Tech Briefs magazine interviewed me about this research and published the interview in their July 2019 edition.

Membership

Senior Member

IEEE – Institute of Electrical and Electronics Engineers (since 2019)

Invited Talks and Presentations

Deus Ex LLMs: AI vs Humans in Post-Quantum Cryptographic Hardware Code Generation Invited Talk at AICAD4Sec Workshop 2025	2025
Hardware Security Research for Mission-Critical Systems Invited Talk for MC Dean	2025
TPUXtract: A Comprehensive Hyperparameter Stealing Framework Keysight Device Security Workshop	2025
FALCON STRIKE: Breaking the Emerging Post-Quantum Standard with a Side-Channel Attack Invited Talk at GomacTech (Government Microcircuit Applications & Critical Technology Conference)	2025
Honest to a Fault: Root-Causing Fault Attacks with Pre-Silicon RISC Pipeline Characterization Invited Talk at GomacTech (Government Microcircuit Applications & Critical Technology Conference)	2025
TPUXtract: A Comprehensive Hyperparameter Stealing Framework on Edge TPUs Invited Talk at GomacTech (Government Microcircuit Applications & Critical Technology Conference)	2025
Stealing Lattice Secrets from Hardware Invited Talk at National Science Foundation HWiQ Workshop	2025
Untrusted Silicon, Untrusted AI Invited Talk at the Foresight Vision Weekend Puerto Rico	2025
Stealing Secrets from Edge AI Devices Invited Talk at the Edge AI Foundation	2025
How to Use GPT in Academic Writing for Computer Engineering Invited lecture at the NCSU ECE Graduate Student Orientation	2024
Side-Channel Analysis and the Future Invited talk at University of Idaho	2024
Hardware Security and the Future: Why Should You Care? Invited talk at ECE Friday Colloquium at NCSU	2024
Pre-Silicon Vulnerability Assessment of AI/ML Hardware Invited Talk at GLS-VLSI Special Session on Hardware Security	2024
Securing Neural Network Hardware Against Side-Channel Attacks Invited Talk at Qualcomm Product Security Summit	2024
Emerging Security Challenges at the Junction of AI and Hardware Keynote at IEEE Microelectronics Design & Test Symposium (MDTS)	2024
The Third Decade of Physical Side-Channel Analysis Distinguished Lecture Series, I-SENSE, Florida Atlantic University	2024
A Full Stack Solution for Edge AI Invited Talk at the New England Hardware Security Day	2024
Securing Floating Point Side-Channels Invited Talk at GomacTech (Government Microcircuit Applications & Critical Technology Conference)	2024
Defenser: A Complete Solution to Secure Multi-Tenant FPGAs Invited Talk at GomacTech (Government Microcircuit Applications & Critical Technology Conference)	2024
A Pre-Silicon Vulnerability Analysis Tool for Edge AI Invited Talk at GomacTech (Government Microcircuit Applications & Critical Technology Conference)	2024
Physical Side-Channel Analysis and the Future: Why Should You Care? Webinar at CAEML IUCRC	2024

Emerging Topics in Secure Intelligent Devices Invited talk at the University of Passau, Germany	2023
Emerging Threats on AI/ML Hardware Invited talk at US-UK Security in the Era of Global Semiconductor Initiatives	2023
IEEE Council of Electronic Design Automation Panelist at AI Hardware Security	2023
Privacy and Post-Quantum Cryptography Invited Lecture at Privacy Enhancing Technologies Course (Bilgi University)	2023
Secure AI Hardware By Design: From Cryptographic Proofs to Silicon Tapeout Invited Talk at GomacTech (Government Microcircuit Applications & Critical Technology Conference)	2023
Building and Breaking Post-Quantum Cryptography Hardware Invited Talk at NIST Crypto Reading Club	2023
The Next Decade of Cryptographic Engineering: Post-Quantum Cryptography Keynote at DesignCon'23	2023
The Future of Physical Side-channel Analysis: the Next Decade Invited Talk at NSA Center of Academic Excellence	2023
Falcon Down: Breaking Falcon Post-Quantum Signature Scheme through Side-Channel Attacks Invited Talk at NIST 4th Workshop on Post-Quantum Cryptography Standardization	2022
Multi-Tenant Cloud FPGAs: Security and Safety Risks Keynote at the ACM Cloud Computing Security Workshop (CCSW)	2022
Machine Learning for Side-Channel Security Assessment of Next-Generation Cryptosystems Invited Talk at Special Session on AI-Enabled Security at IOLTS'22	2022
Machine Learning and Side-Channel Analysis: The Path Forward Invited Talk at Ansys Inc.	2022
Learning Based Techniques for Breakthrough in Side-Channel Security Assessment CAEML Workshop on Machine Learning for Hardware Design and Optimization	2022
Embedded Digital RFID for Chip Asset Tracking Symposium on Counterfeit Parts and Materials	2022
Physical Side-Channel Leakage Analysis of Edge Tensor Processing Units Invited Talk at Google Inc.	2022
Securing Edge AI Devices Against Side-Channel Attacks with Hardware Masking Workshop on Security for Custom Computing Machines	2022
Machine Learning and Side-Channel Analysis: What Did We Learn? Intel IPAS Tech Sharing Talk	2022
Breaking and Securing Lattice-Based Post-Quantum Cryptography against Side-Channels Aselsan Corporation 3rd Annual Workshop on Post-Quantum Cryptography (In Turkish)	2022
Securing Neural Networks Against Side-Channel Attacks with Hardware Masking Florida Institute for Cybersecurity Research Webinar	2022
SeqL: Scan-Chain Locking and a Broad Security Evaluation Seminar at the IEEE CEDA CAD for Assurance	2021
Hardware Masking for Neural Network Side-Channel Mitigation Seminar at Semiconductor Research Corporation e-Workshop	2021
Horizontal Side-Channel Vulnerabilities of Post-Quantum Key-Exchange Protocols Invited talk at 2021 Hardware and Embedded Security Top Picks	2021
Scan Chain attacks on Neural Networks Invited talk at Trustworthy and Reliable AI accelerator design (TRAIN) – Embedded Systems Week 2021	2021

Machine Learning and Side-Channel Analysis: Happily Ever After or Bitter Divorce? Seminar at Villanova University	2021
Stealing Neural Network Models through the Scan Chain: A New Threat for ML Hardware Invited talk at Virtual Workshop on Machine Learning & Hardware Security 2021 (MIHWSEC)	2021
The Future of Physical Side-Channel Analysis: The Next Decade "Future of Cryptographic Engineering" Webinar	2021
Machine Learning and Side-Channel Analysis: How Do They Couple? Invited Talk at Sabanci University	2021
Deus Ex Machina: Learning Techniques for Breakthrough in Side-Channel Assessment of Circuits Seminar to the NSF/IUCRC Center of Advanced Electronic for Machine Learning (CAEML)	2021
Deep Learning Attacks on Post-Quantum Hardware Invited talk at IEEE International Conference on Computer-Aided Design (ICCAD),	2020
Reverse Engineering Neural Networks: The Hard(ware) Way Seminar Talk at Worcester Polytechnic Institute (WPI), IEEE International Conference on Physical Assurance and Inspection of Electronics (PAINE), and Riscure Inc. Hybrid Workshop	2020
Deep-Learning Based Side-Channel Attacks Seminar to the NSF/IUCRC Center of Advanced Electronic for Machine Learning (CAEML)	2019
Pushing Physical Side-Channels Beyond Cryptography Seminar talk at UC San Diego for the Security for Custom Computing Machines Workshop	2019
Mission Impossible 7: Securing the IoT Landscape Gave a video-lecture at Bogazici University as part of CmpE490: Internet of Things	2019
Hardware Security Research at NC State: Outreach to Turkey Seminar talk at Koc University, Bogazici University, Middle East Technical University, and Bilkent University	2018
Securing Cryptographic Systems Against Quantum Adversaries and Hardware Exploits Seminar talk at the University of Kentucky, University of Utah, North Carolina State University, Tufts University, University of New Mexico, George Mason University, and Arizona State University	2018
Side-Channel Analysis and Physical Unclonable Functions Guest lectures for ECE 382: Security at Hardware/Software Interface	2017
Weak vs. Strong PUFs: Which is Better for the Internet-of-Things? Poster presentation at the Cryptographic Hardware and Embedded Systems (CHES) conference	2016
Make PUFs Great Again! Presentation at Computer Aided Design and Implementation for Cryptography and Security Workshop	2016
Hardware Hacking with the Doubling Attack Guest lecture for ECE/CS 5580: Cryptographic Engineering	2016
Cryptoengineering the Future: Emerging Cryptographic Engineering Trends Poster presentation at CIESCA day 2015	2015
Renaissance of Precomputation in a Post-Quantum World Presentation at NIST Workshop on Cybersecurity in a Post-Quantum World	2015
Drilling the Embedded Pyramid: Design Dimensions for Secure Embedded Systems Received <i>Best Poster</i> award, poster presentation at CIESCA day 2014	2014
PUFs for the Internet-of-Things Security Research Presentation at Qualcomm Inc.	2014
A Tale of Two Schemes: Crypto Engineering for the Two Ends of Computing Spectrum Seminar talk at Virginia Tech and Sabanci University	2014
Welcome to the Future of Security: Lattice-Based Cryptography Received <i>Best Presentation</i> award, presentation at CIESCA day 2013	2013

A Method to Authenticate SoCs on Various FPGA Boards by Utilizing Process Variations

2013

Hardware demo and presentation at the Research Symposium on Embedded Security

Silicon Fingerprinting for Embedded Systems

2013

Poster presentation at DAC 2013 A. Richard Newton Young Forum

Academic Service

Reviewer and Panelist	National Science Foundation 2019–2025
Panel Moderator	Secure Packaging: Initiatives, Research, and Workforce Development; IEEE PAINE conference 2022
Proposal Reviewer	Army Research Office 2024, 2021 Dutch Research Council 2024, 2022 Maryland Industrial Partnerships Program 2022
Guest Editor	ACM DTRAP: Special Issue on the Digital Threats of Hardware Security 2020–2022 MDPI Cryptography Special Issue: Post-Quantum Cryptography: From Theoretical Foundations to Practical Deployments 2019–present
Award Committee	IEEE Top Picks in Hardware and Embedded Security 2022
Organizing Committee	IEEE PAINE conference'22'23 IEEE Hardware Oriented Security and Trust (HOST)'22'23'24'25
Technical Program Chair	IEEE Hardware Oriented Security and Trust (HOST)'25 Attacks and Solutions in Hardware Security (ASHES)'25 IEEE Physical Assurance and Inspection of Electronics (PAINE)'23
Track Chair	International Conference on Reconfigurable Computing and FPGAs (Reconfig)'18'19
Technical Program Committee	Cryptographic Hardware and Embedded Security (CHES)'25'24'23'22'21 Design Automation Conference (DAC)'22'21'20'19 Design, Automation and Test in Europe (DATE) '25'23'21'20'19'18 International Symposium Field-Programmable Gate Arrays (FPGA) '25'24'23'22'21'20'19 ACM ASIA Conference on Computer and Communications Security International Conference on Computer Design (ASIACCS)'22'21'20 Attacks and Solutions in Hardware Security (ASHES) '24'23'22'21 International Conference of Computer Design (ICCD) '25'24'23'22'21'20 International Conference on Computer Aided Design (ICCAD)'19'18'17 Architecture and Hardware for Security Applications (AHSA)'21'20'19'18'17 Hardware-Oriented Security and Trust (HOST) '25'24'23'22'21'20 Hardware and Architectural Support for Security and Privacy (HASP)'17 Malicious Software and Hardware in Internet of Things (Mal-IoT)'17 Emerging Technologies in Security and Privacy of Distributed, Grid and Cloud Computing Systems (ESP-DGC)'15

Reviewer – Journal

ACM Transactions on Architecture and Code Optimization (TACO)
ACM Journal on Emerging Technologies in Computing Systems (JETC)
IEEE Transactions on Computers (TC)
IEEE Transactions on Information Forensics and Security (TIFS)
IEEE Transactions on Computer-Aided Design (TCAD)
IEEE Transactions on Very Large Scale Integration Systems (VLSI)
IEEE Transactions on Circuits and System (TCAS)
IEEE Transactions on Emerging Topics in Computing (TETC)
IEEE Journal on Emerging and Selected Topics in Circuits and Systems (JETCAS)
IEEE Embedded System Letters (ESL)
Springer Journal on Cryptographic Engineering (JCEN)
Springer Journal of Hardware and Systems Security (HAAS)
Elsevier Journal of Microprocessors and Microsystems (MICPRO)
MDPI Journal of Cryptography
Oxford University Press The Computer Journal (COMPJ)

Reviewer – Conference

Cryptographic Hardware and Embedded Systems (CHES)'17'16'15'14'10
Design Automation Conference (DAC)'18'17'15
Design, Automation and Test in Europe (DATE)'16'15'14'13
Hardware-Oriented Security and Trust (HOST)'17'16'15'14'13
Asia and South Pacific Design Automation Conference (ASP-DAC)'16
IEEE Computer Society Annual Symposium on VLSI (ISVLSI)'16
Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE)'15
International Conference on Reconfigurable Computing (ReConFig)'14
International Workshop on Security (IWSEC)'13
International Conference of Computer Design (ICCD)'13
Lightweight Cryptography for Security & Privacy (LightSec)'13
Workshop on Embedded Systems Security (WESS)'13
Field-Programmable Logic and Applications (FPL)'10
Very Large Scale Integration (VLSI-SoC)'10