Aydin Aysu

Assistant Professor
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** *2012–2016*
Thesis: *Resource-Constrained and Resource-Efficient Modern Cryptosystem Design* Blacksburg, VA

M.Sc. in Electronics Engineering, **Sabanci University** *2008–2010*
Thesis: *A Baseline H.264 Video Encoder Hardware Design* Istanbul, Turkey

B.Sc. in Microelectronics Engineering with Mathematics Minor, **Sabanci University** *2004–2008*
Istanbul, Turkey

Honors and Awards

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
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)

Research Interests

Hardware-oriented cybersecurity: applied cryptography, computer architectures, and hardware security primitives

Funding Awarded

Total: $3,618,693; Personal Share: $2,534,257

National Security Agency, Co-PI, $150,000 2023–2024
GenCyberPack: Professional Development for Middle and High School Teachers on Cybersecurity

National Science Foundation, Sole PI, $339,842 2023–2026
SaTC: CORE: Small: An Automated Framework for Mitigating Single-Trace Side-Channel Leakage

Office of Naval Research, Sole PI, $489,044 2022–2025
Event Horizon: Hardware Security Emulators for Next-Generation Edge AI/ML

Google LLC, Sole PI, $60,000 2022–2023
Demonstrating and Mitigating Security Vulnerabilities of Edge Tensor Processing Units

Goodnight Early Career Innovator Award, Sole PI, $66,000 2022–2025
Early Career Award for Outstanding Research Contributions

National Science Foundation CCF, Sole PI, $199,780 2022–2024
SHF: Small: A New Approach for Hardware Design of High-Precision Discrete Gaussian Sampling

National Science Foundation PFI, Co-PI, $249,767 2022–2023
PFI-TT: Embedded Radio Frequency Identification (RFID) to secure the semiconductor supply chain

Office of Naval Research, co-PI, $799,930 2021–2024
Enabling Secure and Efficient Sharing of Accelerators in Expeditionary Systems

NSF I/UCRC: Center for Advanced Electronics through Machine Learning, PI, $101,000 2020–2022
ML-Based Security Analysis and Mitigation of Homomorphic Encryption Side-Channels

NCSU R. Ray Bennett Faculty Fellow Award, Sole PI, $40,000 2019–2020
High Achieving Untenured Young Faculty Award

National Science Foundation CAREER, Sole PI, $438,689 2020–2025
Physical Side-Channels Beyond Cryptography: Transforming the Side-Channel Framework for Deep Learning

NSF I/UCRC: Center for Advanced Electronics through Machine Learning, Co-PI, $123,728 2020–2021
FPGA Hardware Accelerator for Real Time Security

Semiconductor Research Corporation, PI, $210,000 2019–2022
Differential Power Analysis of Deep Neural Networks with Mitigations at the Architecture Level

National Science Foundation CRII, Sole PI, $174,751 2019–2021
CRII: SaTC: Secure Instruction Set Extensions for Lattice-Based Post-Quantum Cryptosystems

NSF I/UCRC: Center for Advanced Electronics through Machine Learning, PI, $89,034 2019–2020
Enabling Side-Channel Attacks on Post-Quantum Protocols through Machine Learning

NCSU Faculty Research & Professional Development, Sole PI, $7,928 2019–2020
ATOM-Crypt: A Tiny and Optimized Microcontroller Design for Emerging Lightweight Cryptography Standard

Equipment Donation, Sole PI, $6,272 2018–2019
Xilinx and Nvidia

Research Experience

North Carolina State University **Assistant Professor**
Departments: Assistant Professor at ECE and Adjunct Professor at CS *2018–Present*
Research Group: *HECTOR – Hardware Cybersecurity Research* (Raleigh, NC)

- Leading a research lab on hardware and embedded cybersecurity
- 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

The University of Texas at Austin **Post-Doctoral Research Fellow**

Advisors: Prof. Mohit Tiwari, Prof. Michael Orshansky *2016–2018*
Projects: *Secure Computer Architectures, Micro-Architectural Attacks, Side-Channels* (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 **Research Assistant**
Advisor: Prof. Patrick Schaumont *2012–2016*
Projects: *Post-Quantum Crypto., Physical Unclonable Functions, Anonymous Protocols* (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 **Summer Research Intern**
Project: *Authentication with Physical Unclonable Functions* *Jun–Aug 2014*
(San Diego, CA)

- 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

Vestek Research and Development Corp., Pixellence Design Team **Digital Design Engineer**
Project: *Depth Estimation and Adjustment for 3DTV-Video Enhancement* *2010–2012*
(Istanbul, Turkey)

- Completed the full design and implementation flow from software description to commercial FPGA end-product
- 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*
(Istanbul, Turkey)

- Designed low-power and low-energy hardware components for H.264/MPEG-4 Video Coding
- 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*
(Raleigh, NC)

- Developed a new graduate course on how to establish trust at the hardware root-of-trust
- 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*
(Raleigh, NC)

- Taught an undergraduate course on the fundamentals of digital electronics to 600+ sophomores

The University of Texas at Austin, ECE Department **Guest Lecturer**
Graduate Course: *EE 382: Security at the Hardware/Software Interface* *Fall 2017*
(Austin, TX)

- Gave a series of guest lectures on hardware-based cybersecurity: side-channel attacks and PUFs
- 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 Languages, EE 302: Digital Integrated Circuits* *2008–2010*
(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, Fall 2019, Fall 2020, Fall 2021

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, Spring 2022

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–present) Furkan Aydin (2019–present) Emre Karabulut (2020–present) Ferhat Yaman (2021–present) Faiz Alam (2021–present) Priyank Kashyap (2022–present) Digvijay Anand (2022–present) Ashley Kurian (2022–present) Arsalan Malik (2022–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-present)
MSc Committee Chair	Gregor Haas (2019–2021)
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)
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=Yhq5Me0AAAAJ&hl=en`
17 journal articles, **46** conference proceedings, **2** theses, and **1** patent.
Students and post-docs advised are marked with the * symbol.

Journal Articles

[1] *Aydin, Furkan**, and **Aydin Aysu**. ”Leaking secrets in homomorphic encryption with side-channel attacks.” Journal of Cryptographic Engineering (2024): 1-11.

[2] **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.

[3] *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.

[4] **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)

[5] *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**

[6] *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.

[7] *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.

[8] *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.

[9] *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.

[10] *Mert, Ahmet Can**, *Emre Karabulut**, Erdinç Öztürk, Erkay 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.

[11] Ozcan, Erdem, and **Aydin Aysu**. "High-Level-Synthesis of Number-Theoretic Transform: A Case Study for Future Cryptosystems." IEEE Embedded Systems Letters (2019).

[12] **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.

[13] **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.

[14] **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.

[15] **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.

[16] **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*

[17] **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

[18] *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.

[19] Mert, Ahmet Can, Ferhat Yaman, *Emre Karabulut**, Erdinc Ozturk, Erkay Savas, and **Aydin Aysu**. "A Survey of Software Implementations for the Number Theoretic Transform." In International Conference on Embedded Computer Systems (SAMOS). 2023.

[20] *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.

[21] *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.

[22] **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.

[23] *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.

[24] *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.

[25] 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.

[26] *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**

[27] *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.

[28] 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.

[29] *Dubey, Anuj* Emre Karabulut**, Amro Awad, **Aydin Aysu**. “High-Fidelity Model Extraction Attacks via Remote Power Monitors” IEEE International Conference on Aritficial Intelligence Circuits and Systems (AICAS), pp. 328-331. IEEE, 2022.

[30] *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

[31] *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.

[32] *Karabulut, Emre**, Erdem Alkim, and **Aydin Aysu**. “Single-Trace Side-Channel Attacks on ω-Small Polynomial Sampling.” Hardware Oriented Security and Trust (HOST), 2021

[33] *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**

[34] 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.

[35] *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

[36] *Mert, Ahmet Can**, *Emre Karabulut**, Erdinç Öztürk, Erkay 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**

[37] *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.

[38] 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.

[39] *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.

[40] *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.

[41] *Potluri, Seetal**, **Aydin Aysu**, and Akash Kumar. ”Seql: Secure scan-locking for ip protection.” In 2020 21st International Symposium on Quality Electronic Design (ISQED), pp. 7-13. IEEE, 2020.

[42] *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.

[43] *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.

[44] **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**

[45] 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**

[46] **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**

[47] 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

[48] **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.

[49] **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.

[50] 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.

[51] **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.

[52] **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.

[53] 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.

[54] 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.

[55] 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.

[56] 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.

[57] **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.

[58] 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.

[59] **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.

[60] **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.

[61] **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.

[62] 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.

[63] Akin, Abdulkadir, **Aydin Aysu**, Onur Can Ulusel, and Erkay 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

[64] Guo, Xu, **Aydin Aysu**. ”Security protocols for unified near field communication infrastructures.” United States patent US 9497573 B2, Granted 2016, Nov 15.

Theses

[65] **Aydin Aysu**. ”Resource-constrained and resource-efficient modern cryptosystem design.” Doctoral Dissertation, Virginia Polytechnic Institute and State University, 2016.

[66] **Aydin Aysu**. ”A baseline H.264 video encoder hardware design” Master Thesis, Sabanci University, 2010.

News Coverage of Research

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)
Member	IACR – International Association for Cryptologic Research (since 2013)

Invited Talks and Presentations

Securing Neural Network Hardware Against Side-Channel Attacks 2024
Invited Talk at Qualcomm Product Security Summit

Emerging Security Challenges at the Junction of AI and Hardware 2024
Keynote at IEEE Microelectronics Design & Test Symposium (MDTS)

The Third Decade of Physical Side-Channel Analysis 2024
Distinguished Lecture Series, I-SENSE, Florida Atlantic University

A Full Stack Solution for Edge AI 2024
Invited Talk at the New England Hardware Security Day

Securing Floating Point Side-Channels 2024
Invited Talk at GomacTech (Government Microcircuit Applications & Critical Technology Conference)

Defenser: A Complete Solution to Secure Multi-Tenant FPGAs 2024
Invited Talk at GomacTech (Government Microcircuit Applications & Critical Technology Conference)

A Pre-Silicon Vulnerability Analysis Tool for Edge AI 2024
Invited Talk at GomacTech (Government Microcircuit Applications & Critical Technology Conference)

Physical Side-Channel Analysis and the Future: Why Should You Care? 2024
Webinar at CAEML IUCRC

Emerging Topics in Secure Intelligent Devices 2023
Invited talk at the University of Passau, Germany

Emerging Threats on AI/ML Hardware 2023
Invited talk at US-UK Security in the Era of Global Semiconductor Initiatives

IEEE Council of Electronic Design Automation 2023
Panelist at AI Hardware Security

Privacy and Post-Quantum Cryptography 2023
Invited Lecture at Privacy Enhancing Technologies Course (Bilgi University)

Secure AI Hardware By Design: From Cryptographic Proofs to Silicon Tapeout 2023
Invited Talk at GomacTech (Government Microcircuit Applications & Critical Technology Conference)

Building and Breaking Post-Quantum Cryptography Hardware 2023
Invited Talk at NIST Crypto Reading Club

The Next Decade of Cryptographic Engineering: Post-Quantum Cryptography 2023
Keynote at DesignCon'23

The Future of Physical Side-channel Analysis: the Next Decade 2023
Invited Talk at NSA Center of Academic Excellence

Falcon Down: Breaking Falcon Post-Quantum Signature Scheme through Side-Channel Attacks 2022
Invited Talk at NIST 4th Workshop on Post-Quantum Cryptography Standardization

Multi-Tenant Cloud FPGAs: Security and Safety Risks 2022
Keynote at the ACM Cloud Computing Security Workshop (CCSW)

Machine Learning for Side-Channel Security Assessment of Next-Generation Cryptosystems 2022
Invited Talk at Special Session on AI-Enabled Security at IOLTS'22

Machine Learning and Side-Channel Analysis: The Path Forward 2022
Invited Talk at Ansys Inc.

Learning Based Techniques for Breakthrough in Side-Channel Security Assessment 2022
CAEML Workshop on Machine Learning for Hardware Design and Optimization

Embedded Digital RFID for Chip Asset Tracking 2022
Symposium on Counterfeit Parts and Materials

Physical Side-Channel Leakage Analysis of Edge Tensor Processing Units 2022
Invited Talk at Google Inc.

Securing Edge AI Devices Against Side-Channel Attacks with Hardware Masking 2022
Workshop on Security for Custom Computing Machines

Machine Learning and Side-Channel Analysis: What Did We Learn? 2022
Intel IPAS Tech Sharing Talk

Breaking and Securing Lattice-Based Post-Quantum Cryptography against Side-Channels 2022
Aselsan Corporation 3rd Annual Workshop on Post-Quantum Cryptography (In Turkish)

Securing Neural Networks Against Side-Channel Attacks with Hardware Masking 2022
Florida Institute for Cybersecurity Research Webinar

SeqL: Scan-Chain Locking and a Broad Security Evaluation 2021
Seminar at the IEEE CEDA CAD for Assurance

Hardware Masking for Neural Network Side-Channel Mitigation 2021
Seminar at Semiconductor Research Corporation e-Workshop

Horizontal Side-Channel Vulnerabilities of Post-Quantum Key-Exchange Protocols 2021
Invited talk at 2021 Hardware and Embedded Security Top Picks

Scan Chain attacks on Neural Networks 2021
Invited talk at Trustworthy and Reliable AI accelerator desigN (TRAIN) – Embedded Systems Week 2021

Machine Learning and Side-Channel Analysis: Happily Ever After or Bitter Divorce? 2021
Seminar at Villanova University

Stealing Neural Network Models through the Scan Chain: A New Threat for ML Hardware 2021
Invited talk at Virtual Workshop on Machine Learning & Hardware Security 2021 (MIHWSEC)

The Future of Physical Side-Channel Analysis: The Next Decade 2021
”Future of Cryptographic Engineering” Webinar

Machine Learning and Side-Channel Analysis: How Do They Couple? 2021
Invited Talk at Sabanci University

Deus Ex Machina: Learning Techniques for Breakthrough in Side-Channel Assessment of Circuits 2021
Seminar to the NSF/IUCRC Center of Advanced Electronic for Machine Learning (CAEML)

Deep Learning Attacks on Post-Quantum Hardware 2020
Invited talk at IEEE International Conference on Computer-Aided Design (ICCAD),

Reverse Engineering Neural Networks: The Hard(ware) Way 2020
Seminar Talk at Worchester Polytechnic Institute (WPI), IEEE International Conference on Physical Assurance and Inspection of Electronics (PAINE), and Riscure Inc. Hybrid Workshop

Deep-Learning Based Side-Channel Attacks 2019
Seminar to the NSF/IUCRC Center of Advanced Electronic for Machine Learning (CAEML)

Pushing Physical Side-Channels Beyond Cryptography 2019
Seminar talk at UC San Diego for the Security for Custom Computing Machines Workshop

Mission Impossible 7: Securing the IoT Landscape 2019
Gave a video-lecture at Bogazici University as part of CmpE490: Internet of Things

Hardware Security Research at NC State: Outreach to Turkey 2018
Seminar talk at Koc University, Bogazici University, Middle East Technical University, and Bilkent University

Securing Cryptographic Systems Against Quantum Adversaries and Hardware Exploits 2018
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

Side-Channel Analysis and Physical Unclonable Functions 2017
Guest lectures for ECE 382: Security at Hardware/Software Interface

Weak vs. Strong PUFs: Which is Better for the Internet-of-Things? 2016
Poster presentation at the Cryptographic Hardware and Embedded Systems (CHES) conference

Make PUFs Great Again! 2016
Presentation at Computer Aided Design and Implementation for Cryptography and Security Workshop

Hardware Hacking with the Doubling Attack 2016
Guest lecture for ECE/CS 5580: Cryptographic Engineering

Cryptoengineering the Future: Emerging Cryptographic Engineering Trends 2015
Poster presentation at CESCA day 2015

Renaissance of Precomputation in a Post-Quantum World 2015
Presentation at NIST Workshop on Cybersecurity in a Post-Quantum World

Drilling the Embedded Pyramid: Design Dimensions for Secure Embedded Systems 2014
Received *Best Poster* award, poster presentation at CESCA day 2014

PUFs for the Internet-of-Things Security 2014
Research Presentation at Qualcomm Inc.

A Tale of Two Schemes: Crypto Engineering for the Two Ends of Computing Spectrum 2014
Seminar talk at Virginia Tech and Sabanci University

Welcome to the Future of Security: Lattice-Based Cryptography 2013
Received *Best Presentation* award, presentation at CESCA day 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 2022 National Science Foundation 2021 National Science Foundation 2019
Panel Moderator	Secure Packaging: Initiatives, Research, and Workforce Development; IEEE PAINE conference 2022
Proposal Reviewer	Dutch Research Council 2022 Maryland Industrial Partnerships Program 2022 Army Research Office 2021
Proposal Reviewer	Maryland Industrial Partnerships Program 2022
Guest Editor	ACM DTRAP: Special Issue on the Digital Threats of Hardware Security 2020–present MDPI Cryptography Sepcial 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’22’23
Track Chair	International Conference on Reconfigurable Computing and FPGAs (Reconfig)'18'19
Technical Program Committee	Cryptographic Hardware and Embedded Security (CHES)'22 Design Automation Conference (DAC)'22'21'20'19 Design, Automation and Test in Europe (DATE)'22'21'20'19'18 International Symposium Field-Programmable Gate Arrays (FPGA)'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)'22'21 International Conference of Computer Design (ICCD)'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)'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