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

NSF CAREER	NSF Faculty Early Career Development 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 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

Research Experience

North Carolina State University **Assistant Professor**
Departments: Assistant Professor at ECE and Adjunct Professor at CS *2018–Present*
Research Group: *HECTOR – Hardware and Embedded 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 embedded 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*

- Developed novel authentication protocols with PUFs for multi-vendor IoT Applications — (San Diego, CA)
- 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*

- 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* — *Fall 2018-19*

- 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* — *Spring 2019*

- Taught an undergraduate course on the fundamentals of digital electronics to 161 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 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

Publication List

Google Scholar profile: `https://scholar.google.com/citations?user=Yhq5Me0AAAAJ&hl=en`

Journal Articles

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

[2] **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.

[3] **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.

[4] **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.

[5] **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.

[6] **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*

[7] **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

[8] Mert, Ahmet Can, Erkay Savas, Erdinc Ozturk, **Aydin Aysu**. "A Flexible and Scalable NTT Hardware: Applications from Homomorphically Encrypted Deep Learning to Post-Quantum Cryptography" Design, Automation, and Test in Europe (DATE) —Accepted, Best Application Paper Award— 2020

[9] Potluri, Seetal, **Aydin Aysu**, Akash Kumar. "SeqL: Secure Scan-Locking for IP Protection", International Symposium on Quality Electronic Design (ISQED) —Accepted— 2020

[10] Tan, Qinhan, Seetal Potluri, **Aydin Aysu** "Efficacy of Satisfiability-Based Attacks in the Presence of Circuit Reverse-Engineering Errors", IEEE International Symposium on Circuits and Systems (ISCAS) —Accepted— 2020

[11] Dubey, Anuj, Rosario Cammarota, **Aydin Aysu**. "MaskedNet: A Pathway for Secure Inference against Power Side-Channel Attacks" International Symposium on Hardware Oriented Security and Trust (HOST) —Accepted— 2020

[12] **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. —Best Paper Award MSE Track— 2019

[13] 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, —*Nominated for Best Paper Award*— 2019

[14] **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*

[15] 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

[16] **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.

[17] **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.

[18] 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.

[19] **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.

[20] **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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] **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.

[26] 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.

[27] **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.

[28] **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.

[29] **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.

[30] 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.

[31] 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

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

Theses

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

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

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

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 2019

Guest Editor

ACM DTRAP: Special Issue on the Digital Threats of Hardware Security 2020
MDPI Cryptography Sepcial Issue: Post-Quantum Cryptography: From Theoretical Foundations to Practical Deployments 2019

Track Chair

International Conference on Reconfigurable Computing and FPGAs (Reconfig)'18'19

Technical Program Committee

Design Automation Conference (DAC)'20'19
Design, Automation and Test in Europe (DATE)'20'19'18
International Symposium on Field-Programmable Gate Arrays (FPGA)'20'19
International Conference on Computer Aided Design (ICCAD)'19'18'17
Architecture and Hardware for Security Applications (AHSA)'19'18'17
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 Transactions on Embedded Computing Systems (TECS)
IEEE Transactions on Computers (TC)
IEEE Transactions on Information Forensics and Security (TIFS)
IEEE Transactions on Very Large Scale Integration Systems (VLSI)
IEEE Transactions on Circuits and System (TCAS)
IEEE Embedded System Letters (ESL)
Springer Journal on Cryptographic Engineering (JCEN)
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)'18'18'17'15
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