Furkan Aydin

Email: faydn@ncsu.edu ◆ **Phone:** 919-746-3091
LinkedIn: http://www.linkedin.com/in/furkan-aydin-/
Website: https://furkanaydin.wordpress.ncsu.edu

Summary

- PhD candidate in computer engineering at North Carolina State University (Expected graduation: May 2024)
- 5 years' hardware security and 8 years' hardware design experience as a research assistant

Education

- **Ph.D.** in Computer Engineering, North Carolina State University, Raleigh, NC Aug 2019 – present
- **Visiting Researcher** in Computer Engineering, North Carolina State University, Raleigh, NC Feb 2019 – Jun 2019
- **M.Sc.** in Electrical and Electronics Engineering, Ozyegin University, Istanbul, TURKEY Sep 2015 – Aug 2018
- **B.Sc.** in Electrical and Electronics Engineering, Ozyegin University, Istanbul, TURKEY Sep 2009 – Jun 2014

Work Experience

- **Research Assistant,** North Carolina State University, Raleigh, NC Feb 2019 – present
- **Teaching Assistant,** North Carolina State University, Raleigh, NC Aug 2019 – Dec 2022
- **Offensive Security Research Intern,** Intel Corporation, Chandler, AZ Jun – Aug 2021
- **Research/Teaching Assistant,** Ozyegin University, Istanbul, TURKEY Sep 2015 – Jun 2019
- **Assistant Process Engineer (Part-Time),** Emerson Process Management, Istanbul, TURKEY Mar – Aug 2014
- **Intern,** Emerson Process Management, Istanbul, TURKEY Jul – Sep 2013

Projects

PhD

- Hardware Security Emulators for Next Generation Edge AI/ML Dec 2022 – present
  (Supported by US Navy – Office Of Naval Research)
- Side-Channel Security Analysis of NTT Implementations for SABER and Dilithium Jun – Aug 2021
  (Internship with the Intel Product Assurance and Security group at Intel Corporation)
- ML-Based Security Analysis of Homomorphic Encryption Side-Channels Jan 2021 – July 2023
  (Supported by the National Science Foundation and Center for Advanced Electronics through Machine Learning)
- Enabling Side-Channel Attacks on Post-Quantum Protocols through Machine Learning Feb 2019 – May 2021
  (Supported by the National Science Foundation and Center for Advanced Electronics through Machine Learning)

MS

- Innovative Optical Wireless Communication Technologies for 5G and Beyond Aug 2017 – Jan 2019
  – FPGA Implementation of OFDM for Visible Light Communication Systems
  (Supported by The Scientific & Technological Research Council of Turkey – TUBITAK)
- M-RIVA: Methodology development for Real-time Implementation of Video Algorithms on FPGAs Feb 2016 – May 2017
  – Hardware Implementations of Image Fusion Algorithm
  (Supported by TUBITAK and European Union's Artemis Joint Undertaking as part of project named ALMARVI)
- FPGA Implementation of a Real-Time Full HD Video Transmission for FSO Laser Communication Feb – Aug 2016
  (Project at OKATEM – Center of Excellence in Optical Wireless Communication Technologies)

Research Interests

- Implementing cryptography/machine learning/image processing/communication algorithms on embedded systems
- Developing and implementing countermeasures to protect against hardware-based attacks
- Identifying and analyzing potential threats and vulnerabilities at pre-silicon and post-silicon stage

Technical Experience

- Hardware design (RTL design and validation, RISC-V based SoC)
- Embedded software development (ARM-based Cortex-M and MSP40 microcontrollers, Raspberry Pi, NVDIA Jetson)
- Hardware security (Side-channel attacks, fault attacks, defenses against side-channel attacks)

Programming Languages: Verilog * C/C++ * Python

Tools: Vivado Synthesis / Xilinx ISE / Quartus Prime / Synopsys Design Compiler * ModelSim * MATLAB
Riscure's Security Tools (Inspector Software, icWaves, Transceiver, Current Probe, EM Probe, etc.)

Training and Certificate

Riscure Inspector Certificate for Side-Channel Analysis and Fault Injection: Mar 2019

The training course addressed theory and practice of side-channel security. Topics that have been addressed include cryptology, side-channels, signal processing, power analysis, fault injection attacks, and machine learning based attacks.

Courses Taken

- Cryptographic Engineering and Hardware Security
- Secure Processor Architecture
- ASIC and FPGA Design
- System on Chip Design
- Advanced FPGA Design and Computer Arithmetic
- Digital Electronics and FPGA Design
- Embedded System Design
- Microprocessors
- Network Security
- Computer Networks
- Advanced Object-Oriented Programming
- Introduction to Business I (Decision Making)
- Introduction to Business II (Entrepreneurship)
- Introduction to Economics

Courses - Teaching Assistant

- Cryptographic Engineering and Hardware Security
- Computer Systems Programming
- Introduction to Computer Systems
- Digital Electronics and FPGA Design
- Digital Systems

Publications

- **Aydin, F.**, and Aysu, A.: **Leaking Secrets in Homomorphic Encryption with Side-Channel Attacks.** Journal of Cryptographic Engineering, Springer, pp. 1-11, January 2024.
- **Aydin, F.**, and Aysu, A.: **Exposing and Mitigating Side-Channel Leakage of SEAL Homomorphic Encryption Library.** In Proceedings of the 6th ACM Workshop on Attacks and Solutions in Hardware Security (ASHES 2022), pp. 95-100, Los Angeles, CA, USA, November 2022.
- **Aydin, F.**, Karabulut, E., Potluri, P., Alkim, E., and Aysu, A.: **RevEAL: Single-Trace Side-Channel Leakage of the SEAL Homomorphic Encryption Library.** In Proceedings of the Design, Automation and Test in Europe (DATE), pp. 1527-1532, Antwerp, Belgium, March 2022.
- **Aydin, F.**, Aysu, A., Towari, M., Gerstlauer, A., and Orhansky, M.: **Horizontal Side-Channel Vulnerabilities of Post-Quantum Key Exchange and Encapsulation Protocols**. Journal of ACM Transactions on Embedded Computing Systems (TECS), pp. 1-22, October 2021.
- Kashyap, P., **Aydin, F.,** Potluri, S., Franzon, P., and Aysu, A.: **2Deep: Enhancing Side-Channel Attacks on Lattice-Based Key-Exchange via 2D Deep Learning**. Journal of IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), pp. 1217-1229, November 2020.
- Regazzoni, F., Bhasin, S., Pour, A. A., Alshaer, I., **Aydin, F.**, Aysu, A., Beroulle, V., Di Natale, G., Franzon, P., Hely, D., Homma, N., Ito, A., Jap, D., Kashyap, P., Polian, I., Potluri, S., Ueno, R., Vatajelu, E. I., and Yli-Mayry, V.: **Machine Learning and Hardware Security: Challenges and Opportunities –Invited Talk–**. In Proceedings of the 2020 International Conference on Computer-Aided Design (ICCAD), pp. 1-6, San Diego, CA, USA, November 2020.
- **Aydin, F.,** Kashyap, P., Potluri, S., Franzon, P., and Aysu, A.: **DeePar-SCA: Breaking Parallel Architectures of Lattice Cryptography via Learning Based Side-Channel Attacks**. In Proceedings of the 2020 International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation (SAMOS), pp. 262-280, October 2020.
- Levent, V. E., Saglam, G., Ugurdag, H. F., Annafianto, N. F. R., **Aydin, F.,** Tesfay, S. W., Aly, B., Elamassie, M., Kebapci, B., and Uysal, M.: **FPGA Based DCO-OFDM PHY Transceiver for VLC Systems**. In Proceedings of the 11th International Conference on Electrical and Electronics Engineering (ELECO), pp. 418-421, Bursa, Turkey, December 2020.
- **Aydin, F.,** Ugurdag, H. F., Levent, V. E., Güzel, A. E., Annafianto, N. F. R., Özkan, M. A., Akgün, T., and Erbas, C.: **Rapid Design of Real-Time Image Fusion on FPGA Using HLS and Other Techniques.** In Proceedings of IEEE/ACS International Conference on Computer Systems and Applications (AICCSA), Aqaba, Jordan, pp.1-6, October/November 2018.
- Levent, V. E., Güzel, A. E., Tosun, M., Buyukmihci, M., **Aydin, F.,** Gören, S., Erbas, C., Akgün, T., and Ugurdag, H. F.: **Tools and Techniques for Implementation of Real-Time Video Processing Algorithms.** Journal of Signal Processing Systems, vol.91, no.1, pp.93-113, September 2018.

Synergistic Activities

- **Seminars and Workshops:**

  - Presented a paper on "Single-Trace Side-Channel Leakage of SEAL Homomorphic Encryption" at the Design, Automation & Test in Europe Conference & Exhibition (DATE) in 2022.

  - Invited to present a talk organized by fhe.org on the topic of "Single-Trace Side-Channel Attack on SEAL Homomorphic Encryption Library" in 2022.

  - Presented research work titled "Deus Ex Machina: Learning Techniques for Breakthrough in Side-Channel Security Assessment of Integrated Circuits" at the CAEML Webinar in 2021.
- **Undergraduate Student Supervision:**

  - Successfully mentored three undergraduate students (Wesley Cowand, Bryan Wilson, and Devin Whitmore) in their research projects at North Carolina State University.
- **Reviewer Activities:**

  - Contributed as a reviewer for Journal of IEEE Transactions on Circuits and Systems, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, PeerJ Computer Science, and IEEE/ACM International Conference on Computer-Aided Design in the field of hardware security and hardware design.