Kemal Derya

Worcester, MA kderya@wpi.edu kemalderya.github.io kemal-derya

EDUCATION

Worcester Polytechnic Institute *August 2022 – Present*
Ph.D. Candidate *in Electrical and Computer Engineering* *Worcester, MA*

- Working on AI safety, microarchitectural attacks, and hardware security

Sabanci University *January 2020 – July 2022*
M.S. *in Electronics Engineering (GPA: 3.85/4.00)* *Istanbul, Turkey*

- Worked on post-quantum cryptography and digital hardware design.

Sabanci University *Sept 2014 – June 2019*
B.S. *in Electronics Engineering (with Tuition Fee Scholarship GPA: 3.67/4.00)* *Istanbul, Turkey*

PROFESSIONAL EXPERIENCE

Analog Devices Inc. *January 2025 - Present*
Systems Engineering Intern *Boston, MA*

- Added automated scripts to ensure ASPICE System Engineering compliance in the team's system projects
- Developed scripts to ensure system requirements and specifications conform to the team's guidelines
- Built CI/CD pipeline on Github to automate ASPICE compliance checks and publish the incompatible requirements at each system level

PAVOTEK *March 2022 – July 2022*
Digital Design Engineer *Istanbul, Turkey*

- Developed state-of-the-art digital systems essential for defense applications
- Utilized my expertise in FPGA design methodologies and digital signal processing
- Devised GSM protocol and produced Verilog code leveraging MATLAB Simulink
- Created reliable, high-performance digital hardware solutions on Zynq board

ABB Robotics *June 2018 – August 2018*
Summer Intern *Istanbul, Turkey*

- Contributed to the design and prototyping of robotic components, enhancing product development
- Developed a framework that controls industrial robots through voice commands

SKILLS

Programming: C, C++, Python, Verilog

Technical: AI Safety, PyTorch, TensorFlow, Hardware Security, Computer Architecture, Digital Hardware Design, FPGA, ASIC

PROJECTS

Exploiting LLM Vulnerabilities Through Fixed-Point Variables IEEE SaTML 2025

- Found a vulnerability on LLMs where carefully crafted queries produce non-halting responses
- Made assessments on different GPT, LLama, and Gemini language models

Finding Leakage by Leveraging Reinforcement Learning Pre-Print

- Developed reinforcement learning algorithms to automate attack synthesis for identifying microarchitectural data leakage vulnerabilities on Intel architectures

Extracting Secret Keys using Rowhammer DRAM Profiling ACM ASIACCS 2025

- Executed Rowhammer attacks to profile DRAM modules and extracted private keys used in TLS handshakes
- Issued CVE-2024-5288 on wolfSSL library

Skipping Instruction Sequence using Rowhammer Exploit IEEE EuroS&P 2025

- Introduced a Rowhammer gadget that breaks the instruction code to bypass a critical code piece

Accelerating Lattice-based PQC schemes MICPRO

- Designed and implemented NTT-based polynomial multiplier hardware on FPGA
- Enhanced design reconfigurability for application to various PQC schemes

PUBLICATIONS & PRE-PRINTS

- G. Hammouri, **K. Derya** and B. Sunar, "Non-Halting Queries: Exploiting Fixed Points in LLMs," 2025 IEEE Conference on Secure and Trustworthy Machine Learning (SaTML), Copenhagen, Denmark, 2025, pp. 1-22, doi: 10.1109/SaTML64287.2025.00009.
- Tol, M.C., **Derya, K.** and Sunar, B., 2025. μ RL: Discovering Transient Execution Vulnerabilities Using Reinforcement Learning. arXiv preprint arXiv:2502.14307.
- **Derya, K.**, Tol, M.C. and Sunar, B., 2024. Fault+ probe: A generic rowhammer-based bit recovery attack. arXiv preprint arXiv:2406.06943.
- Adiletta, A., Tol, M.C., **Derya, K.**, Sunar, B. and Islam, S., 2024. LeapFrog: The Rowhammer Instruction Skip Attack. arXiv preprint arXiv:2404.07878.
- **Kemal Derya**, Ahmet Can Mert, Erdinç Öztürk, Erkay Savaş, CoHA-NTT: A Configurable Hardware Accelerator for NTT-based Polynomial Multiplication, Microprocessors and Microsystems, Volume 89, 2022, 104451, ISSN 0141-9331, https://doi.org/10.1016/j.micpro.2022.104451.
- **Derya, K.**, 2022. Accelerating lattice-based cryptosystems (Master Thesis).

TEACHING EXPERIENCE

Worcester Polytechnic Institute

- ECE 3829 - Advanced Digital System Design With FPGAs
- ECE 2049 - Embedded Computing In Engineering Design

Sabanci University

- CS 303 - Logic and Digital System Design
- EE 308 - Microprocessor Based System Design