Hossam ElAtali

E-mail: hossam.elatali@gmail.com Website: elatalhm.github.io

Education

PhD Computer Science – System Security	University of Waterloo	2021 – present

Topics: HW-assisted security, confidential computing, memory safety, side channels

Skills: *Computer architecture development (Verilog/Chisel, RISC-V, Aarch64, QEMU, cache coherence)*
ML HW acceleration (TPU/NPU/GPU)
Compiler extensions (LLVM)
Firmware and operating systems (C/C++, Assembly, Linux kernel, UEFI)

Supervisor: Prof. N. Asokan

M.Sc. Computer Hardware and Software Engineering	Universität Stuttgart	2012 – 2015

Final GPA: 1.3 (i.e., Very Good)

B.Sc. Electronics	German University of Cairo	2007 – 2012

Final GPA: 0.74 (i.e., A+), **ranked 3rd**

Professional Experience

PhD Intern	Huawei, Helsinki System Security Lab	2025

- Developed system security solutions for Aarch64 (1 patent submitted)

Relevant skills

Aarch64, Assembly, QEMU, Linux kernel, UEFI

Technical Lead		2020 – 2021
Senior Software Development Engineer	Mentor Graphics	2018 – 2020
Software Development Engineer		2015 – 2018

- Developed C++ solutions for Mentor Graphics's emulation hardware.
- Led a team to develop a brand-new product for verifying Optical Transport Network designs-under-test (DUTs).

Relevant skills

C++, Linux, Qt, GUI, Bash, Verilog, HW/SW Interface, Custom Firmware, GDB/Valgrind, Python

Publications

- **H. ElAtali**, M. Gülmez, T. Nyman, N. Asokan, "*BLACKOUT: Data-Oblivious Computation with Blinded Capabilities*", arXiv preprint. 2025. [link]
- **H. ElAtali**, N. Asokan, "*CacheSquash: Making caches speculation-aware*", arXiv preprint. 2025. [link]
- **H. ElAtali**, X. Duan, H. Liljestrand, M. Xu, N. Asokan, "*BliMe Linter*", IEEE SecDev Conference. 2024. [link]
- **H. ElAtali**, J. Z. Jekel, L. J. Gunn, N. Asokan, "*Data-Oblivious ML Accelerators using Hardware Security Extensions*", International Symposium on Hardware Oriented Security and Trust (HOST). 2024. [link]
- **H. ElAtali**, L. J. Gunn, H. Liljestrand, N. Asokan, "*BliMe: Verifiably Secure Outsourced Computation with Hardware-Enforced Taint Tracking*", Network and Distributed Systems Symposium (NDSS). 2024. [link]
- **H. ElAtali**, "*Configurable Shared Cache and Memory Model for Parallel NoC Simulation*", Master's thesis, University of Stuttgart, 2015.
- **H. ElAtali**, "*Simulation of Realistic Defects for Validating Test-and Diagnosis-Algorithms*", Bachelor's thesis, University of Stuttgart, 2011. [link]

Awards

- Best Poster Award (2022) – Cybersecurity and Privacy Institute, University of Waterloo
- Entrance Scholarship (2021) – University of Waterloo
- DAAD Full Scholarship (2012-2015) – German Academic Exchange Service