Hossam ElAtali

E-mail:	hossam.elatali@gmail.com
LinkedIn:	hossam-elatali-05545b20
Website:	elatalhm.github.io

Education

PHD Computer Science – Platform Security 2021 – present

University of Waterloo, CrySP Group

Topics: Hardware-assisted defenses, trusted execution environments, run-time attacks, side channels
Skills: *Computer architecture development, Verilog/Chisel, RISC-V, LLVM, C++, Assembly, Linux*
Supervisor: Prof. N. Asokan

M.Sc. INFOTECH – Computer Hardware and Software Engineering 2012 – 2015

Universität Stuttgart

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

B.Sc. Information and Engineering Technology – Electronics 2007 – 2012

German University in Cairo

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

Professional Experience

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

Mentor, a Siemens Business

- Developed our Multimedia solutions, C++ GUI-based applications used with Mentor's emulation hardware to verify designs under test (DUTs) implementing multimedia protocols such as HDMI.
- Led a team to develop a brand-new product for verifying the protocol layer of Optical Transport Networks.

Relevant skills

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

Publications

- H. ElAtali, J.Z. Jekel, L. J. Gunn, N. Asokan, "*Data-Oblivious ML Accelerators using Hardware Security Extensions*", arXiv preprint. 2024. https://doi.org/10.48550/arXiv.2401.16583.
- 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), San Diego, CA, USA. 2024. http://doi.org/10.14722/ndss.2024.24105.
- 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, http://doi.org/10.18419/opus-2852.

Awards

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