Mahmoud Abumandour

+1 (778) 320-8958 | BC, Canada | mahmoud_abumandour@sfu.ca
linkedin.com/in/abumandour | github.com/i3abghany | i3abghany.github.io

Education

Simon Fraser University — **Burnaby, Canada**
PhD in Computer Science — ***Sep 2024 – Present***
MSc in Computer Science | Thesis: Uncovering and Mitigating Bit-Flip Vulnerabilities in Edge DNNs — ***Sep 2022 – Aug 2024***
Mansoura University — **Mansoura, Egypt**
BSc in Computer and Communication Engineering | Ranked 1st of 180 students — ***Sep 2017 – Jul 2022***

Experience

Simon Fraser University — **Burnaby, Canada**
Graduate Research Assistant — ***Sep 2022 – Present***

- Designed a data-independent bit-flip attack that degrades modern LLMs to 0% accuracy with fewer than 25 flips
- Designed a bit-flip defense for LLMs that throttles white-box bit-flip attacks on GPUs with less than 1% overhead
- Teaching Assistant for Intro to Computer Systems, Compiler Design, Computer Architecture, and Distributed Systems

Max Planck Institute for Security and Privacy — **Bochum, Germany**
Research Intern — ***Jun 2026 – Sep 2026***

- Developed an FPGA-based fault-injection framework to evaluate the security of hardened cores
- Uncovered and reported multiple security vulnerabilities in OpenTitan's CPU and surrounding ecosystem

Intel Corporation — **Santa Clara, CA (Remote)**
CPU Architecture Intern — ***Jan 2024 – May 2024***

- Modeled and evaluated CPU front-end features, including instruction prefetching and instruction caching
- Characterized workloads by instruction-cache footprint and branch behavior to support architectural exploration
- Analyzed sources of miscorrelation between functional and cycle-accurate cache simulators

Master Micro — **Cairo, Egypt**
Software Engineering Intern — ***Oct 2021 – Feb 2022***

- Designed a range-based file format for EDA lookup tables, reducing average range-query latency by more than 50% over serialized binary file streaming

Google Summer of Code (QEMU) — **Remote**
Software Developer — ***May 2021 – Aug 2021***

- Implemented and maintained multi-core, multi-level cache emulation in upstream QEMU
- Used to analyze cache performance of the xv6 OS kernel and matrix multiplication userspace programs in QEMU

Projects and Open-Source Contributions

- **Rx32 Core:** A fine-grained multithreaded RISC-V core with dynamic thread scheduling and thread-aware hazard detection. It reaches 0.95 CoreMark IPC on two threads, up from 0.69 on one
- **RISC-V Newlib**: Profiled and optimized upstream newlib for RISC-V, benchmarking on gem5 and RISC-V Pi Pico 2
- **Fuzzing Emulator**: Userspace fuzzing with RISC-V emulation achieving linear scaling with host workers by avoiding kernel context-switch overhead
- **pAES:** Low-power, Low-area AES encryption core for FPGA with 80% smaller area than standard pipelined design

Publications and Talks

- Srinija Ramichetty, **Mahmoud Abumandour**, Alaa R. Alameldeen, Guru Venkataramani. *EnsembleHealer: Autonomous Recovery from Model Poisoning in Decentralized Federated Learning*. ACM CF, 2026
- **Mahmoud Abumandour**, Srinija Ramichetty, Guru Venkataramani, Alaa R. Alameldeen. *WeightSentry: Real-Time Bit-Flip Protection for Deep Neural Networks on GPUs*. HASP, 2025

Skills

Languages: C++, C, Rust, Python, x86 Assembly, Bash, Java, SystemVerilog
Tools: gem5, QEMU, LLVM, PyTorch, TensorFlow, Ghidra, perf, Git, Docker, Linux, Xilinx Vivado
Areas: Computer Architecture, Performance Modeling, Hardware Security, ML Security, Fuzzing, FPGA, RISC-V