ALHAD DAFTARDAR

678-308-7561 • adaftardar.github.io • ajd9396@nyu.edu

Education

NEW YORK UNIVERSITY | Brooklyn, NY *September 2022 – Present*
PhD in Electrical Engineering
Research Advisors: Brandon Reagen, Siddharth Garg, Benedikt Bünz (collaborating advisor)

UNIVERSITY OF MICHIGAN | Ann Arbor, MI *August 2020 – April 2022*
MS in ECE (Integrated Circuits/VLSI), 4.00 GPA
Research Advisors: David Blaauw, Hun-Seok Kim, Ronald Dreslinski (collaborating advisor)

GEORGIA INSTITUTE OF TECHNOLOGY | Atlanta, GA *August 2016 – May 2020*
BSEE, CS Minor, Honors Program, 4.00 GPA
ECE Senior Scholar Award (for highest GPA)
Batts and Brown Innovation Award ($4000 scholarship) – *via the Vertically Integrated Projects program*

Publications

- **Alhad Daftardar,** Jianqiao Mo, Joey Ah-kiow, Benedikt Bünz, Siddharth Garg, Brandon Reagen, "zkPHIRE: A Programmable Accelerator for ZKPs over HIgh-degRee, Expressive Gates", **under review**
- Jianqiao Mo, **Alhad Daftardar,** Joey Ah-kiow, Kaiyue Gao, Benedikt Bünz, Siddharth Garg, Brandon Reagen, "MTU: The Multifunction Tree Unit for Accelerating Zero-Knowledge Proofs, **HASP 2025** (co-located with MICRO 2025)
- **Alhad Daftardar,** Jianqiao Mo, Joey Ah-kiow, Benedikt Bünz, Ramesh Karri, Siddharth Garg, Brandon Reagen, "Need for zkSpeed: Accelerating HyperPlonk for Zero-Knowledge Proofs", ***International Symposium on Computer Architecture (ISCA), 2025***
- **Alhad Daftardar,** Brandon Reagen, Siddharth Garg, "SZKP: A Scalable Accelerator Architecture for Zero-Knowledge Proofs", ***33rd International Conference on Parallel Architectures and Compilation Techniques (PACT), 2024***
- Sung Kim, Morteza Fayazi, **Alhad Daftardar**, Kuan-Yu Chen, Jielun Tan, Subhankar Pal, Tutu Ajayi, Yan Xiong, Trevor Mudge, Chaitali Chakrabarti, David Blaauw, Ronald Dreslinski, Hun-Seok Kim, "Versa: A 36-Core Systolic Multiprocessor with Dynamically-Reconfigurable Interconnect and Memory," ***Journal of Solid State Circuits***, 2022
- Daniel Bliss, et al. Enabling Software-Defined RF Convergence with a Novel Coarse-Scale Heterogeneous Processor. ***ISCAS*** 2022
- Sung Kim, Morteza Fayazi, **Alhad Daftardar**, Kuan-Yu Chen, Jielun Tan, Subhankar Pal, Tutu Ajayi, Yan Xiong, Trevor Mudge, Chaitali Chakrabarti, David Blaauw, Ronald Dreslinski, Hun-Seok Kim, "Versa: A Dataflow-Centric Multiprocessor with 36 Systolic ARM Cortex-M4F Cores and a Reconfigurable Crossbar-Memory Hierarchy in 28nm," ***2021 IEEE Symposium on VLSI Circuits***, 2021
- Patrick Coppock, Momen Yacoub, Bruce Qin, **Alhad Daftardar**, Zayd Tolaymat, Vincent Mooney, "Hardware Root-of-Trust-based integrity for shared library function pointers in embedded systems," ***Microprocessors and Microsystems***, Volume 79, 2020

Research Experience

New York University | Brooklyn, NY *September 2022 – Present*
Graduate Student Research Assistant
Accelerating Zero-Knowledge Proofs (ZKPs)

- Conducting design-space exploration of ZKP primitives (NTT, MSM, SumCheck) in hardware to evaluate area-latency tradeoffs
- Modeling accelerators for state of the art ZKP protocols (HyperPlonk, Groth16)
- Building High-Level Synthesis library and chiplet library for agile hardware design of cryptographic kernels

University of Michigan | Ann Arbor, MI *August 2020 – December 2021*
Graduate Student Research Assistant
DARPA DSSoC – Forward Error Correction (FEC) Encoding Engine

- Designed microarchitecture for FEC engine that supports 3 reconfigurable encoders on 1 accelerator (LDPC, Polar, Turbo)
  - Each encoder reprogrammable at runtime w.r.t. encoder-specific parameters (frozen bit locations, parity-check matrix, etc.)
- Implemented encoders in SystemVerilog

DARPA SDH – Transmuter/Versa: Hardware Accelerator based on reconfigurable crossbar-memory hierarchy for big data workloads

- Mapped error correction code kernels onto architecture to evaluate programmability, reconfigurability, architectural features
- Led software-side efforts to extend prior version of chip from 32-core design to 128-core design for tapeout
- Led software verification of various algorithms (2D convolution, matrix-multiply, sorting)

Vertically Integrated Projects: Secure Hardware | Atlanta, GA *August 2018 – May 2020*

Undergraduate Research Assistant

Hardware Root-of-Trust Based Integrity for Shared Library Function Pointers in Embedded Systems

- Developed a secure hardware root-of-trust (RoT) to mitigate effects of malware attacks on the Global Offset Table (GOT)
- Implemented RoT in Verilog modules programmed onto Xilinx Zedboard with PetaLinux OS for software interface
- Wrote malware that overwrote GOT function pointers and succeeding in redirecting program flow in absence of RoT
- Demonstrated RoT storage/retrieval interface that eliminated program dependence on GOT and nullified malware effects

Vertically Integrated Projects: Agile Communication Architectures | Atlanta, GA *August 2019 – May 2020*

Undergraduate Research Assistant, Blue Team Lead

Automatic Modulation Classification on SDRs using ResNet Classifier

- Implemented machine learning models on Software Defined Radios for use in modulation classification
- Led Hardware Team in the direct implementation of ML classifiers onto SDRs with GNURadio for real-time signal classification

Vertically Integrated Projects: Secure Hardware | Atlanta, GA *January 2017 – December 2019*

Undergraduate Research Assistant, Team Lead, Project Supervisor

Assessing the security potential of Non-Linear Multiple Input Signature Register (NLMISR)

- Researched NLMISR as alternative to Secure Hash Algorithm-2 (SHA-2) for low power/low area data encryption applications
- Designed 128-bit NLMISR and testing infrastructure (in VHDL) to search for hash collisions (empirical evaluation of collision resistance and other cryptographic properties)

Teaching Experience

High-Level Synthesis for Scientific Computing (NYU) *January 2025 – May 2025*

- Present lectures to seminar class on HLS design flow and tools
- Write tutorials on using Catapult and Vivado HLS
- Grade student presentations/projects

Parallel Computer Architecture (University of Michigan) *January 2022 – April 2022*

- Discussion/recitation sections, office hours
- Help students with their programming assignments

Course Projects

VLSI Design II (University of Michigan) *January 2022 – April 2022*

End-to-End Low-Power Keyword Spotting Accelerator

- Led a 6-person team in building a 4 mm^2 chip in 130 nm CMOS with analog front-end, feature-extraction engine, and NN backend
  - 89% accuracy at classifying audio signals into 1 of 10 words from Google Speech Dataset
- Specialized in GRU-based neural network backend (fixed point MATLAB modeling, controller logic, verification tests)
- **Won 1st place Apple Design Competition (judged by Apple circuit design engineers) and won Apple Airpods Pro**

VLSI for Communications and Machine Learning (University of Michigan) *October 2021 – December 2021*

Homomorphically Encrypted FIR Convolution using Ring Learning with Error (RLWE)

- Explored noise accumulation problem in *somewhat* HE using RLWE
- Analyzed tradeoffs between necessary bit-width for large ciphertext-to-plaintext modulus ratio and supportable FIR length
- Investigated hardware techniques for efficiently computing modulus operations in ring-based arithmetic
- Implementing 32-tap FIR in SystemVerilog and performed synthesis/timing analysis

Work Experience

Systems & Technology Research | Boston, MA *May 2019 – August 2019*

Cyber Physical Systems Intern

Software Defined Hardware (SDH program, a DARPA Initiative)

- Programming language design & development targeting accelerated hardware for data intensive algorithms
- Learned/self-taught MITCHELL language & implemented NLP algorithms to demonstrate MITCHELL's massive parallelism features
- Developed and demonstrated a full, proof-of-concept pipeline from algorithm implementation in MITCHELL, to compilation to customized low-level libraries, to simulation onto hardware-accelerator simulators

Leadership/Extracurriculars

New York University | Brooklyn, NY

- Co-founder – Abandoned Researchers of Brooklyn Campus *May 2024 – Present*
  - Organized Summer Mixer Series and Fall Hangout Series for PhD students in Tandon School of Engineering
- Quadball (Quidditch) Team, Chaser *September 2022 – April 2023*

University of Michigan | Ann Arbor, MI

- Quidditch Team, Chaser *August 2021 – April 2022*
- Indian Student Association, Secretary *May 2021 – April 2022*

Selected Graduate Coursework

Parallel/Custom Computer Architecture (Michigan, NYU)
Computer Architecture (Georgia Tech, Michigan)
Cryptography (NYU)
Deep Learning (Michigan, NYU)
Cryptography of Blockchains (Audited at NYU)
VLSI for Communications and Machine Learning (Michigan)
VLSI Design I, VLSI Design II (Michigan)
Information Processing in Neural Systems (Georgia Tech)
Advanced Hardware Security (Georgia Tech)
Probability (NYU)

Skills

Languages: (System)Verilog, Python, Rust, C/C++, MATLAB, RISC-V, MIPS, VHDL, SML
Software: Catapult HLS, Vivado HLS, Design Compiler, Cadence Virtuoso
Social: Improv Comedy, Rock Climbing, Public Speaking