Alhad Daftardar

✉ ajd9396@nyu.edu | 🌐 adaftardar.github.io | in alhad-daftardar | 🎓 Google Scholar

Education

New York University **Brooklyn, NY**
Ph.D. Candidate — Electrical and Computer Engineering *2022 - May 2027 (Expected)*
Research: Accelerating Zero-Knowledge Proofs and Verifiable ML
Advisors: Brandon Reagen & Siddharth Garg; Benedikt Bünz (collaborator)

University of Michigan (4.00 GPA) **Ann Arbor, MI**
MS — Electrical and Computer Engineering *2020 - 2022*
Research: Reconfigurable Multicore Systems, Error-Correction Code Accelerators
Advisors: David Blaauw & Hun-Seok Kim; Ronald Dreslinski (collaborator)

Georgia Institute of Technology (4.00 GPA) **Atlanta, GA**
BS — Electrical Engineering *2016 - 2020*
Research: Hardware Security, Software-Defined Radios
Advisors: Vincent Mooney; Matthieu Bloch

Research Overview

4th year PhD student at NYU. I design **scalable, high-performance hardware architectures** for **trustworthy and verifiable AI/ML**, focusing on **Zero-Knowledge Proofs (ZKPs)**. My research leverages hardware–software co-design to accelerate emerging ZKP protocols, and I collaborate with computer architects, cryptographers, and AI/ML experts in my work. Through these collaborations, I've published at top architecture and VLSI venues like **ISCA**, **PACT**, and **JSSC**, and I organized the first ever **ZKARCH** workshop at **MICRO '25**.

Publications (with links)

Conference Publications

- Need for zkSpeed: Accelerating HyperPlonk for Zero-Knowledge Proofs (**ISCA 2025**)
  Alhad Daftardar, Jianqiao Mo, Joey Ah-kiow, Benedikt Bünz, Ramesh Karri, Siddharth Garg, Brandon Reagen.
- SZKP: A Scalable Accelerator Architecture for Zero-Knowledge Proofs (**PACT 2024**)
  Alhad Daftardar, Brandon Reagen, Siddharth Garg.
- MTU: The Multifunction Tree Unit for Accelerating Zero-Knowledge Proofs (**HASP 2025, Best Paper Runner Up**)
  Jianqiao Mo, **Alhad Daftardar**, Joey Ah-Kiow, Kaiyue Guo, Benedikt Bünz, Siddharth Garg, Brandon Reagen.
- Versa: A Dataflow-Centric Multiprocessor with 36 Systolic ARM Cortex-M4F Cores and a Reconfigurable Crossbar-Memory Hierarchy in 28nm (**Symposium on VLSI Circuits 2021**)
  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.
- Enabling Software-Defined RF Convergence with a Novel Coarse-Scale Heterogeneous Processor (**ISCAS 2022**)
  D. W. Bliss, T. Ajayi, A. Akoglu, I. Aliyev, T. Basaklar, L. Belayneh, D. Blaauw, J. Brunhaver, C. Chakrabarti, L. Chang, K.-Y. Chen, M.-H. Chen, X. Chen, A. R. Chiriyath, **A. Daftardar**, et al.

Preprints (Under Review)

- (on arXiv) zkPHIRE: A Programmable Accelerator for ZKPs over HIgh-degRee, Expressive Gates
  Alhad Daftardar, Jianqiao Mo, Joey Ah-kiow, Benedikt Bünz, Siddharth Garg, Brandon Reagen.

Journal Publications

- Versa: A 36-Core Systolic Multiprocessor With Dynamically Reconfigurable Interconnect and Memory
  (**Journal of Solid State Circuits 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.

- Hardware Root-of-Trust-based integrity for shared library function pointers in embedded systems
  (**Microprocessors and Microsystems 2020**)
  Patrick Coppock, Momen Yacoub, Bruce Qin, **Alhad Daftardar**, Zayd Tolaymat, Vincent Mooney.

Workshops and Outreach

ZKARCH - 1st Workshop on Architectures for ZKPs and Verifiable Computing **Seoul, Korea**
Organizer *October 2025*

- Organized the ***first*** workshop on ZKP hardware, co-located with **MICRO 2025**
- **Led the technical program**, speaker invitations, social media outreach, and on-site hosting
- Gave a talk on our work on **SZKP** and **zkSpeed**
- Secured **3 industry talks (Irreducible, Ingonyama, Fabric Cryptography)** and 5 academic research talks

International Symposium on Performance Analysis of Systems and Software **Seoul, Korea**
Student Organizer *September 2025 – Present*

- Assisting Prof. Brandon Reagen (Program Committee Chair) with organizing the conference
- Coordinating PC invitations, website maintenance, and administrative duties

Brooklyn Researcher Brigade, NYU Tandon School of Engineering **Brooklyn, NY**
Co-founder, Vice President *April 2024 – Present*

- Founded and co-organized a monthly cross-department mixer series fostering community among PhD students
- Secured department sponsorship and official student club status through a competitive application process
- Grew attendance to **70+ attendees** at major events, sustained regular engagement (10–20 attendees weekly)

NYU Computer Architecture Day **Brooklyn, NY**
Session Chair *March 2024*

- Facilitated talks by computer architecture students across NYC/tri-state area

Research Experience

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

- Initiated a line of work designing **novel hardware architectures for ZKP primitives** (NTT, MSM, SumCheck) and analyzing their area–latency trade-offs across design points
- Developed accelerators for advanced ZKP protocols (Jolt, HyperPlonk, Groth16) to assess performance scalability
- Published work at **ISCA**, **HASP**, **PACT**, achieving **500-1000**× speedups over existing software baselines
- Building High-Level Synthesis and chiplet libraries for agile hardware design of ZKPs (zkSNARKs, zkSTARKs, zkVMs) for verifiable ML inference, blockchain, and image transformation

University of Michigan **Ann Arbor, MI**
Graduate Student Research Assistant *August 2020 – December 2021*
Accelerating Reconfigurable Architectures and Forward Error Correction

- Led software-side scaling of 36-core to 128-core Versa Architecture (published at **VLSI** and **JSSC**)
- Designed microarchitecture for 3-in-1 ECC Encoding Accelerator (LDPC, Polar, Turbo), co-authored **ISCAS** paper

Georgia Institute of Technology **Atlanta, GA**
Undergraduate Research Assistant *August 2018 – May 2020*
Hardware Root-of-Trust Based Integrity for Shared Library Function Pointers

- Devised malware attack on Global Offset Table & mitigation via HW Root-of-Trust, co-authored journal paper

Teaching Experience

New York University **Brooklyn, NY**
Teaching Assistant *January 2025 – May 2025*
Course: High-Level Synthesis for Scientific Computing (Graduate)

New York University **Brooklyn, NY**
Guest Lecturer *March 2025 – December 2025*
Course: CS-UY 2204 Intro to Digital Logic (Undergraduate)

University of Michigan **Ann Arbor, MI**
Teaching Assistant *January 2022 – May 2022*
Course: EECS 470 Parallel Computer Architecture (Graduate)

Patents

Accelerated Zero-Knowledge Proofs U.S. Provisional Patent Application No. 63/862,337, filed August 12, 2025.

Mentorship

Brendan Sweezey: *PhD in ECE* — Accelerating verifiable image transformation

Gaurav Kuwar: *MS in Computer Engineering* — Modular HLS frameworks for ZKP primitives; accelerating zkVMs

William Zimmerman: *BS in Computer Engineering* — HLS for elliptic curve arithmetic; verifiable attention layers

Selected Graduate Coursework

Parallel Computer Architecture (UMich, NYU)
Cryptography (NYU)
Cryptography of Blockchains (Audited at NYU)
VLSI Design I, VLSI Design II (UMich)
Advanced Hardware Security (Georgia Tech)
Computer Architecture (Georgia Tech, UMich)
Deep Learning (UMich, NYU)
VLSI for Communications and ML (UMich)
Neural Signal Processing (Georgia Tech)
Probability (NYU)

Skills

Languages: C++/C, HLS C, SystemVerilog, Python, Rust, Scripting (Bash, TCL), RISC-V, VHDL, Standard ML
Tools: Catapult HLS, Vitis HLS, Design Compiler, Cadence, FPGAs, microcontrollers

Work Experience

Systems and Technology Research **Boston, MA**
Cyber-Physical Systems Intern *April 2018 – August 2018*
Programming Languages for Software-Defined Hardware

- Designed and implemented programming language features in MITCHELL (Standard ML) to target accelerated hardware for data-intensive algorithms, showcasing its parallelism through NLP workloads
- Built an end-to-end proof-of-concept pipeline—from algorithm design in MITCHELL to custom low-level libraries and hardware-accelerator simulation