Nikola Samardzic

US Citizen | phone: +1-857-244-5304 | mail: nsamar@csail.mit.edu | web: n-samar.github.io

EDUCATION

Massachusetts Institute of Technology Boston, MA
Ph.D. Computer Science Sept. 2020 – May 2024 (expected)

- Advisor: Prof. Daniel Sanchez

M.Sc. Computer Science Sept. 2020 – May 2022

- Coursework: computer architecture, computer networking, distributed systems, algorithms engineering, machine learning, geometric computing.

University of California, Los Angeles Los Angeles, CA
B.Sc. Computer Science Sept. 2016 – June 2020

- Research advisor: Prof. Jason Cong; GPA: 3.98/4.00 (Summa Cum Laude and Phi Beta Kappa)
- Extensive math and theoretical computer science coursework: stochastic processes, linear algebra (honors), probability theory, algebra (honors), analysis (honors), complex analysis (honors), Galois theory, number theory, systems of differential equations,etc.

RESEARCH CONTRIBUTIONS

- Drove the design of a hardware accelerator for computation on encrypted data that improves state-of-the-art performance by >1,000x.
- Drove the design of and implemented a compiler that automatically translates arbitrary PyTorch neural network models into programs that run model inference *on encrypted data*, targeting both CPUs and our accelerator.
- Designed and implemented an FPGA-accelerated quotient polynomial computation engine that improves end-to-end zero knowledge proof generation time by 50% over state-of-the-art.
- Implemented the fastest sorting accelerator in the 4-60GB range, using FPGAs.

WORK EXPERIENCE

- **Ulvetanna (Intern, 2023):** Designed and implemented the first FPGA-accelerated quotient polynomial computation (QPC), a key kernel in zero knowledge proofs (ZKPs); improved QPC price-performance by 9x over state-of-the-art. This improves ZKP performance in Ulvetanna's server by 50%. Ulvetanna's business model is based on providing fast and cheap ZKPs.
- **NAND Capital (Intern, 2020):** I was the first employee in a three-person hedge fund start-up funded by Founder's Fund and Paradigm; Developed basic data pipelines for running experiments on large amounts of market data. Used the pipeline to find predictable trends in markets.
- **Goldman Sachs (Intern, 2018):** Created custom NLP model for performing a specific accounting classification task that was previously performed full time by two employees.
- **SpaceX (Intern, 2017):** Created software to automate defining and testing of all propulsion joints on SpaceX rockets; Was offered to leave school and begin full time work as a freshman.

RECOGNITION & PUBLICATIONS

- Over 350 citations since start of PhD. 214 citations in 2023.
- Best MIT Electrical Engineering and Computer Science Master's Thesis award for 2023 (3 awardees per year).
- F1, my first-author publication, received the MICRO 2021 TopPicks award, which "collects some of the most significant research papers in computer architecture based on novelty and potential for long-term impact." It is awarded to only 12 papers annually.
- Research funded by National Science Foundation (NSF), Defense Advanced Research Projects Agency (DARPA), Google, Samsung, Wistron, and the MIT Fellowship.
- Bronze medal at the International Junior Science Olympiad in Tehran, Iran.

Selected Publications:

- **Nikola Samardzic***, Simon Langowski*, Srinivas Devadas, Daniel Sanchez. Accelerating Zero-Knowledge Proofs Through Hardware-Algorithm Co-Design. (under submission)
- **Nikola Samardzic***, Aleksandar Krastev*, Simon Langowski, Srinivas Devadas, Daniel Sanchez. Fhelipe: A Compiler and DSL for Tensor Programming in Fully Homomorphic Encryption. (under submission)
- **Nikola Samardzic**, Daniel Sanchez. BitPacker: Enabling High Arithmetic Efficiency in Fully Homomorphic Encryption Accelerators. ASPLOS 2024.
- **Nikola Samardzic**, Axel Feldmann, Aleksandar Krastev, Nathan Manohar, Nicholas Genise, Srinivas Devadas, Karim Eldefrawy, Chris Peikert, Daniel Sanchez. CraterLake: A Hardware Accelerator for Efficient Unbounded Computation on Encrypted Data. ISCA 2022.
- **Nikola Samardzic***, Axel Feldmann*, Aleksandar Krastev, Srinivas Devadas, Ron Dreslinski, Christopher Peikert, Daniel Sanchez. F1: A Fast and Programmable Accelerator for Fully Homomorphic Encryption. MICRO 2021.
- **Nikola Samardzic***, Weikang Qiao*, Vaibhav Aggarwal, M.C. Frank Chang, Jason Cong. Bonsai: High-performance Adaptive Merge Tree Sorting. ISCA 2020.

*** indicates equal contribution**

AREAS & SKILLS

- Areas: computer architecture, computer systems, performance engineering, cryptography, FPGA, ASIC, compilers, HW/SW codesign, software engineering, ML performance.
- Skills: C++, Rust, Python, Verilog, Minispec/Bluespec, Linux, Excel.