Hang Su

http://nomadtype.ninja

Email : hs2nu@virginia.edu | TEL : +1-434-227-0299

Education

MAY 2021 expected — **University of Virginia**, Charlottesville, VA
Master of Science in Computer Science, GPA: 3.70
Thesis: *Shorter and Faster Post-Quantum Designated-Verifier zkSNARKs from Lattices*
Advisor: David J. Wu

AUG 2019 from Sep 2015 — **Shanghai Jiaotong University**, Shanghai, China
University of Michigan – Shanghai Jiao Tong University Joint Institute (UM-SJTU JI)
Bachelor of Science in Electrical and Computer Engineering, GPA: 3.10

Spring 2018 — Exchange Semester at **North Carolina State University**, Raleigh, NC
Courses: Logic, Programming Language, Interactive Game Design, Theoretical CS, Gpa: 4.0

Research Interest

Cryptography, Computer Security, Programming Language Theory.

Publication

Yuval Ishai, **Hang Su**, and David J. Wu. *"Shorter and Faster Post-Quantum Designated-Verifier zkSNARKs from Lattices"*

In 2021 ACM Conference on Computer and Communications Security (CCS). To appear.

Research Experiences

Current from Jan 2020 — **Research Assistant**, advised by Dr. David J. Wu, at University of Virginia
Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zkSNARK) from Lattice-Based Assumption

- Implemented a lattice-based post-quantum zkSNARK over extension fields with smaller parameters.
- Designed an concrete-efficient Module-Learn-With-Error (MLWE) based encryption scheme.
- Developed a variant Fast Fourier Transform (FFT) over cosets for fields with small characteristics.
- Built a high-performance proof-of-concept implementation fully using **C++**.
- Obtained **10.3× smaller** proof size than previous post-quantum candidates.
- Achieved **39.4× smaller** proof size and **60.2× faster** prover than previous lattice-based assumption, all while achieving a much higher level of soundness.
- Published a first-authored full length paper at ACM CCS 2021, Seoul, South Korea.

Spring 2018 — **Research Assistant**, advised by Dr. Tim Menzies, at North Carolina State University
Topic Modeling in Human-Readable Structure

- Developed a faster and more succinct topic modeling method based on Latent Dirichlet Allocation.
- Accelerated topic classification within a tolerable range of error.
- Comprehended the mechanism of state-of-art practical data mining skills.

Fall 2017 — **Research Assistant** at Emerging Computing Technology Laboratory, Shanghai Jiaotong University
Logic Circuit Delay Decrease and Approximate Logic Synthesis Algorithms

- Proposed applying max-flow min-cut algorithm on approximated Boolean Function.
- Developed a robust library for parsing BLIF format logic circuit file.
- Built a rapid logic circuit simulator by translating target circuit into **C++**, and benchmarking over compiled code. Simulator achieved **over 5,000× speed-boost** than naive implementations.

Selected Projects

Fall 2019 — **SIMP (Simple IMperative Language)** at University of Virginia, CS6620 (Compiler)
Implemented a C-like imperative language based on LLVM and ANTLR.

- Implemented Hindley-Milner type system and type annotation syntax.
- Supported function definition, macro definition in types and variables.
- Utilized LLVM to generate an intermediate representation and an executable file.

Fall 2018 — Online **C/C++** auto-grader web application for CS courses, UM-SJTU JI

- Deployed grading tasks on ubuntu server and isolated execution through Dockers.
- System withstood the test for over 100 students till now without any failure or crash.

Spring 2018 — **Pyskell (Haskell DSL in Python)** at North Carolina State University, CSC495 (Programming Language)

- Comprehended Hindley-Milner inference and provided an implementation based on Union-Find.
- Integrated the type signature with Python syntax through Python decorator syntax.
- Produced a set of typeclasses, including '`Eq`' and '`Enum`', to further simplify the syntax.
- Created a lazy list like Haskell with infinite length through Python generator.

Fall 2017 **Multi-Threaded Database** at Shanghai Jiaotong University, VE482 (Operating System)

- Re-designed database and separated the parallel components from the sequential components.
- Debugged through the rewritten code and eliminated deadlock situations.
- Boosted the performance of the database by 5 time on a machine with 4-core CPU.

Fall 2017 **Five-Stage MIPS CPU** at Shanghai Jiaotong University, VE370 (Intro to Computer Organization)

- Created basic memory usage instructions, arithmetic-logical instructions and jump instructions.
- Understood the two-level data hazard detection and two-level load use hazard.
- Simulated the CPU behavior with Vivado simulator and successfully ran on a FPGA board.

Services

Undergraduate Teaching Assistant since 2018, served more than 200 students in UM-SJTU JI.

Summer 2018	Intro to Signal and Systems	Assisted instructor in designing exams and assignments.
Fall 2018	Operating System	Maintained and developed auto grading server; held lab sessions.

Programming Languages & Skills

Languages	Proficient: `C/C++`, `Python`, `Haskell`; Intermediate: `Latex`, `Scheme`, `Shell`, `Verilog`
Technology	`Unix`, `Git Version Control`, `Docker`