

Hang Su

<http://nomadtype.ninja>

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

EDUCATION

- MAY 2021 **University of Virginia**, Charlottesville, VA
expected 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 **Shanghai Jiaotong University**, Shanghai, China
from SEP 2015 *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

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** **Research Assistant**, advised by Dr. David J. Wu, at UNIVERSITY OF VIRGINIA
from JAN 2020 *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.
 - 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 Docker.
 - System withstood the test for over 100 students till now without any failure or crash.

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