Hang Su

Cryptography Engineer, Polyhedra

Email: hs2nu@virginia.edu
Website: https://nomadtype.ninja

Research Interest

Cryptography, Computer Security, Theoretical Computer Science (in general aspect).

Education

University of Virginia (UVA), Charlottesville, VA, USA — Sept 2019 – May 2021
M.S. in Computer Science
Thesis: *Shorter and Faster Post-Quantum Designated-Verifier zkSNARKs from Lattices*
Thesis Advisor: David J. Wu

Shanghai Jiao Tong University (SJTU), Shanghai, China — Sept 2015 – Aug 2019
B.S. in Electrical and Computer Engineering

Publications

[1] **Jolt-b: Recursion Friendly Jolt with Basefold Commitment**
Hang Su, Qi Yang, Zhenfei Zhang
IACR eprint, 2024

[2] **Shorter and Faster Post-Quantum Designated-Verifier zkSNARKs from Lattices**
Yuval Ishai, Hang Su, and David J. Wu
ACM Conference on Computer and Communications Security (**CCS**), 2021

Research Experiences

Research Assistant, advised by David J. Wu, at **UVA** — Jan 2020 – May 2021
Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zkSNARK) from Lattice-Based Assumption

- Obtained **10.3**× **shorter** proof than previous post-quantum candidates.
- Achieved **42**× **shorter** proof, **60**× **faster** prover, and **a much higher level of soundness** than prior lattice-based zkSNARKs.
- Compared to the most efficient pre-quantum zkSNARKs by Groth, our prover and verifier are faster (by **1.2**× and **2.8**×).

Industry Experiences

Cryptography Engineer, at **Polyhedra**, Boston, MA, USA — Oct 2024 – present

Cryptography Researcher, at **Cysic Labs**, Boston, MA, USA — Oct 2023 – Oct 2024
Supervised by Xiong Fan and Zhenfei Zhang

Software Engineer, at **Algorand**, Boston, MA, USA — github.com/ahangsu
Protocol Engineering — Mar 2023 – Sept 2023

- Prototyped the TEAL assemble language's debugger with support for the Debug Adapter Protocol (DAP).
  - Allows users to set breakpoints, step forward/backward, and inspect runtime variables.
- Introduced new features in simulate endpoint to evaluate transactions locally, without committing them to the network.
  - Enhances flexibility in live chain data querying through utilizing TEAL as a query language.
  - Empowers smart contract debugging over live chain data.

Programmability Engineering — Jul 2021 – Mar 2023

- Lead the design and development of PyTeal, a feature-rich Python library for Algorand smart contract development.
- Prototyped Application Binary Interface (ABI) for efficient and standardized interoperation between smart contracts.
- Implemented new features for Algorand SDKs to interact with network effortlessly.

Services

External Reviewer ICALP 2022

Teaching

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

Summer 2018	VE216: Intro to Signal and Systems	Assisted instructor in designing exams and assignments.
Fall 2018	VE482: Operating System	Maintained and developed auto grading server; held lab sessions.

Open-Source Contributions

Jolt, Official implementation of Jolt zkVM in Rust. Jul 2024 – Aug 2024
`https://github.com/a16z/jolt`

go-algorand, Official implementation of Algorand protocol in Golang. Jul 2021 – Sept 2023
`https://github.com/algorand/go-algorand`

PyTeal, Python library for Algorand smart contract, compiles to Algorand assembly language TEAL. Jul 2021 – Mar 2023
`https://github.com/algorand/pyteal`

AVM-debugger, Debugger for AVM adhering to the Debugger Adapter Protocol. Jul 2023 – Sept 2023
`https://github.com/algorand/avm-debugger`

Skills

Computer Skills	Languages	`C/C++, Python, Haskell, Rust, Golang, OCaml, Scheme, Shell, Coq,` LaTeX
	Technology	`Linux, Git Version Control, Docker`
Languages	(Almost) Native	Chinese, English
	Still learning	Japanese (Fluent), German (Beginner), Hebrew (Beginner), Espanol (Beginner)