Wei Jie KOH

Los Angeles, CA | contact@kohweijie.com | github.com/weijiekoh | kohweijie.com

Cryptography engineer experienced in zero-knowledge systems, client-side optimisations, and smart contracts.

Work Experience

Independent Researcher Jul 2024 — Present
Bain Capital Crypto *USA*

- Researched optimisations for Montgomery multiplication and the security of trusted execution environments.
- Executed due diligence on startups to assist in the firm's investment decisions.

Researcher Jan 2024 — Jul 2024
Geometry Research *Remote*

- Implemented secp256k1/r1 and ed25519 WebGPU shaders to accelerate signature verification for Fuel Labs.

Cryptography Researcher May 2022 — Jan 2024
Geometry Ventures *Remote*

- Published explanatory articles on state-of-the-art protocols.
- Performed technical research and due diligence on early-stage startups and projects.

Cryptography Engineer Jun 2019 — Dec 2021
Ethereum Foundation (Privacy & Scaling Explorations) *Remote*

- Pioneered user-facing zero-knowledge tools to enhance privacy in the Ethereum ecosystem.
- Built circom circuits and EVM contracts for the Semaphore and MACI projects.
- Worked with external security auditors to harden mission-critical components.
- Coordinated the Perpetual Powers of Tau ceremony with 70+ participants.
- Tracked, evaluated, and coordinated grantee milestones.

Software Engineer May 2018 — Jun 2019
ConsenSys Solutions *Singapore*

- Wrote EVM smart contracts to enable on-chain trading of security tokens.
- Collaborated with ConsenSys Diligence on a security audit.

Featured Projects

Optimised CM31 Number Theoretic Transform	https://github.com/worldfnd/ProveKit/tree/main/cm31_ntt
WebGPU-accelerated signature verification	https://github.com/FuelLabs/wgpu-sigops
Semacaulk	https://github.com/geometryxyz/semacaulk
secp256k1 hash-to-curve in circom	https://github.com/geometryxyz/secp256k1_hash_to_curve
Minimum Anti-Collusion Infrastructure	https://github.com/appliedzkp/maci
Perpetual Powers of Tau	https://github.com/weijiekoh/perpetualpowersoftau
Semaphore	https://github.com/appliedzkp/semaphore

Awards

ZPrize 2023 Oct 2023 — Mar 2024

- Special Mention (Best WebGPU Solution) for Multi-Scalar Multiplication

Selected Articles

- A Deep Dive into Logjumps: a Faster Modular Reduction Algorithm
- Optimizing Montgomery Multiplication in WebAssembly
- Hashing to the `secp256k1` Elliptic Curve
- Semacaulk, a gas-efficient zero-knowledge set membership protocol
- Deanonymising the Kucoin Hacker
- Announcing the Perpetual Powers of Tau Ceremony to benefit all zk-SNARK projects
- Private voting and whistleblowing in Ethereum using Semaphore

Talks

- zkParis: Deep Dive into WebGPU
- Solidity Singapore: Simple Private Information Retrieval (SimplePIR)
- ZK Podcast: MACI with Koh Wei Jie
- ZK Podcast: Trusted Setup Ceremonies Explored
- DevCon Osaka: A trustless Ethereum mixer using zero-knowledge signalling
- DevCon Osaka: Hands-on Applications of Zero-Knowledge Signalling

Skills

- **Programming Languages**: Rust, C, Typescript, Solidity, Python, WGSL, circom.

Education

Yale-NUS College 2013 — 2017
BA in Anthropology *Singapore*

- Graduated with the pioneer class of Singapore’s first liberal arts college.
- Capstone project: *The Syncretic Imagination of a New Religious Movement in Singapore*.

Yale University Spring 2015
Visiting International Student Program *New Haven, CT*

- Completed courses in human rights and philosophy.