Koh Wei Jie

Profile

Wei Jie is an senior applied cryptography and software engineer specialising zero-knowledge proofs and smart contracts. He has built decentralised applications that combine production-grade software engineering with zero-knowledge circuits, on-chain protocols, and privacy-preserving design.

Homepage

kohweijie.com

Contact details

contact@kohweijie.com
https://github.com/weijiekoh

Personal information

Permanent residence and employment authorisation: USA
Citizenship: Singaporean
Current residence: SF Bay Area
Languages: English (native), Mandarin (conversational)

Programming languages

Most frequently used: Rust, JS/TS, and Python.
Working knowledge of: WGSL, Perl, C, Java, SQL, and R.

Experience

Technical Lead at Renegade. **2026.01–present**

- Maintained production and testnet systems for dark pools deployed on Base and Arbitrum handling US$90M per year of DEX liquidity.
- Improved the stability and reliability of the startup's market-maker hedging mechanism.
- Implemented trading infrastructure for version 2 of the protocol.

Independent Researcher at Bain Capital Crypto. **2024.07–2025.04**

- Implemented and optimised the number-theoretic transform algorithm for the complex M31 field extension to contribute to Tools for Humanity's next-gen client-side proof generation efforts.
- Wrote *A deep dive into Logjumps: a faster modular reduction algorithm* to explain, algorithmically, a newly discovered modular reduction technique for large prime fields.
- Wrote *Optimizing Montgomery Multiplication in WebAssembly* to showcase optimisation techniques for large-prime field multiplications in web browsers.

Researcher at *Geometry Research*. **2024.01–2024.07**

- Implemented ECDSA signature recovery for the secp256k1 and secp256r1 elliptic curves, as well as EdDSA signature verification for curve25519 in WebGPU.

Researcher at *Geometry*. **2022.05–2024.1**

- Performed investment thesis research, technical due diligence, and mentored early-stage startups and projects.
- Implemented hash-to-curve (RFC 9380) in `circom` for secp256k1.
- Built Semacaulk, a gas-efficient ZK set membership gadget.
- Implemented cryptographic algorithms in WebGPU, including the Poseidon hash function. Won a Special Mention (Best WebGPU Solution) for MSMs at ZPrize 2023.

Software Engineer at *AppliedZKP*, *Ethereum Foundation*. **2019.06–2021.12**

- Built Semaphore, a privacy gadget for ZK set membership proofs.
- Built MACI, a bribery-resistant quadratic voting system. Collaborated with clr.fund to deploy multiple public goods funding rounds, facilitating US$10,000s of USD contributions.
- Facilitated the Perpetual Powers of Tau ceremony, a phase-1 trusted setup for the BN254 elliptic curve.
- Built ZK developer tools including `circom-helper` and `zkey-manager`.

Software Engineer at *ConsenSys Singapore*. **2018.05–2019.06**

Education

BA in Anthropology. *Yale-NUS College (Singapore)*. **2013–2017**

Diploma in Information Technology. *Ngee Ann Polytechnic (Singapore)*. **2007–2010**