

Xiangan He

617-710-4886 || xianganhe.com || xiangan9@gmail.com || [linkedin.com/in/xianganhe](https://www.linkedin.com/in/xianganhe) || github.com/xBalbinus

Experience

Software Engineer

June 2022 - November 2023

Warp (formerly Illusory Systems)

- Developed and enhanced continuous integration (CI) pipelines on GitHub.
- Created a dockerized end-to-end testing tool, accelerated the recovery of \$200M of hacked assets.
- Designed and implemented a website staging environment, development server, and trigger Lambda functions using a variety of services (including WireGuard, AWS WAF, Route53, CloudFront, S3, EC2), enhancing system security.

Software Engineer

August 2023 - November 2023

Protocol Labs

- Developed REST API for storing & fetching data from Filecoin Virtual Machine receiving 10M+ requests/day.
- Worked with team leaders to develop a standard protocol managing data storage deal creation on Filecoin network.
- Built and maintained multiple fullstack web-applications visualizing network activity and static sites for conference events.

Cryptography Associate

May 2023 - August 2023

Trail of Bits

- Developed static analysis tool for detecting bugs in zero-knowledge circuits, outperformed state of the art by 100x reduction in memory usage and 10x increase in speed (Rust).
- Improved a DARPA-funded tool for generating zero-knowledge proofs of exploitability, by creating binary imitations of systems (Verilog, Assembly).
- Audited and reported denial of service bugs in a cryptography audit on a wallet privacy protocol, shadowed audits on cryptographic systems such as Twitter's private-messaging feature.
- Evaluated an implementation of the CGGMP21 threshold signature scheme over the secp256k1 curve (Go).

Security Engineer

July 2022 - May 2023

Veridise

- Built automated formal verification tooling used in the Security-as-a-Service product (Python, C++).
- Engaged 20+ security audit clients, reporting vulnerabilities and penetration testing to safeguard \$50M+ in funds.
- Automated the security assessment report production process by generating LaTeX from Notion exports via a CLI tool.

Application Security Auditor

February 2022 - June 2022

Yearn Finance

- Collaborated with security teams to develop and enhance security policies, measures, and procedures
- Conducted security assessments, vulnerability scans, and penetration testing against decentralized finance protocols.
- Provided support in incident response and resolution activities by isolating affected systems preventing further exposure.

Technical Skills

Languages: Solidity, Python, Rust, Go, C/C++, Javascript/Typescript, Java, HTML/CSS, R, Circom, Verilog, Assembly, LaTeX

Frameworks: React, Node.js, NextJS, JUnit, Pytest, AWS CDK, ElectronJS

Developer Tools: Git, Docker, Kubernetes, VMWare, BurpSuite, Binary Ninja, VSCode, Foundry, Hardhat

Libraries: SMTLIB, pandas, NumPy, Matplotlib, PyTorch, Tensorflow

Open-Source Projects

Python Project Index

- Implemented additional event-based emailing triggered whenever users add an email to their account.

BuildGuild, Fullstack Contributor

- Built several fullstack decentralized application templates for rapid prototyping and productionizing.

Semiotic, Cryptography Engineer

- Worked with the lead cryptographer to build data relayers, zero-knowledge circuits and verifiers for cross blockchain bridge.

Honors & Awards

- Protocol Labs Impact Evaluator (top 3 of 122 teams); Developer Grants Recipient (2023)
- Gates Scholar (300 out of 34000+)
- ETHGlobal HackMoney, Marketmake, Road to Web3 Best Hack Award Winner (2020-2021)
- ParadigmCTF 2022 (13th out of 200+ teams)

Education

Boston College

September 2021 - May 2024

- Bachelor of Science in Computer Science, Math, Finance. Honors.
- Research Assistant under Prof. Lewis Tseng and Prof. Donglai Wei, focusing on Distributed Systems and Artificial Intelligence.
- Publication: "Zephyr: An Economically Feasible Zero-Knowledge Light Client" (Abstract, [ACM SIGMetrics Performance Review](#))