

# THOR KAMPHEFNER

[thorck@pm.me](mailto:thorck@pm.me) • [github](#) • [twitter](#) • [linktree](#) • San Francisco, CA

I am an zero knowledge cryptography engineer and educator. My work tends to alternate between implementations of novel zero-knowledge proof systems, such as Protostar and STARKs, and educational initiatives, such as the Uncloak Cryptography Engineering course, a 16 module course on general cryptography engineering practices. I also co-organize industry events, most notably ZK Hack Hackathon series.

## EXPERIENCE

---

### Implementing zk-news

Jan 2024-Present

Implementing a hacker-news style discussion board, in coordination with the ZK Hack Discord group, intended to complement the ZK Mesh newsletter, and facilitate cross-domain communication in zero knowledge. Initial release expected March 2024.

### Stone Prover Reimplementation Grantee

Nov 2023-Present

In September 2023, Starkware open-sourced their proving library, the Stone Prover, a C++ library for generating FRI proofs over AIR traces generated from Cairo Assembly (CASM) programs. In the interest of developing an option for client-side proving, I am currently developing a minified Rust re-implementation of the Stone Prover, called [Pebble Stark](#).

### Uncloak Cryptography

Nov 2022-Apr 2023

[Uncloak](#) is a fledgling cryptography wiki and cryptography engineering course, aiming to increase the accessibility of cryptography engineering as a discipline for interested software engineers, supported under a grant by the Ethereum Foundation.

### Zuzalu Hackathon Winner

Apr 2023

Won the Zuzalu 2023 Hackathon for [partial implementation](#) of the CCS generalized arithmetization scheme, with Waylon Jepsen and Shumo Chu.

### Proofs Arguments and Zero Knowledge Study group Co-runner

Dec 2021-Dec 2022

Initiated and co-ran the Zero Knowledge [cryptography study group](#) with the good [Dr. Justin Thaler](#), which you can find through [the zkHack discord server](#).

### ZK Hack Co-organizer

Apr 2023, Nov 2023

Co-organized [ZK Hack Lisbon](#) and [ZK Hack Istanbul](#), a series of zero-knowledge hackathons.

### Lead Cryptography Engineer at Entropy Cryptography

Nov 2021-Nov 2022

Led cryptography engineering at [entropy](#), a trustless, chain-agnostic asset custodian, built with threshold signatures, and the Substrate blockchain building framework. Designed and implemented the [GG20](#) threshold signature scheme.

### Paper coauthor: Combining GHOST and Casper

Dec 2018-July 2019

coauthored a mathematical security paper with my mentor Yan Zhang analyzing the security and liveness properties of the Ethereum 2.0 beacon chain consensus protocol. [Paper Link](#).

- 
- Education: San Jose State University, BA Applied Mathematics: 2015 – 2020
  - [Assorted talks](#)