# Conghao Shen

First Year Computer Science Master Student with Systems Specialization
Stanford, California, US | +1 (510) 387-8301 | tom.shen.cn@gmail.com
https://github.com/tsunrise | https://www.linkedin.com/in/conghao-shen-b179b5169/ | https://tomshen.io

## PROFESSIONAL SUMMARY

I am a first-year Master's student in Computer Science from Stanford University, with a focus on Systems. I am excited to build efficient, scalable, and secure systems with my engineering skills. I started coding in high school and have experience in various areas, from a simple full-stack web application to efficient secure multi-party computation protocol.

## EDUCATION

**Master of Science, Computer Science, Stanford University** **Expected Graduation June 2024**

- Intended Specialization in Systems

**Bachelor of Arts, Computer Science, UC Berkeley** **Graduated May 2022**

- GPA 3.98/4.0, Dean's List, Honors to Date
- Coursework: Algorithms, Computer Security, Programming Languages, Operating Systems, Machine Learning, Probability theory

## WORK EXPERIENCE

**Software Engineering Intern, Arista Networks** **May 2021 - Aug 2021**

- Developed backend to connect REST APIs to interact with low-level endpoints of network switches.
- Wrote automation tests to check the correctness of existing logic without time-consuming deployment.
- Refactored old Java codebase to Go backend, without affecting backward compatibility.

## PROJECTS

**Coauthor, LISA (Lightweight Secure Aggregation for Federated Learning)** **Paper Submitted August 2022**

- Built a secure aggregation multi-party computation system for federated learning under distributed trust model.
- Wrote a performant server that was required to handle 50k client connections simultaneously.
- Designed a customized application layer over TCP, using message queue idiomatic to allow multiple threads to share one socket safely.
- Used Rust asynchronous programming to reduce CPU idle time for an IO-heavy application.

**Contributor, Arkworks (https://github.com/arkworks-rs)** **May 2020 - May 2022**

- A collection of libraries (crates) in Rust for building a zero-knowledge proof system.
- Implemented state-of-the-art cryptographic primitives such as the low-degree test using FRI, cryptographic sponge, polynomial commit scheme, and Merkle Tree.
- Built complex protocols like interactive oracle proof systems in Rust with proper documentation.

**Contributor, Manta Network DeFi (https://github.com/Manta-Network/manta-rs/)** **Sep 2021 - Present**

- Build a server for "trusted setup", a ceremony for many proof systems used by decentralized finance.
- Integrated cryptographic algorithms like Poseidon hash function to current codebases.
- Audited and reviewed pull requests and provide constructive feedback when requesting changes.

**Course Project, Lisp Compiler** **Sep 2021 - Dec 2021**

- Used OCaml to implement a lisp-style compiler to x86 assembly.
- Added supports for arithmetic, variables, heap allocation, closure with capture, and optimizations like inlining, constant propagation, and common subexpression elimination.

## SKILLS

**Programming Languages**: Proficient in Rust, Python, C, Java, Go. Familiar in Typescript, JavaScript, HTML/CSS, OCaml.
**Technologies/Frameworks**: React, PyTorch, Tokio-rs, Git, Gerrit, Cloudflare Workers, AWS