Conghao Shen

(510)-387-8301 tomshen@berkeley.edu tomshen.io

EDUCATION

University of California - Berkeley, CA **May 2022**

Computer Science B.A. GPA:3.98/4.00

Relevant Coursework: CS170: Algorithms **CS161:** Computer security **CS162:** Operating Systems **CS189:** Machine learning **CS188:** Artificial Intelligence **Math 113:** Abstract Algebra **DATA100:** Data Science **CS61B:** Data Structures **CS61C:** Machine Structures **CS70:** Discrete Mathematics and Probability Theory **CS61A**

SKILLS

Coding Experience: Proficient: Rust, Java, Python, Go, C. Familiar: OCaml, JavaScript, C++

Skills: common data structures and algorithms, cryptography (common symmetric/public key encryption algorithm, interactive proofs, etc.), basic web skills (React, Go), data analysis (classic regression & classification methods)

HIGHLIGHTED PROJECTS & EXPERIENCE

Summer Internship — Summer 2021

Arista Networks, Santa Clara, CA

- Develop backend to connect web interface to low-level interaction with network switches.
- Write efficient programs that can be synchronized in multi-container environment.
- Design integration tests to test correctness of existing logic without expensive deployment to VM.

CIFAR-10 Image Classification — Spring 2021

Course Project: CS189: Introduction to Machine Learning

- Implement forward and backprop for fully connected layers, ReLU layers, softmax, and CNN layers in numpy. Then switched to pytorch and implemented and training ResNet-18 for CIFAR-10.
- Achieved **rank 8** over 421 students on public leaderboard. (Accuracy = 0.924)

End-to-End Encrypted File Sharing System — Spring 2020

Course Project: CS 161: Computer Security – UC Berkeley

- Develope a secure file storage/sharing system that uses untrusted data server.
- Use symmetric encryption with PKCS5 padding and message authentication code to ensure confidentiality and integrity of user's file even if attacker has whole access to the data server. Encryption method is IND-CPA secure.
- Derive user's private key from password, using salting and slow hash functions to prevent dictionary attack.
- User can share file and revoke access to another user in constant time (regardless of the size of file)
- Use digital certificates to ensure authenticity (access tokens sent by users are signed)
- Our team is one of ten teams (out of $\geqslant$100 teams in spring semester) whose final submission survived all hidden attacks.

RESEARCH & EXTRACURRICULAR ACTIVITIES

Cryptography and ZK-SNARKS — Starting from Summer 2020

Advised by Professor Alessandro Chiesa at UC Berkeley

- Implement efficient cryptographic algorithms like univariate sumcheck, merkle tree, and univariate low degree test.
- Write arithmetic circuits for some verifier algorithms so they can be compiled to R1CS constraints system.
- Design interface for interactive oracle proof and an algorithm to convert an public-coin interactive protocol to SNARK.
- Go to https://github.com/tsunrise to see my contributions.

Eiffel – Secure Federated Learning protocol — Starting from Summer 2021

Advised by Professor Raluca Ada Popa at UC Berkeley

- Paper working in progress: a significant improvement compared to Prio+
- My contribution: develop efficient asynchronous client-server system in C++ where each server is required to hold more than 16000 concurrent connections; write some implementation of cryptographic algorithms described in paper.