Conghao Shen

Berkeley, CA (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: Python, Rust, Java, C. Familiar: Go, 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

- Internship in progress: develop cluster-based control web backend for network switches.
- Deploy go code over containerized services in remote clusters.

CIFAR-10 Image Classification — Spring 2021

Course Project: CS189: Introduction to Machine Learning

- Implemented 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

- Developed 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 ⩾100 teams in spring semester) whose final submission survived all hidden attacks.

An Approximation Algorithm for an NP-Hard Problem — Spring 2020

Course Project: CS 170: Algorithms – UC Berkeley (https://github.com/tsunrise/cs170-proj)

- Given a positive weighted, connected, undirected graph, estimate a connected dominating set that minimizes the average pairwise distance between nodes. This model helps telecommunication companies to build cell tower and cables at low cost.
- Our final submission ranked 5th among 309 teams.
- Algorithm uses randomized decisions and heuristics to reach local minimum in few iterations.
- Program uses artificial bee colony algorithm and multiprocessing to speed up computation.

RESEARCH & EXTRACURRICULAR ACTIVITIES

Research Intern — Starting from Summer 2020

Cryptography and ZK-SNARKS

RISELAB - *UC Berkeley*

- Implemented efficient cryptographic algorithms like Sumcheck, Merkle tree, and cryptographic sponge functions.
- Writing R1CS constraints for basic polynomial operations and Merkle trees. Those constraints are helpful for interactive oracle proofs of knowledge.
- Go to https://github.com/tsunrise to see my contributions.

Last Updated: 5/25/2021