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: 3.971/4.0

Relevant Coursework: **CS170:** Algorithms **CS161:** Computer security **CS61A:** The Structure and Interpretation of Computer Programs **CS61B:** Data Structures **CS61C:** Great Ideas of Computer Architecture (Machine Structures) **CS70:** Discrete Mathematics and Probability Theory **EE16A:** Designing Information Devices and Systems **CSC8:** Foundations of Data Science

SKILLS

Coding Experience: Proficient: Python, Java, C. Familiar: C++, PHP, Go, Javascript
Skill Set: common data structures and algorithms, cryptography (AES-CTR/AES-CBC, public key encryption, certificate chain, hashing), web skills (React, Go), parallelism (OpenMP, Go, Intel Intrinsics)
What I am working on this semester: Advanced Algorithms, Cryptography, memory safety

HIGHLIGHTED PROJECTS & EXPERIENCE

✂ **Byte Scissor** Fall 2019

Personal Project: https://github.com/tsunrise/ByteScissor)

- Implemented a secret sharing scheme, using C++.
- The tool splits a file into fragments. File can be restored if required amount of fragments (any of those) are recovered.
- Wrote finite-field arithmetic code (add/substract/multiply/inverse) to speed up calculation and avoid overflow error.
- Designed a file format to compress fragment size by 50% and added sanity check to ensure basic data integrity.
- Used OpenMP to speed up program by 4x on common personal computers.

🔒 **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)

🎮 **Game: CYBERSNAKE** Spring 2019

Course Project: CS 61B: Data Structures – UC Berkeley (Demo: https://tomshen.io/goto/snake.html)

- Cooperated with another team member using a shared repository to write a Java multi-player game from scratch
- Built frameworks and kernel supporting clock, data saving, user I/O by myself.
- Wrote well-documented Java interfaces to allows other programmers to write plugins easily.
- Built various tests, including randomized tests and edge cases.

LEADERSHIP & EXTRACURRICULAR ACTIVITIES

UC Berkeley EECS Department - *Academic Intern* Fall 2019

- Supported weekly sections of 50+ students.
- Helped students to debug the code and understand core concepts such as trees, heaps, asymptotic, etc.

CalHacks 2019: 48 hour hackathon - *Team Lead*

- Developed the prototype of a social AR-based App. User can post notes anywhere (on the table, near a tree, etc) and others can see it using their camera. Used Google Cloud API for map data and Apple AR Kit.
- My contribution: use React to build an interactive map, showing the location of the post; assign work to other team members to allow efficient cooperation

3/13/2020