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(In Progress):** Operating Systems and System Programming **Math 113 (In Progress):** Abstract Algebra **DATA100:** Data Science **CS61B:** Data Structures **CS61C:** Machine Structures **CS70:** Discrete Mathematics and Probability Theory **CS61A**

SKILLS

Coding Experience: Proficient: Python, Java, Rust, 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

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.

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.
- Designed a file format to compress fragment size by 50% and added sanity check to ensure basic data integrity.

RESEARCH & EXTRACURRICULAR ACTIVITIES

Research Intern Starting from

Linear-time and zero-knowledge sum-check protocol for arithmetic circuit Summer 2020

SCIPR-Lab - *UC Berkeley*

- Focus on doubly efficient interactive proof protocol. Prover takes linear time and verifier takes logarithmic time to check that a general arithmetic circuit produces correct output, given the inputs.
- My role: develop efficient, safe, well-documented implementations of state-of-art algorithms and protocols on paper, using Rust.
- Implemented an interactive sum-check protocol and then used `blake-2s` hashing and Fiat-Shamir transform to allow both prover and verifier to do their jobs offline. Used traits and generics to allow others to extend the library easily.
- Deploy automated code inspection tools to ensure code quality.
- Actively cooperate and communicate with other members in the research group. Use polynomial commitment scheme built by others in my implementation of zero-knowledge sum-check.

Last Updated: 9/10/2020