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

Security | Algorithms | Data Structures | ML & AI | Compilers | Assembly | Operating System | Abstract Algebra | Machine Structures

Programming Languages: Rust, Java, Python, Go, C, OCaml, JavaScript, C++

EXPERIENCE

Summer Internship

Summer 2021

Arista Networks, Santa Clara, CA

- Develop backend to connect REST APIs to low-level interaction with network switches.
- Write efficient programs that can be synchronized in a multi-container environment.
- Design automation tests to check correctness of existing logic without expensive deployment to VM.

Course Projects

End-to-End Encrypted File Sharing System (CS161) Spring 2020

- Develop a secure file storage/sharing system that uses untrusted data server, where users can share files in constant time.
- Use symmetric encryption with proper padding and message authentication code to ensure confidentiality and integrity of the user's file even if the attacker has full access to the data server. The encryption method is IND-CPA secure.
- Derive user's private key from a password, using salting and slow hash functions to prevent dictionary attack.
- Our team is one of ten teams (out of $\geqslant$100 teams in the spring semester) whose final submission survived all hidden attacks.

CIFAR-10 Image Classification (CS189) Spring 2021

- 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 the public leaderboard. (Accuracy = 0.924)

RESEARCH

Cryptography and ZK-SNARKS

Starting from Summer 2020

Advised by Professor Alessandro Chiesa at UC Berkeley

Arkworks: Open-source crypto primitives (https://github.com/arkworks-rs)

- Build generic Merkle Tree where multiple CRH can be plugged in. Write circuits for path verification.
- Implement of low-degree test using FRI. FRI verifier also has its constraints that can be included in SNARKs.
- Work with others to build a cryptographic sponge using Poseidon, which can absorb and squeeze bytes, and field elements.
- Write code for polynomial commit scheme for univariate polynomial.

Interactive Oracle Proof Framework in Rust

- Design and build framework for public-coin IOP [BCS16] and RS-IOP [SCRSVW19].
- Implement BCS transform algorithm that converts and public coin IOP to succinct non-interactive proof.
- Many optimizations have been done, such as sharing multiple oracles in one Merkle tree and serializing by cosets.
- System building from scratch: ~10k lines of rust code.

Eiffel – Secure Federated Learning Protocol

Starting from Summer 2021

Advised by Professor Raluca Ada Popa at UC Berkeley

- Work on a paper WIP with two graduate students. This paper will be a significant improvement compared to Prio+, where many costly MPC such as Beaver Triple generation is generated by clients instead.
- My contribution: Implementation of an efficient asynchronous server that can handle more than 16000 concurrent client connections. Implementation of some crypto primitives for federated learning.