Yuwen Zhang

908-656-4092 | yuwen01@berkeley.edu | linkedin.com/in/yuwen01 | github.com/yuwen01

Education

University of California, Berkeley Berkeley, CA
Master of Science in Computer Science *Aug. 2023 – May 2024*

University of California, Berkeley 3.95
Bachelor of Arts in Computer Science, Minor in Mathematics *Aug. 2019 – May 2023*

Operating Systems, Machine Structures / Computer Architecture, Algorithms, Machine Learning, Linear Algebra

Experience

Cryptography Research January 2023 – April 2024
University of California, Berkeley Skylab *Berkeley, CA*

- Created a compiler to enable constant verifier communication for distributed verifier zero knowledge proofs.
- Augmented Prio, a private analytics platform, by enabling batch sanitization of client input.
- In a research prototype Prio-style analytics system, reduced end-to-end dollar cost by **2-3x**.
- Created a novel solution to the private heavy hitters problem, with up to **3.8x** dollar cost savings over prior work.
- To appear at IEEE S&P 2024.

Summer Backend Engineering Intern Jun. 2022 – Aug. 2022
Strava Inc. *San Francisco, CA*

- Developed Scala microservice backend for interactive maps and high level analytics for athlete outdoor activities
- Optimized rendered map data using RDP reduction and SIA smoothing algorithms for both visual clarity and load speed. Reduced file size by up to **54%**. Worked with frontend and mobile engineers to design an API contract.
- Implemented an Apollo GraphQL endpoint for serving recommendations for local sport types during a weeklong internal hackathon.

Summer Backend Engineering Intern Jun. 2021 – Aug. 2021
American Express *Phoenix, AZ*

- Used Go, Spring Boot Java, and Couchbase to create a containerized, synchronized backend REST API wrapper for replaying credit card transactions.
- Used Grafana and Prometheus to display resource consumption and other usage metrics.
- Wrote thorough tests and communicated effectively in an Agile scrum team with five other interns.

Projects

Space efficient Zero Knowledge Proofs Jan. 2021 – March 2023

- Designed a streaming algorithm to implement the PST13 polynomial commitment scheme in O(log N) space.
- Contributed to Arkworks, a popular open-source ecosystem for developing ZKPs.
- Experimented with streaming large R1CS files in repeated chunks for space efficient proof systems.

Secret Key Recovery Multi Party Computation Sept. 2022 – May 2023

- Designed a secure protocol for recovering lost secret keys using distributed trust, using an MPC circuit inspired by BGW and MP-SPDZ.

Technical Skills

Languages: C, C++, Rust, Java, Python, Scala, Go, React.js
Developer Tools: Git, Github, Docker, Google Cloud Platform, Microsoft Azure, VS Code, Visual Studio, IntelliJ
Libraries: Pandas, NumPy, Matplotlib, Tokio