Ganyu Xu

xuganyu96@gmail.com | +1-604-329-5822 | linkedin.com/in/ganyu-bruce-xu | github.com/xuganyu96

Education

U of Waterloo, MASc in Electrical and Computer Engineering, GPA 94.6/100 — Expecting May 2025

U of California, Berkeley, BA in Mathematics and Statistics, GPA: 3.464/4.0 — Sep 2015 – May 2019

Technical skills

Programming languages: Rust, Python 3, C, Bash, SQL

Cryptography & communication security: TLS, ECC, RSA, DSA, Diffie-Hellman key exchange, OpenSSL

Web development: Flask, Docker, AWS serverless stack, HTML/CSS, Linux, Apache Airflow, PostgreSQL/MySQL

Experience

Research assistant, University of Waterloo – Waterloo, Ontario, Canada — May, 2024 - Present

- Designed and implemented post-quantum cryptographic primitives and secure communication protocols

Senior data engineer, LeanTaaS Inc. – Santa Clara, CA, United States — July 2019 - Sep 2023

- Automated business analytics and legacy manual workflow for operioperative management in 100+ healthcare systems throughout the US
- Improved ETL pipeline scalability by migrating data ingestion from PostgreSQL to AWS S3 and moving Airflow's workers from EC2 to ECS
- Accelerated enterprise customer onboarding by automating manual data quality review, cutting onboarding timeline from 4 months to 1 month
- Increased developer productivity by containerizing development environment, building unit testing framework, and integrating CI/CD practices
- Reduced pipeline downtime by implementing service availability monitoring and engineer on-call alarms via DataDog
- Recruited and mentored junior developers through project design review, pair programming, and technical workshops

Projects

RustCrypto/crypto-bigint

- Implemented **finite field arithmetics** for heap-allocated big integers
- Ported stack-only random prime generation to heap-allocated big integers

RustCrypto/RSA

- Integrated Marvin toolkit for detecting timing variability in RSA implementation

rustls

- Identified incorrect TLS termination at google.com and fixed the example binaries to connect to other properly working TLS server

Apache Airflow

- Fixed improper exception handling in Python multiprocessing that causes critical process to become zombie instead of exiting upon database disconnect
- Fixed incorrect DagRun list view serialization that causes the webapp to crash when DagRun config is not JSON-serializable
- Implemented user-specified retries for `airflow db check`