Yuxiang Qiu

yuxqiu@proton.me | github.com/yuxqiu | yuxqiu.github.io Last updated in 2025-11-27

Education

University College London 09/2021 - 06/2025

MEng Computer Science

- **Grades**: First Class (1st year: 87%, rank: 1/150; 2nd year: 86%; 4th year: 85%)
- **Coursework**: Algorithms for Computer Systems, Computer Architecture & Concurrency, Decentralized Finance, Intro to Cryptography, Logic, Malware, Networked Systems, Security, Supervised Learning, Theory of Computation

Georgia Institute of Technology 08/2023 – 05/2024

BS Computer Science (Exchange Student)

- **GPA**: 4.0/4.0
- **Coursework**: Blockchain & Cryptocurrency, Compiler & Interpreter, Computer Graphics, Deep Learning, Design & Analysis of Algorithm, Processor Design, Quantum Computing

Experience

TensorZKP: Efficient Zero-Knowledge Proof Acceleration using Tensor Cores 09/2025 – Now

- Background: Existing systems, such as BatchZK, achieve high-throughput batched zero-knowledge proof generation on NVIDIA GPUs but fail to saturate memory bandwidth. We introduce **TensorZKP**, which accelerates batched proving for Libra- and Brakedown-based protocols by reformulating core operations as matrix multiplications and fully exploiting Tensor Cores and the Tensor Memory Accelerator.
- Research: **Designed matrix-multiplication-based formulations of linear-time sumcheck** to enable rapid proofs of polynomial-product sums and efficient evaluation table updates; discovered fixed-constant Barrett reduction (Shoup-style) can be applied to sumcheck table updates and reformulated it as two matrix multiplications.
- Implementation: **Built a high-performance reduction kernel** for matrix-multiplication outputs, supporting arbitrary primes with specialized optimizations for Mersenne and pseudo-Mersenne primes; **developed a custom GEMM kernel** inspired by DeepGEMM for **fast sparse matrix multiplication in Spielman-code linear-time encoding**, incorporating warp specialization and load balancing through inverted expander graphs.
- Advisor: Prof. Jiaheng Zhang and Dr. Tao Lu

Trustless Efficient Light Clients 10/2024 - 04/2025

- Background: Light clients enable resource-constrained devices to interact with blockchains but face scalability challenges due to linear-time verification and linear-size proofs. Current approaches are either not general-purpose (tied to specific chains and consensus mechanisms) or impose excessive burdens on provers.
- Research: Designed Mim, a general-purpose light client protocol that achieves **constant-size or logarithmic-size proofs** for committee rotations using folding-based SNARKs; introduced a **Merkle accumulator** into the protocol to solve the bootstrapping problem, reducing the frequency of expensive SNARK proofs and proof-generation time.
- Implementation: Authored 8,000+ lines of Rust using `arkworks` and `sonobe`; implemented a generic R1CS hash-to-curve for BLS12 curves; discovered and fixed **a completeness bug** in `arkworks` affecting emulated field variables.
- Experiment: Evaluated Mim on a Sui-like blockchain; single-day committee rotation proofs can be generated in **<12 hours** without accumulator, and one-year chain history can be proven in **<7 days** with accumulator (assuming sufficient memory), while maintaining **~1-3s constant verification time** regardless of chain length.
- Advisor: Prof. Philipp Jovanovic and Dr. Alberto Sonnino

TaskEval 06/2024 – 09/2024

UCL Software Optimisation, Learning and Analytics Research Lab *London, UK*

- Background: Recent advances in LLMs show the promise of using it to judge text quality. However, current methods lack interpretability and are vulnerable to adversarial attacks. To address this, we explored methods to score a software patch explanation by measuring how well an LLM can accomplish tasks with this explanation.
- Research: Reviewed 10+ available datasets; proposed LLM-as-a-judge as the baseline; evaluated and **enhanced 4 text perturbation methods**; **designed diversity metrics** and **improved diversity** of generated text.
- Implementation: Integrated SWE-bench and implemented fault localization and differential testing as tasks.
- Experiment: Designed and conducted experiments to analyze the performance (in terms of agreement, Kendall's Tau, and Spearman's correlation) in different settings (with CoT, different perturbations, etc.).

- Advisor: Prof. Federica Sarro and Prof. Sergey Mechtaev

Software Development Engineer Intern 06/2023 – 08/2023
Amazon *London, UK*
- Researched cross-platform portability of Java apps running on Windows, resulting in a ~10-page research report.
- Developed a Java application and library that performs **incompatibility detection at the bytecode** level (checking for 7 different types of cross-platform issues) with **~80% accuracy and 90%+ recall** on real-world JARs.
- Optimized libraries by profiling hot spots and bringing parallelism to CPU-bound tasks, resulting in a **3x speedup**.

Teaching Assistant
UCL
- 2024-2025: COMP0002 Principles of Programming, COMP0004 Object-Oriented Programming
- 2022-2023: Developed an open-source course and tutored 12 students in six programming languages (C, C++, Rust, Haskell, Java, Python), shell scripting, computer networking, and frontend/backend development.

Open Source Contributions
- **AI**: `pytorch/torcheval` (#195), `princeton-nlp/SWE-bench` (#186, #189, #212)
- **Crypto**: `arkworks-rs/r1cs-std` (#157, #161, #171)
- **PL**: `rust-lang/rust-clippy` (#11865, #12084, #12094), `typst/biblatex` (#34)

Projects

Probabilistic Data Structures and Algorithms 02/2025 - 04/2025
- Accelerated the Morris Counter by implementing **geometric sampling**, achieving **up to 8x speedup** while preserving error guarantees, validated through rigorous benchmarking on varied stream sizes and error parameters.
- Developed an **adaptive sketch selection mechanism** that dynamically chooses between Count Min Sketch and Count Sketch queries by estimating the L2 norm, **reducing MSE** across diverse Zipfian distributions.
- Designed **two novel Deletable Learned Bloom Filter**, a Sandwiched Learned Bloom Filter (SLBF) with two Counting Bloom Filters and a Learned Bloom Filter (LBF) with three Standard Bloom Filters, optimizing tradeoffs between FPR, FNR, and deletability, with simulations showing **superior FPR for SLBF** and **guaranteed deletability for LBF** with a controlled FNR.

TrueLearn 01/2023 - 08/2023
- **Led a team** of 4 students to **implement a Python machine-learning library** with a family of baseline and Bayesian classifiers for building learner models to predict their engagement with educational resources.
- **Created 9 static and interactive visualizations** to present the learner representations in humanly-intuitive ways.
- Advisor: Dr. Sahan Bulathwela

Awards

UCL Studentship for Research 2024
UCL Faculty Undergraduate Scholarships for Excellence (1 student per faculty, 1 out of 1000+ students) 2022

Publications

TensorZKP: Efficient Zero-Knowledge Proof Acceleration using Tensor Cores
Tao Lu, Yuxiang Qiu, Jipeng Zhang, Yanpei Guo, Wenjie Qu, Zonghui Wang, Wenzhi Chen, Jiaheng Zhang
In Preparation

A Toolbox for Modelling Engagement with Educational Videos
Yuxiang Qiu, Karim Djemili, Denis Elezi, Aaneel Shalman Srazali, Mar'ia P'erez-Ortiz, Emine Yilmaz, John Shawe-Taylor and Sahan Bulathwela
Proceedings of the AAAI Conference on Artificial Intelligence, 2024

TrueLearn: A Python Library for Personalised Informational Recommendations with (Implicit) Feedback
Yuxiang Qiu, Karim Djemili, Denis Elezi, Aaneel Shalman, María Pérez Ortiz and Sahan Bulathwela
6th Workshop on Online Recommender Systems and User Modeling, ACM RecSys 2023