

Michael Tu

michaeltu83@gmail.com | <https://github.com/tumichaels> |
<https://www.linkedin.com/in/michael-tu-a5b4a41bb>

EDUCATION

Yale University

New Haven, CT

B.S., M.S. in Computer Science

May 2025

- *Relevant coursework:* Operating Systems, Computer Architecture, Distributed Systems, Zero Knowledge Proofs, Parallel Programming, Algorithms, Machine Learning
- *Awards:* Andy Keidel Undergraduate Endowment Award (2022), Tetelman Fellowship for International Research (2023), Yale Richter Fellowship (2024)

EXPERIENCE

Broadcom

Palo Alto, CA

Security R&D Engineer

Sep 2025 – present

- Re-architected network traffic pipelines from batch ingestion to a streaming compute model in Java, eliminating high-overhead object allocations to slash memory footprint by 10x and minimize garbage collection pauses.
- Redesigned microsegmentation policy APIs to support scalable security policy enforcement and dynamic filtering across large-scale network environments.
- Enhanced network simulation infrastructure to validate microsegmentation security policies before deployment, improving reliability and reducing policy enforcement inconsistencies.

Yale Applied Cryptography Laboratory

New Haven, CT

Research Assistant

Jan 2025 – Aug 2025

- Designed a privacy-preserving client/server protocol enabling users to query distributed databases without revealing query contents, reducing server workload while maintaining strong privacy guarantees.
- Led a cross-functional research team of 4 in developing a C++ cryptographic library implementing Ring-LWE (post-quantum lattice-based cryptography), contributing to protocol design, API architecture, performance optimization, and security evaluation.
- Performed threat modeling and security analysis of private information retrieval protocols, evaluating adversarial capabilities, trust assumptions, attack surfaces, and mitigation strategies while validating formal privacy guarantees.
- Derived system security requirements from protocol threat models and translated security assumptions into implementation and deployment guidance.

Yale Disaggregated Memory Group

New Haven, CT

Research Assistant

May 2024 – Dec 2024

- Analyzed memory access distributions for LLama3 and DLRM ml models to construct a performance model for distributed memory architectures, focusing on CXL 3.0 remote memory.
- Discovered significant skew in memory access patterns for models like LLama3, leading ongoing efforts to further characterize these skews across different operational phases.

PROJECTS

CPSC 420 Processor

Jan 2023 – May 2023

- Designed and implemented a 5-stage pipelined processor in Verilog for a custom MIPS-based ISA, developing expertise in low-level system architecture, privilege boundaries, speculation, and hardware/software interactions.
- Extended processor architecture with speculative execution and out-of-order commit mechanisms, requiring careful analysis of architectural correctness and system behavior.

SKILLS

Programming Languages: C++, C, Python, Verilog, Racket, HTML/CSS, Java, Assembly, Golang, Cuda

Security & Systems: Threat Modeling, Applied Cryptography, Post-Quantum Cryptography (Ring-LWE), Privacy-Preserving Systems, Distributed Systems Security, Computer Architecture, Operating Systems

Developer Tools: Git, Github, Protobuf, Jupyter Notebook, L^AT_EX(Overleaf/R Markdown), Figma, VS Code, Linux, Windows, Bash, Excel