

Research Interests:

Cryptography: provable security, private information retrieval, (post-)quantum tools

Computer Security: secure and private outsourced storage

Education

University of Chicago, 2024 PhD in Computer Science, Advisor: David Cash
(expected)

University of Chicago, 2021 MS in Computer Science, Advisor: David Cash

Rochester Institute of Technology, 2018 BS in Computer Science and Applied Mathematics (double major)
GPA: 3.86 / 4.0

Selected Publications

- *Leakage-Abuse Attacks Against Structured Encryption for SQL*, with Ruth Ng, Daren Khu, Yao'An Li, Joelle Lim, Derrick Ng, Jed Lim, and Yiyang Song (USENIX 2024)
- *A Lower Bound for One-Round Oblivious RAM*, with David Cash and Andrew Drucker (TCC 2020)
- *Time-sliced quantum circuit partitioning for modular architectures*, with Jonathan M. Baker, Casey Duckering, and Frederic Chong (CF 2020)
- *Very hard electoral control problems*, with Zack Fitzsimmons, Edith Hemaspaandra, and David E. Narváez (AAAI 2019)

Pre-prints

- *Plinko: Single-Server PIR with Efficient Updates via Invertible PRFs*, with Sarvar Patel, Giuseppe Persiano, and Kevin Yeo (In submission)
- *Structured Encryption for Indirect Addressing*, with Ruth Ng, David Cash, and Eileen Ee (EPRINT)
- *Decomposing Quantum Generalized Toffoli with an Arbitrary Number of Ancilla*, with Jonathan M. Baker, Casey Duckering, and Frederic Chong (arXiv)

Professional Experience

Google PhD Student Researcher, where I collaborated with the Private Computing team
9/23 - 5/24 on cryptographic research

Meta PhD Student Internship, where I worked on query optimization for Meta's internal
6/22 - 9/22 query language

BMW Manufacturing Student Co-op working on data mining for the Research and Innovation Center at BMW
1/18 - 5/18

Teaching

Cryptography, University of Chicago, Autumn 2021, 2020, 2019

Computer Security, University of Chicago, Winter 2023, 2021, 2020

Graph Theory, University of Chicago, Spring 2019

Intro to Machine Learning, University of Chicago, Winter 2019

Intro to Computer Science, University of Chicago, Autumn 2018

Theoretical Computer Science Tutor, Rochester Institute of Technology, Spring 2016 - Fall 2017