Alexander Hoover

University of Chicago
5730 S. Ellis Ave. Chicago, IL 60637.

Updated April 2024
alexhoover@uchicago.edu
axhoover.com

Research Interests

Using cryptography to make outsourced computation efficient, useful, secure and private.
Areas – Secure Outsourced Computation, Privacy, Provable Security, (Post-)quantum Cryptography

Education

Ph.D. in Computer Science, University of Chicago — 2018 – 2024
Advisor: Prof. David Cash

M.S. in Computer Science, University of Chicago — 2018 – 2021
Advisor: Prof. David Cash

B.S. in CS and Math, Rochester Institute of Technology — 2015 – 2018
With Honors — 3.86 / 4.0

Employment History

PhD Student Researcher, Google — Sept 2023 – May 2024
Collaborating with Kevin Yeo and the Private Computing team

Graduate Research Assistant, University of Chicago — Sept 2018 – June 2024
Advisor: Prof. David Cash

PhD Student Internship, Meta — June 2022 – Aug 2022

Student Co-op, BMW Manufacturing — Jan 2018 – May 2018

Publications

[1] 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.
In Proc. of the 33rd USENIX Security Symposium, ***(USENIX Security) 2024***

[2] A Lower Bound for One-Round Oblivious RAM
with David Cash and Andrew Drucker.
In Proc. of the 18th International Conference on Theory of Cryptography, ***(TCC) 2020***

[3] Time-Sliced Quantum Circuit Partitioning for Modular Architectures
with Jonathan M. Baker, Casey Duckering, and Frederic Chong.
In Proc. of the 17th ACM International Conference on Computing Frontiers, ***(CF) 2020***

[4] Very hard electoral control problems
with Zack Fitzsimmons, Edith Hemaspaandra, and David E. Narváez.
In Proc. of the AAAI Conference on Artificial Intelligence, ***(AAAI) 2019***

Preprint

[5] Plinko: Single-Server PIR with Efficient Updates via Invertible PRFs
with Sarvar Patel, Giuseppe Persiano, and Kevin Yeo.
In submission.

[6] Structured Encryption for Indirect Addressing
with Ruth Ng, David Cash, and Eileen Ee.

[7] Decomposing Quantum Generalized Toffoli with an Arbitrary Number of Ancilla
with Jonathan M. Baker, Casey Duckering, and Frederic Chong.

Teaching Experience

Teaching Assistant, University of Chicago

- Cryptography — Autumn ('19, '20, '21)
- Computer Security — Winter ('20, '21, '23)
- Graph Theory — Spring '19
- Introduction to Machine Learning — Winter '19
- Introduction to Computer Science — Autumn '18

Theoretical Computer Science Tutor, Rochester Institute of Technology — Spring '16 - Fall '17

Selected Talks

Conference Talks

- *A Lower Bound for One-round Oblivious RAM* — TCC 2020

Invited Talks

- Plinko: Single-Server PIR with Efficient Updates via Invertible PRFs
  Guest Lecture, Yale University, April 2024
- Plinko: Single-Server PIR with Efficient Updates via Invertible PRFs
  Guest Lecture, University of Illinois Urbana-Champaign, May 2024
- Plinko: Single-Server PIR with Efficient Updates via Invertible PRFs
  CyLab Crypto Seminar, Carnegie Mellon University, May 2024

Academic Service

Conference Reviewer

- Crypto
- Eurocrypt
- Theory of Cryptography (TCC)
- Public Key Cryptography (PKC)
- Journal of Cryptology

Conference Volunteer

- Theory of Cryptography (TCC) — 2022

Organizer for UChicago Cryptography Reading Group — 2022-2023
Created to bring students and faculty together to read and discuss cryptography papers.