Kaiwen (Kevin) He

U.S. citizen | khe01@mit.edu | github.com/kevin-he-01 | Website: https://kevin-he-01.github.io/ | Cambridge, MA

Research Interests

Secure multi-party computation (MPC): joint computation on private data while maintaining individual privacy. I am especially interested in the application of homomorphic secret sharing (HSS) techniques to MPC.

Education

Massachusetts Institute of Technology — Cambridge, MA

- Ph.D. candidate in Computer Science — Sep 2023 – Current
- M.S. in Computer Science — Sep 2023 – Sep 2025

University of California San Diego — La Jolla, CA

- B.S. in Computer Engineering — Sep 2020 – Jun 2023

Experience

Research Intern, Aarhus University – Aarhus, Denmark — May 2026 – Aug 2026

- Investigated security of MPC in practice: `https://mpcinthewild.github.io/`

Teaching Assistant, MIT – Cambridge, MA — Jan 2026 – May 2026

- 6.5610, Applied Cryptography.

Research Experiences for Undergraduates, UC San Diego – La Jolla, CA — Jun 2022 – May 2023

- Collected weekly data from 2^{32} or 4 billion hosts (the entire IP address space).
- Designed a new open source ZGrab 2.0 module with 7829 lines of code to collect data from IPsec hosts.

Academic Services

External Reviewer, CANS 2026

External Reviewer, Proceedings of the IEEE

Talks

Aarhus University Crypto Summer Day — Aarhus, Denmark
Dyad (ongoing work on multi-party computation) — July 2026

Aarhus University Crypto Seminar — Aarhus, Denmark
Concretely-Efficient Multi-Key Homomorphic Secret Sharing and Applications — June 2026

IEEE S&P — San Francisco, CA
Concretely-Efficient Multi-Key Homomorphic Secret Sharing and Applications — May 2026

Northeastern University, Crypto Reading Group — Boston, MA
Concretely-Efficient Multi-Key Homomorphic Secret Sharing and Applications — March 2026

Boston University, BUSec Seminar — Boston, MA
Concretely-Efficient Multi-Key Homomorphic Secret Sharing and Applications — February 2026

Google — New York, NY
Concretely-Efficient Multi-Key Homomorphic Secret Sharing and Applications — January 2026

Berkeley Security Seminar — Berkeley, CA
Concretely-Efficient Multi-Key Homomorphic Secret Sharing and Applications — January 2026

UCSD Security Lunch — La Jolla, CA
Concretely-Efficient Multi-Key Homomorphic Secret Sharing and Applications — January 2026

MIT CIS Seminar (with Lali Devadas) — Cambridge, MA

Multi-Key Homomorphic Secret Sharing, From Theory To Practice December 2025

CSAW New York, NY
Passive SSH Key Compromise via Lattices November 2024

ACM CCS Copenhagen, Denmark
Passive SSH Key Compromise via Lattices November 2023

Awards and Honors

Recipient, Qualcomm Innovation Fellowship May 2026
Making Modern Cryptography Faster and More Energy-Efficient Through Hardware Acceleration of Modular Arithmetic

Most notable paper: technical impact, CSAW Applied Research Competition November 2024
Passive SSH Key Compromise via Lattices

Recipient, Irwin Mark Jacobs and Joan Klein Jacobs Presidential Fellowship, MIT September 2023
Offered to newly admitted Ph.D. students who have demonstrated exemplary academic and research achievements, and thus show great promise for future accomplishments.

Recipient, SIM San Diego Scholarship, Society of Information Management (SIM) San Diego October 2022
Offered to nominated *students only.*

Publications

VROOM: Accelerating (Almost All) Number-Theoretic Cryptography Using Vectorization and the Residue Number System August 2026
Simon Langowski, Kaiwen He, Srinivas Devadas
USENIX Security 2026

Concretely-Efficient Multi-Key Homomorphic Secret Sharing and Applications May 2026
Kaiwen He, Sacha Servan-Schreiber, Geoffroy Couteau, Srinivas Devadas
IEEE S&P 2026

Passive SSH Key Compromise via Lattices November 2023
Keegan Ryan, Kaiwen He, George Arnold Sullivan, Nadia Heninger
ACM CCS 2023

Critique of: "A Parallel Framework for Constraint-Based Bayesian Network Learning via Markov Blanket Discovery" by SCC Team From UC San Diego October 2022
Arunav Gupta, John Ge, John Li, Zihao Kong, Kaiwen He, Matthew Mikhailov, Bryan Chin, Xiaochen Li, Max Apodaca, Paul Rodriguez, Mahidar Tatineni, Mary Thomas, and Santosh Bhatt
IEEE TPDS 2022

Skills

Programming Languages: Python, JavaScript, Go, Java, Bash, C, C++, Rust, TypeScript, x86 and ARM Assembly, Kotlin.
Other: Cryptography, Cryptanalysis, Technical Writing, Technical Presentation, Research.