Kaiwen He

Cambridge, MA | khe01@mit.edu | kevin-he-01.github.io | github.com/kevin-he-01

Research Interests

I am broadly interested in **applied cryptography**. My current research focuses on making theoretical cryptographic constructs practically efficient and applicable to real-world scenarios.

Education

Massachusetts Institute of Technology, Ph.D. candidate in Computer Science — Cambridge, MA

- GPA: 4.0/4.0 — Fall 2023 – Current
- **Advised by:** Srini Devadas

University of California San Diego, B.S. in Computer Engineering — La Jolla, CA

- GPA: 4.0/4.0 — Fall 2020 – Spring 2023
- **Advised by:** Nadia Heninger

Experience

Research Assistant, MIT – Cambridge, MA — June 2024 – Current

- Research on homomorphic secret sharing is currently under submission to IEEE S&P 2026.

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

- Research led to publication “Passive SSH Key Compromise via Lattices” in ACM CCS 2023.
- Collected weekly data from the entire IP address space (2^{32} or 4 billion hosts) to support the publication.
- Designed a new ZGrab 2.0 module for the IPsec protocol in order to collect data from IPsec hosts: `https://github.com/kevin-he-01/zgrab2`.
- Responded to individual data exclusion requests.

Publications

Concretely-Efficient Multi-Key Homomorphic Secret Sharing and Applications — Under Review

Kaiwen He, Geoffroy Couteau, Srinivas Devadas, Sacha Servan-Schreiber

(Under Review) 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 Transactions on Parallel and Distributed Systems

Talks

CSAW — New York, NY

Passive SSH Key Compromise via Lattices — November 8th 2024

ACM CCS — Copenhagen, Denmark

Passive SSH Key Compromise via Lattices — November 29th 2023

Awards and Honors

Most notable paper: technical impact, CSAW Applied Research Competition November 2024

- Paper: Passive SSH Key Compromise via Lattices.

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.

SIM San Diego Scholarship, Society of Information Management (SIM) San Diego October 2022

- Offered to nominated students by SIM San Diego.