

Kaiwen (Kevin) He

Cambridge, MA | khe01@mit.edu | github.com/kevin-he-01 | Personal Website: <https://kevin-he-01.github.io/>

Research Interest and Vision

Applied cryptography: I design *efficient* cryptographic solutions to enhance the security and privacy of *everyone*.

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 Assistant, MIT – Cambridge, MA | Jun 2024 – Current |
| • Reduced multi-key homomorphic secret sharing (MKHSS) latency by $45\times$ and communication by $3\times$ over prior work. | |
| • Ongoing work to accelerate modular multiplication & elliptic-curve arithmetic, with applications to faster zk-SNARKs. | |
| Research Experiences for Undergraduates, UC San Diego – La Jolla, CA | Jun 2022 – May 2023 |
| • Research paper “Passive SSH Key Compromise via Lattices” published in ACM CCS 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. | |
| • Promptly honored all individual data exclusion requests. | |

Talks

| | |
|---|---------------------|
| Google | New York, NY |
| <i>Concretely-Efficient Multi-Key Homomorphic Secret Sharing and Applications</i> | January 2026 |
| Berkeley Security Seminar | Berkeley, CA |
| <i>Concretely-Efficient Multi-Key Homomorphic Secret Sharing and Applications</i> | January 2026 |
| UCSD Security Seminar | La Jolla, CA |
| <i>Concretely-Efficient Multi-Key Homomorphic Secret Sharing and Applications</i> | January 2026 |
| MIT CIS Seminar (with Lali Devadas) | Cambridge, MA |
| <i>Multi-Key Homomorphic Secret Sharing, From Theory To Practice</i> | December 2025 |
| CSAW | New York, NY |
| <i>Passive SSH Key Compromise via Lattices</i> | November 2024 |
| ACM CCS | Copenhagen, Denmark |
| <i>Passive SSH Key Compromise via Lattices</i> | November 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 <i>nominated</i> students only. | |

Publications

Concretely-Efficient Multi-Key Homomorphic Secret Sharing and Applications

May 2026

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

IEEE S&P 2026 (to appear)

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.