

Julie Ha

hajulie@bu.edu | Boston, MA

Education

Boston University Computing and Data Sciences | Boston MA

Sept 2022-Present

4th year Ph.D. student

- Advisor: Mayank Varia
- Topics: Applied cryptography, law and computer science

Boston University | Boston, MA

May 2022

B.A. in Computer Science with Honors

- GPA: 3.69
- Recipient of Computer Science Award for Academic Excellence
- Senior Thesis: Oblivious Searchable Encryption for Irises

Report on research with Prof. Benjamin Fuller at University of Connecticut, introducing a new construction for searchable encryption for biometrics, utilizing constructions from Boldyreva and Tang (PETS 2021) and Pappas et al (Oakland 2014). Presented thesis at Boston University Security Seminar in May 2022.

Publications

Y. Gvili, J. Ha, S. Scheffler, M. Varia, Z. Yang, and X. Zhang. *TurboIKOS: Improved Non-interactive Zero Knowledge and Post-Quantum Signatures*. In International Conference on Applied Cryptography and Network Security (ACNS) 2021.

Link: <https://eprint.iacr.org/2021/478>

Research Experience

Boston University | Boston, MA

September 2021 - Present

Undergraduate Research Assistant

- Work with Profs. Ran Canetti and Gabe Kaptchuk to implement zero-knowledge proof on Apple's private set intersection protocol

NSF Research Experience for Undergraduates (REU) | Storrs, CT

June 2021 - August 2021

Research Student

- Work with Prof. Benjamin Fuller at University of Connecticut on encrypted proximity search on irises using primitives such as Bloom Filters, Locality Sensitive Hashes (LSH), and statistical noise from biometrics to reduce leakage and improve efficiency

Boston University Center for RISCS | Boston, MA

May 2020 - July 2021

Undergraduate Research Assistant

- Work with Prof. Mayank Varia and Dr. Sarah Scheffler on a zero-knowledge proof system using "MPC-in-the-head" paradigm
- Implemented TurboIKOS in Python

Teaching Experience

Fall 2021: Undergraduate Teaching Assistant for CS357: Introduction to Information Security

Spring 2022: Grader for CS538: Fundamentals of Cryptography, Grader for CS558: Network Security

Spring 2023: Graduate TA for CS558

Spring 2025: Graduate TA for DS593: Privacy in Practice

Fall 2026: Graduate TA for DS653: Crypto for DS

Outreach

CodeBreakers | Boston, MA (Remote)

June 2020 - August 2020

Coordinator

- Instructed cryptography portion of a summer program for high school sophomores and juniors to help create relationships in STEM and introduce topics in computer science
- Created activities related to computer science to facilitate engagement remotely

Rewards

Hariri Institute Community Recognition Awards - Graduate Student Excellence Award (June 2023)

Talks

University of Connecticut Security Seminar (July 2021)

International Conference for Applied Cryptography and Network Security (June 2021)

Posters

New England Security Day 2024

Annual Boston Security Usability Research Day 2024

External Reviewer

Crypto 2022

USENIX Security 2022

CCS 2023

USENIX Security 2023

CCS 2024

USENIX Security 2025

Privacy Enhancing Technologies Symposium (PETS) 2026

Relevant Coursework

Cryptography: Applied Cryptography, Fundamentals of Cryptography, Advanced Cryptography, Network Security

Law: Law and Algorithms