Eysa Lee

eysa_lee@brown.edu
www.eysalee.com

Professional Experience

Postdoctoral Research Associate August 2023 – Present
Data Science Institute, Brown University, Providence, Rhode Island
Host: Anna Lysyanskaya

Quantum Computing Summer Associate Summer 2022
Future Lab for Applied Research and Engineering, JPMorgan Chase, NYC, New York

Research Intern Summer 2019
Visa Research, Palo Alto, California

Intern in Summer Program in Applied MPC and Implementations Summer 2018
Bar-Ilan University, Ramat Gan, Israel

Education

Ph.D. in Computer Science Spring 2023
Northeastern University, Boston, MA
Advisor: abhi shelat
Thesis: *Securely Computing Threshold Variants of Signature Schemes (and More!)*

B.S. in Computer Science Spring 2017
B.S. in Mechanical Engineering
The University of Texas at Austin, Austin, TX

Publications

Note: Unless otherwise noted, authors ordered alphabetically, as is convention in cryptography.

Manuscripts

- J. Doerner, Y. Kondi, **E. Lee**, and a. shelat. "Threshold ECDSA in Three Rounds". https://eprint.iacr.org/2023/765

Journals

J1. M. Chen, R. Cohen, J. Doerner, Y. Kondi **E. Lee**, S. Rosefield, and a. shelat. "Multiparty Generation of an RSA Modulus", in Journal of Cryptology. Vol. 35(2).

Conference Proceedings

6. J. Doerner, Y. Kondi, **E. Lee**, a. shelat, and L. Tyner. "Threshold BBS+ Signatures for Distributed Anonymous Credential Issuance", in IEEE Security and Privacy (Oakland) 2023.

5. A. Dalskov, **E. Lee**, and E. Soria-Vazquez. "Circuit Amortization Friendly Encodings and their Application to Statistically Secure Multiparty Computation", in Asiacrypt 2020.

4. M. Chen, R. Cohen, J. Doerner, Y. Kondi **E. Lee**, S. Rosefield, and a. shelat. "Multiparty Generation of an RSA Modulus", in CRYPTO 2020.

3. J. Doerner, Y. Kondi, **E. Lee**, and a. shelat. "Threshold ECDSA from ECDSA Assumptions: The Multiparty Case", in IEEE Security and Privacy (Oakland) 2019.

2. J. Doerner, Y. Kondi, **E. Lee**, and a. shelat. "Secure Two-Party Threshold ECDSA from ECDSA Assumptions", in IEEE Security and Privacy (Oakland) 2018.

1. C. Freitag, R. Goyal, S. Hohenberger, V. Koppula, **E. Lee**, T. Okamoto, J. Tran, and B. Waters. "Signature Schemes with Randomized Verification," in ACNS, 2017.

Talks

Threshold BBS+ Signatures for Distributed Anonymous Credential Issuance

- SPRING Group Meeting at EPFL (Jan 2023)
- Northeastern University Theory Seminar (Nov 2022)
- Brown University Crypto Reading Group (Nov 2022)
- JP Morgan Crypto Group Meeting (Aug 2022)

Circuit Amortization Friendly Encodings and their Application to Statistically Secure Multiparty Computation

- Asiacrypt 2020 (pre-recorded conference talk)

Secure Two-Party Threshold ECDSA from ECDSA Assumptions

- IEEE S&P 2018 (conference talk)
- Theory and Practice of Multiparty Computation 2018 (workshop talk)

Activities

Teaching Assistantships at Northeastern University:

- CS 4700/5700: Network Fundamentals (instructor David Choffnes, Fall 2022)
- CY 4770: Cryptography (instructor Ran Cohen, Spring 2021)
- CY 4770: Cryptography (instructor Daniel Wichs, Spring 2020)

External Reviewer: ACM CCS (2023), Eurocrypt (2023, 2020, 2019), CRYPTO (2021, 2019, 2018), IEEE S&P (2020), TCC (2020, 2019), CANS (2020), AFT (2020, 2019)

Extracurriculars at Northeastern University:

- Organizer for NEU Crypto Reading Group (Spring 2019, Fall 2019, Spring 2020)
- One of three PhD student liaisons on the design committee for the new lab for NEU's Cybersecurity and Privacy Institute (Fall 2022—Spring 2023)

Women in STEM Outreach:

- Instructor for *Girls Who Code*'s "Summer Immersion Program", an 8-week outreach program teaching computer science to rising junior and senior high school women (Summer 2017)
- Designed and conducted a hands-on activity building and racing mini cardboard boats for UT Austin's annual "Introduce a Girl to Engineering Day" (Spring 2017)