Eysa Lee

✉ eysa_lee@brown.edu
eysalee.com

Research Experience

Aug. 2023 – Present **Postdoctoral Research Associate**, *Data Science Institute*, Brown University, Providence, USA.
- Advisor: Anna Lysyanskaya

June 2022 – Aug. 2022 **Quantum Computing Summer Associate**, *Future Lab for Applied Research and Engineering*, JPMorgan Chase, NYC, USA.

May 2019 – Aug. 2019 **Research Intern**, Visa Research, Palo Alto, USA.
- Host: Peter Rindal

June 2018 – July 2018 **Intern in Summer Program in Applied MPC and Implementations**, Bar-Ilan University, Ramat Gan, IL.

Education

May 2023 **PhD in Computer Science**, *Khoury College of Computer Sciences*, Northeastern University, Boston, MA.
- Advisor: abhi shelat
- Thesis Title: *Securely Computing Threshold Variants of Signature Schemes (and More!)*

May 2017 **Bachelor of Science in Computer Science**, *College of Natural Sciences*, The University of Texas at Austin, Austin, TX.

Bachelor of Science in Mechanical Engineering, *Cockrell School of Engineering*, The University of Texas at Austin, Austin, TX.

Publications

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

Journal Publications

J1. **Multiparty Generation of an RSA Modulus**.
Megan Chen, Ran Cohen, Jack Doerner, Yashvanth Kondi, Eysa Lee, Schuyler Rosefield, abhi shelat
In Journal of Cryptology. Vol. 35(2).

Conference Papers

7. **Threshold ECDSA in Three Rounds**.
Jack Doerner, Yashvanth Kondi, Eysa Lee, abhi shelat
In 45th IEEE Symposium on Security and Privacy (S&P, Oakland), 2024.

6. **Threshold BBS+ Signatures for Distributed Anonymous Credential Issuance**.
Jack Doerner, Yashvanth Kondi, Eysa Lee, abhi shelat, LaKyah Tyner
In 44th IEEE Symposium on Security and Privacy (S&P, Oakland), 2023.

5. **Circuit Amortization Friendly Encodings and their Application to Statistically Secure Multiparty Computation**.
Anders Dalskov, Eysa Lee, Eduardo Soria-Vazquez
In International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), 2020.

4. **Multiparty Generation of an RSA Modulus**.
Megan Chen, Ran Cohen, Jack Doerner, Yashvanth Kondi, Eysa Lee, Schuyler Rosefield, abhi shelat
In Annual International Cryptology Conference (CRYPTO), 2020.

3. **Threshold ECDSA from ECDSA Assumptions: The Multiparty Case**.
Jack Doerner, Yashvanth Kondi, Eysa Lee, abhi shelat
In 40th IEEE Symposium on Security and Privacy (S&P, Oakland), 2019.

2. **Secure Two-Party Threshold ECDSA from ECDSA Assumptions**.
Jack Doerner, Yashvanth Kondi, Eysa Lee, abhi shelat
In 29th IEEE Symposium on Security and Privacy (S&P, Oakland), 2018.

1. **Signature Schemes with Randomized Verification**.
Cody Freitag, Rishab Goyal, Susan Hohenberger, Venkata Koppula, Eysa Lee, Tatsuaki Okamoto, Jordan Tran, Brent Waters
In International Conference on Applied Cryptography and Network Security (ACNS), 2017.

Manuscripts and Other

- **Cryptographers' Feedback on the EU Digital Identity's ARF**.
Carsten Baum, Olivier Blazy, Jan Camenisch, Jaap-Henk Hoepman, Eysa Lee, Anja Lehmann, Anna Lysyanskaya, René Mayrhofer, Hart Montgomery, Ngoc Khanh Nguyen, Bart Praneel, abhi shelat, Daniel Slamanig, Stefano Tessaro, Søren Eller Thomsen, Carmela Troncoso
`https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework issues/200`
- **An Unstoppable Ideal Functionality for Signatures and a Modular Analysis of the Dolev-Strong Broadcast**.
Ran Cohen, Jack Doerner, Eysa Lee, Anna Lysyanskaya, Lawrence Roy. *(In Submission)*
- **Improved Multi-Party Fixed-Point Multiplication**.
Saikrishna Badrinarayanan, Eysa Lee, Peihan Miao, Peter Rindal

Presentations

Talks

An Unstoppable Ideal Functionality for Signatures and a Modular Analysis of the Dolev-Strong Broadcast.
Brown Crypto Day, Aug 2024

Threshold BBS+ Signatures for Distributed Anonymous Credential Issuance.
Nordicrypt, Nov. 2023
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 (pre-recorded conference talk), 2020

Secure Two-Party Threshold ECDSA from ECDSA Assumptions.
IEEE Symposium on Security and Privacy, 2018
Theory and Practice of Multiparty Computation (TPMPC), 2018

Other Workshop Contributions

Saying NO! to Workplace Surveillance: Lessons from Cybersecurity and Privacy Institute.
Speakers: Lisa Oakley, xenia dragon, **Eysa Lee**
Re-Imagining Cryptography and Privacy (ReCAP) Workshop, 2024

crypto_doodles: cryptography through comics and jokes.
Eysa Lee
Re-Imagining Cryptography and Privacy (ReCAP) Workshop, 2024

Service

2025 **PC Member**, *IEEE European Symposium on Security and Privacy (EuroS&P)*.

2025 **PC Member, Research Ethics Committee Member**, *IEEE Symposium on Security and Privacy (S&P)*.

2024 **PC Co-Chair**, *The Conference for Failed Approaches and Insightful Losses in Cryptology (CFAIL)*.
IACR CRYPTO Affiliated Workshop

2024 **PC Member**, *International Conference on Cryptology and Network Security (CANS)*.

2024 **External Reviewer**, *Eurocrypt*.

2023 **External Reviewer**, *Eurocrypt, ACM CCS*.

2021 **External Reviewer**, *CRYPTO*.

2020 **External Reviewer**, *Eurocrypt, IEEE S&P, TCC, CANS, AFT*.

2019 **External Reviewer**, *Eurocrypt, CRYPTO, TCC, AFT*.

2018 **External Reviewer**, *CRYPTO*.

Teaching Experience

Fall 2022, Spring 2021, Spring 2020 **Graduate Teaching Assistant**, *Northeastern University*.

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

Other Activities

Fall 2022 – Spring 2023 **PhD Student Liaison**, *NEU Cybersecurity and Privacy Institute Design Committee*.
One of three PhD student liaisons on the design committee for the new lab space

Spring 2019, Fall 2019, Spring 2020 **Organizer**, *NEU Crypto Reading Group*.

Summer 2017 **Instructor**, *Summer Immersion Program*, Girls Who Code.
8-week outreach program teaching computer science to 19 rising junior and senior high school women