

Research Interests: Cryptography, threshold signatures, digital credentials, multiparty computation

## Academic Positions

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

## Academic Degrees

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.

### Manuscripts

- **Multi-Holder Anonymous Credentials from BBS Signatures.**  
Andrea Flamini, Eysa Lee, Anna Lysyanskaya  
Preprint: <https://eprint.iacr.org/2024/1874>  
(In Submission)
- **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.  
Preprint: <https://eprint.iacr.org/2024/1807>  
(In Submission)
- **Improved Multi-Party Fixed-Point Multiplication.**  
Saikrishna Badrinarayanan, Eysa Lee, Peihan Miao, Peter Rindal.  
Preprint: <https://eprint.iacr.org/2024/1047>

### Technical Reports

- [T1] **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  
Available: <https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/issues/200>

### 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).  
Available: <https://eprint.iacr.org/2020/370>

## 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.  
Available: <https://eprint.iacr.org/2023/765>
- [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.  
Available: <https://eprint.iacr.org/2023/602>
- [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.  
Available: <https://eprint.iacr.org/2020/1053>
- [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.  
Available: <https://eprint.iacr.org/2020/370>
- [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.  
Available: <https://eprint.iacr.org/2019/523>
- [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.  
Available: <https://eprint.iacr.org/2018/499>
- [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.

---

## 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**, [6].  
*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**, [5].  
*Asiacrypt* (pre-recorded conference talk), 2020
- **Secure Two-Party Threshold ECDSA from ECDSA Assumptions**, [2].  
*IEEE Symposium on Security and Privacy (S&P)*, 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*

## Research Experience

- June 2022 – **Quantum Computing Summer Associate**, *Future Lab for Applied Research and Engineering*,  
Aug. 2022 JPMorgan Chase, NYC, USA.
- May 2019 – **Research Intern**, Visa Research, Palo Alto, USA.  
Aug. 2019
  - o Host: Peter Rindal
- June 2018 – **Intern in Summer Program in Applied MPC and Implementations**, Bar-Ilan University,  
July 2018 Ramat Gan, IL.

## Service

- 2024 **PC Member**, *IEEE European Symposium on Security and Privacy 2025 (Euro S&P)*.
- 2024 **PC Member**, *Financial Cryptography and Data Security Conference 2025 (FC)*.
- 2024 **Research Ethics Committee Member**, *IEEE Symposium on Security and Privacy 2025 (S&P)*.
- 2024 **PC Member**, *IEEE Symposium on Security and Privacy 2025 (S&P)*.
- 2024 **Rump Session Co-Chair**, *IACR CRYPTO 2024*.
- 2024 **PC Co-Chair**, *The Conference for Failed Approaches and Insightful Losses in Cryptology (CFAIL)*.  
IACR CRYPTO 2024 Affiliated Workshop
- 2024 **PC Member**, *International Conference on Cryptology and Network Security 2024 (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 2024 **Guest Lecturer**, *Brown University*.
  - o Oct 21, Oct 23: Data, Ethics and Society (DATA 0080). Instructor: Linda Clark.  
Topic: Data privacy.
- Fall 2022, **Graduate Teaching Assistant**, *Northeastern University*.
- Spring 2021,
  - o Fall 2022: Network Fundamentals (CS 4700/5700). Instructor: David Choffnes.
- Spring 2020
  - o Spring 2021: Cryptography (CY 4770). Instructor: Ran Cohen.
  - o Spring 2020: Cryptography (CY 4770). Instructor: Daniel Wicks.
- Summer 2017 **Summer Immersion Program (SIP) Instructor**, *Girls Who Code*.  
8-week outreach program teaching computer science to 19 rising junior and senior high school women

## Industry Adoption

List as of March 2024.

- **Threshold ECDSA in Three Rounds**, [7].  
Ongoing implementation efforts at *Copper, Silence Laboratories, Utila, Sodot, Cloudflare*, and others.

- **Threshold BBS+ Signatures for Distributed Anonymous Credential Issuance**, [6].  
Implemented and deployed by *Dock Network*.
- **Threshold ECDSA from ECDSA Assumptions: The Multiparty Case**, [3].  
Implemented and deployed by *Paypal*, *BlockDaemon*, *Web3auth/Torus*, *Utila*, *Sodot*, and *Coinbase* (deprecated).  
Ongoing implementation efforts at *Vaultody*.
- **Secure Two-Party Threshold ECDSA from ECDSA Assumptions**, [2].  
Implemented and deployed by *BlockDaemon*, *Utila*, *Sodot*, and *Vaultody*.

## Extracurricular

### Northeastern University (NEU)

- Fall 2022 – **PhD Student Liaison**, *NEU Cybersecurity and Privacy Institute Design Committee*.
- Spring 2023 One of three PhD student liaisons on the design committee for the new lab space
- Spring 2019, **Organizer**, *NEU Crypto Reading Group*.  
Fall 2019, Organized weekly group meetings for the crypto group at Northeastern  
Spring 2020

### University of Texas at Austin (UT)

- Fall 2015 – **Undergraduate Student Representative**, *Computer Science Student Advisory Board*.
- Spring 2016 One of six students representing the undergraduate computer science community in meetings with department administrators
- Summer 2015 **Vice President of Finance**, *UT Student Chapter of ACM*.  
– Spring 2016 Managed budget of over \$20,000 for the UT chapter of ACM's 375 members
- Summer 2015 **Co-Head Ambassador**, *UT Computer Science Ambassadors*.  
– Spring 2016 Trained new members and coordinated with staff and faculty on administrative decisions
- Spring 2014 – **Scheduler**, *UT Computer Science Ambassadors*.  
Spring 2015 Arranged and gave tours to prospective undergraduate students visiting the CS department at UT