Eysa Lee

✉ eylee@barnard.edu
🏠 eysalee.com

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

Academic Positions

July 2025 – Present **Assistant Professor**, *Computer Science Department*, Barnard College, NYC, USA.

July 2025 – Present **Affiliated Faculty**, *Department of Computer Science*, Columbia University, NYC, USA.

Aug. 2023 – July 2025 **Postdoctoral Research Associate**, *Data Science Institute*, Brown University, Providence, USA.
- ○ Advisor: Anna Lysyanskaya

Academic Degrees

July 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 **BS in Computer Science**, *College of Natural Sciences*, The University of Texas at Austin, Austin, TX.

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

Awards

- **Postdoc Fellowship**, *Data Science Institute*, Brown University, Awarded 2023.

Teaching and Advising

- **Barnard College**.

Courses taught:
- ○ Fall 2025: Introduction to Computational Thinking and Data Science (COMS BC1016).

Undergraduate students advised:
- ○ Elizabeth Wei (NYU), Cyber NYC REU, Summer 2025

- **Brown University**.

Fall 2024: Guest lecturer for the data privacy module of Data, Ethics, and Society (DATA 0080).

- **Northeastern University**.

Graduate Teaching Assistant:
- ○ 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.

- **Girls Who Code**.

Summer 2017: Instructor for an 8-week outreach program ("Summer Immersion Program") teaching computer science to 19 rising junior and senior high school women

Research Experience

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.

Professional Activities

Conference and Workshop Program Committees

- ACM Conference on Computer and Communications Security (CCS), 2026
- Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt), 2026
- IEEE Symposium on Security and Privacy (S&P), 2026
- The Conference for Failed Approaches and Insightful Losses in Cryptology, 2025 (**PC Co-Chair**) (Crypto 2025 Affiliated Workshop)
- IEEE European Symposium on Security and Privacy (EuroS&P), 2025
- Financial Cryptography and Data Security Conference (FC), 2025
- IEEE Symposium on Security and Privacy (S&P), 2025 (**Research Ethics Committee Member**)
- The Conference for Failed Approaches and Insightful Losses in Cryptology, 2024 (**PC Co-Chair**) (Crypto 2024 Affiliated Workshop)
- International Conference on Cryptology and Network Security (CANS), 2024

Workshop and Conference Organizational Committees

- **Rump Session Co-Chair**, Crypto 2025
- **Rump Session Co-Chair**, Crypto 2024

Barnard Committees

- Computer Science Department Bylaws Committee, 2025

Northeastern Committees

- NEU Cybersecurity and Privacy Institute Design Committee, 2022-2023

Publications

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

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

[9] **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 *Theory of Cryptography Conference (TCC)*, 2025.
Available: `https://eprint.iacr.org/2024/1807`

[8] **Multi-Holder Anonymous Credentials from BBS Signatures**.
Andrea Flamini, Eysa Lee, Anna Lysyanskaya
In *Annual International Cryptology Conference (CRYPTO)*, 2025.
Available: `https://eprint.iacr.org/2024/1874`

[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.

Manuscripts

- **Improved Multi-Party Fixed-Point Multiplication**.
  Saikrishna Badrinarayanan, Eysa Lee, Peihan Miao, Peter Rindal.
  Preprint: `https://eprint.iacr.org/2024/1047`

Presentations

Talks

- **Are we finally getting anonymous credentials?**, [T1].
  3rd Anonymity Day Workshop, April 2025

- **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 the 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

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*.