Eysa Lee

lee.ey@northeastern.edu

www.eysalee.com

Education

Current

Northeastern University, Boston, MA — Fall 2017 – Spring 2023 *(expected)*
Ph.D. in Computer Science
Advisor: abhi shelat

Previous

University of Texas at Austin, Austin, TX — Fall 2012 – Spring 2017
B.S. in Computer Science
B.S. in Mechanical Engineering

Conference Publications[1]

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 *(to appear)*.

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

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

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

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

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.

Journal Publications[2]

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.

Internships

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

Collaborated with both the quantum team (FLARE) and cryptographers from the AI Research group on improving security in the quantum setting, in particular using cryptography to remove trust assumptions for practical quantum networks.

Research Intern — Summer 2019
Visa Research, Palo Alto, California

Worked under the supervision of Peter Rindal on using MPC for more efficient privacy-preserving machine learning.

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

Worked with two other PhD students on an protocol for generating BMR circuits using OT. Optimized for large-scale, honest-majority setting using hyper-invertible matrices and field embedding. Ultimately resulted in an Asiacrypt 2020 paper.

[1] Authors ordered alphabetically, as is convention in cryptography.
[2] See footnote 1.

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: 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 the Cybersecurity and Privacy Institute at NEU (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)

Miscellaneous

2018 and 2019 threshold ECDSA papers ("DKLs") have made appearances in industry:

1. Deployed by Sepior, an "advanced MPC digial asset wallet & custody infrastructure" company acquired by Blockdaemon
   `https://docs.sepior.com/docs/cryptographic-primitives-1`
2. Coinbase's blog and advanced cryptography library
   `https://blog.coinbase.com/fast-secure-2-of-2-ecdsa-using-dkls18-843e10fe2804`
   `https://pkg.go.dev/github.com/coinbase/kryptology#section-readme`

Overviews of my threshold ECDSA works [DK**L**s18, 19] have been presented by coauthors at workshops:

1. NIST Threshold Cryptography Workshop 2019 as the contributed talk talk "A Multiparty Computation Approach to Threshold ECDSA"
   `https://csrc.nist.gov/Events/2019/ntcw19`
2. IACR Real World Cryptography Symposium 2023 as the contributed talk "Threshold ECDSA Towards Deployment"