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 2022.

Manuscripts[3]

S. Badrinarayanan, **E. Lee**, P. Miao, P. Rindal. "Improved Multi-Party Fixed-Point Multiplication", Manuscript. Appeared in a talk at the PPML Workshop at CRYPTO 2021.

Internships

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

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

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.

Activities

Talks: JP Morgan Crypto Group Meeting Aug 2022, Asiacrypt 2020, IEEE S&P 2018, Theory and Practice of Multiparty Computation 2018

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

Teaching: TA for undergraduate cryptography Spring 2021 and Spring 2020 (instructors Ran Cohen and Daniel Wichs, resp.); TA for undergraduate network fundamentals Fall 2022 (instructor David Choffnes)

Outreach: Instructor for an 8-week CS outreach program organized by Girls Who Code (Summer 2017); Organized a hands-on experiment building tiny cardboard boats for UT's "Introduce a Girl to Engineering Day" (Spring 2017)

Other: Organizer for NEU Crypto Reading Group (Spring 2019, Fall 2019, Spring 2020)

Miscellaneous

Threshold ECDSA

Co-author of "DKLs", 2018 and 2019 threshold ECDSA papers, which 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`

Coauthor presented an overview on [DK**L**s18, 19] at the NIST Threshold Cryptography Workshop 2019
`https://csrc.nist.gov/Events/2019/ntcw19`

Digital Art

Technical diagrams, such as those appearing in "Threshold BBS+ Signatures for Distributed Anonymous Credential Issuance"

My "Alice" and "Bob" drawings have made appearances in various technical presentations within and outside of my research group
`https://github.com/eysalee/alice-and-bobs`