Curriculum Vitae – Chelsea H. Komlo

Personal Information

Chelsea H. Komlo
me@chelseakomlo.com; www.chelseakomlo.com

Peer-reviewed Conference and Workshop Publications

Elizabeth Crites, Chelsea Komlo, Mary Maller, Stefano Tessaro, Chenzhi Zhu. **Snowblind: A Threshold Blind Signature in Pairing-Free Groups.** CRYPTO, 2023.

Elizabeth Crites, Chelsea Komlo, Mary Maller. **Fully Adaptive Schnorr Threshold Signatures.** CRYPTO, 2023. Invited to Journal of Cryptology.

Dan Boneh, Chelsea Komlo. **"Threshold Signatures with Private Accountability."** CRYPTO, 2022.

Mihir Bellare, Elizabeth Crites, Chelsea Komlo, Mary Maller, Stefano Tessaro, Chenzhi Zhu. **"Better than Advertised Security for Non-Interactive Threshold Signatures."** CRYPTO, 2022.

Edward Eaton, David Jao, Chelsea Komlo. **"Towards Post-Quantum Updatable Public-Key Encryption via Supersingular Isogenies."** Conference on Selected Areas in Cryptography, 2021.

Chelsea Komlo, Ian Goldberg. **"FROST: Flexible Round-Optimized Schnorr Threshold Signatures."** Conference on Selected Areas in Cryptography, 2020.

Chelsea Komlo, Nick Mathewson, Ian Goldberg. **"Walking Onions: Scaling Anonymity Networks while Protecting Users."** 29th USENIX Security Symposium. 18 pages. August 2020.

Peer-reviewed Journal Publications

Dana Keeler, Chelsea Komlo, Emily Lepert, Shannon Veitch, Xi He. **DPrio: Efficient Differential Privacy with High Utility for Prio.** Proceedings on Privacy Enhancing Technologies, 2023.

Bailey Kacsmar, Chelsea Komlo, Florian Kerschbaum, Ian Goldberg. **"Mind the Gap: Ceremonies for Applied Secret Sharing."** Proceedings on Privacy Enhancing Technologies. Vol. 2020, No. 2. 18 pages. April 2020.

Under Review

Chelsea Komlo, Ian Goldberg, Douglas Stebila. **A Formal Treatment of Distributed Key Generation, and New Constructions.**

Chelsea Komlo, Ian Goldberg. **Arctic: Lightweight and Stateless Threshold Schnorr Signatures.**

Internet Drafts

Deirdre Connolly, Chelsea Komlo, Ian Goldberg, Chris Wood. **"Two-Round Threshold Signatures with FROST."** Crypto Forum Research Group, February 2022.

Notes	Britta Hale, Chelsea Komlo. **"On End-to-End Encryption."**
I have been a reviewer for the following:	- CRYPTO (Program Committee) - CCS (Program Committee) - Real World Cryptography (Program Committee) - Public Key Cryptography (Program Committee) - Journal of Cryptology - Designs, Codes, and Cryptography - Theory of Cryptography Conference - Eurocrypt - AsiaCrypt - LatinCrypt - Privacy Enhancing Technologies Symposium (Program Committee) - Future of PI: Challenges and Perspectives of Personal Identification (Program Committee) - 19th Workshop on Privacy in the Electronic Society (Program Committee) - Advances in Mathematics of Communications - Information and Computation
Work Experience	- Sandbox AQ, Staff Research Scientist (2024-present) - Chief Scientist, Zcash Foundation (2019-2024) - Senior software engineer, HashiCorp, ThoughtWorks (2013-2018)
Awards	- CRYPTO 2023 Best Early Career Paper Award - Recipient of the David R. Cheriton Graduate Scholarship - Recipient of the Provost Doctoral Enterance Award for Women.
Other Services	- Zcash Technical Advisory Board (present) - Tor Project Board of Directors - Tor Research Safety Board

Invited Lectures

"The Past, Present, and Future of Threshold Schnorr Signatures." a16z, June 2024, Elliptic Curve Cryptography Workshop, September, 2024.

"On the Adaptive Security of Threshold Signatures." New York University, June 2024.

"Lessons Learned from Multi-Party Signatures." Johns Hopkins University and Stanford University, May, 2023.

"Threshold Signatures with Private Accountability." Monash University, October 2022, University of St. Gallen, November, 2022.

"Multi-Party Signatures for Discrete-Log Based Cryptosystems." University of Maryland, April 2022.

"Attacks and Fixes on Distributed Key-Generation Protocols." Naval Postgraduate School, November 2021.

"Threshold Signature Schemes: Past, Present, Future." Microsoft Research, Cryptography and Privacy Group, August 2021.

"Introducing FROST: Flexible Round-Optimized Schnorr Threshold Signatures." NIST workshop on Multi-Party Threshold Schemes, October 2020, University of College London Information Security Group, December 2020.

"Where Theory Meets Practice for Privacy Enhancing Technologies." University of Waterloo CrySP Speaker Series, June 2018.

Contributed Talks

"From Theory to Practice to Theory: Lessons Learned from Multi-Party Schnorr Signatures." Real World Crypto, 2023.

"State-Level Secrets: When Theory Meets Practice for Journalists Working with Encrypted Documents." Real World Crypto, 2019.

Education

PhD in Mathematics Currently completing my PhD in the Cryptography, Security, and Privacy lab at the University of Waterloo under the supervision of Dr. Ian Goldberg and Dr. Douglas Stebila.

Masters Degree in Mathematics Completed a masters degree in the Cryptography, Security, and Privacy Lab at the University of Waterloo.