# Curriculum Vitae – Chelsea H. Komlo

## Personal Information

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

## Peer-reviewed Conference and Workshop Publications

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

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

Elizabeth Crites, Chelsea Komlo, Mary Maller. **How to Prove Schnorr Assuming Schnorr: Security of Multi- and Threshold Signatures** October, 2021.

## 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 am/have been a reviewer for the following:

- Journal of Cryptology
- CRYPTO
- Designs, Codes, and Cryptography
- Information and Computation
- LatinCrypt
- Future of PI: Challenges and Perspectives of Personal Identification
- Privacy Enhancing Technologies Symposium (PETs)
- AsiaCrypt

- 19th Workshop on Privacy in the Electronic Society

## Work Experience

- Chief Scientist, Zcash Foundation (2019-present)
- Visiting Researcher, Microsoft Research (2021)
- Senior software engineer, HashiCorp, ThoughtWorks (2013-2018)

## Invited Lectures

**"Threshold Signatures with Private Accountability."** Monash University, October 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.

**"FROST: Flexible Round-Optimized Schnorr Threshold Signatures."** University of College London Information Security Group, December 2020.

**"Introducing FROST: Flexible Round-Optimized Schnorr Threshold Signatures."** NIST workshop on Multi-Party Threshold Schemes, October 2020.

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

## Contributed Talks

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

## Other Services

- Tor Project Board of Directors
- Tor Research Safety Board

## 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. Recipient of the David R. Cheriton Graduate Scholarship and the Provost Doctoral Enterance Award for Women.

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