

## CURRICULUM VITAE – CHELSEA H. KOMLO

---

### PERSONAL INFORMATION

Chelsea H. Komlo  
[me@chelseakomlo.com](mailto:me@chelseakomlo.com); [www.chelseakomlo.com](http://www.chelseakomlo.com)

### 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.

### PEER-REVIEWED CONFERENCE AND WORKSHOP PUBLICATIONS

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

### TECHNICAL REPORTS

Chelsea Komlo, Ian Goldberg. "**FROST: Flexible Round-Optimized Schnorr Threshold Signatures.**" Draft in Progress.

### ONGOING RESEARCH

**Privacy-Preserving Post-Quantum Key Exchange.** Collaboration to define existing key exchange protocols that utilize privacy-preserving properties in a post-quantum setting.

### PUBLIC LECTURES

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

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

### WORK EXPERIENCE

**2019 → Present** Core researcher and engineer at the ZCash Foundation. Currently working on creating a threshold signature scheme for practical use.

**2017 → Present** Core member of the Tor Project on a volunteer basis; worked with the network team on protocol design and implementation.

**2017 → 2018** Core engineer at HashiCorp, worked on Nomad, a high-performance distributed scheduling tool, as well contributed to other projects such as improving the security of underlying gossip protocols.

**2013 → 2017** Senior software engineer at ThoughtWorks, a global technology consulting company. Worked on projects including open-source contributions to Enigmail, Tor, and OTRv4, as well as enterprise software projects in both an engineering, strategy, and security consulting role.

### OTHER SERVICES

**2020** External Reviewer, Privacy Enhancing Technologies (PETs) Symposium

**2019 → Present** Member of the Tor Research Safety Board.

## EDUCATION

**Ph.D in Mathematics** Currently pursuing my Ph.D with an emphasis on cryptography as a member of the Cryptography, Security, and Privacy lab at the University of Waterloo.

**Masters Degree in Mathematics** Completed a masters degree with a focus on computer science at the University of Waterloo.