Marcella Hastings
marcellahastings@gmail.com
marcellahastings.com

Education

University of Pennsylvania, Philadelphia, Pennsylvania USA
Ph.D., M.S., Department of Computer Science, February 2021
Advisor: Nadia Heninger
PhD Committee: Brett Hemenway Falk, Steve Zdancewic, Sebastian Angel, abhi shelat (Northeastern University)

Tufts University, Medford, Massachusetts USA
B.S., Computer Science and Mathematics, May 2015
Summa Cum Laude

Work Experience

Bolt Labs Holdings, Inc, USA (remote)
Cryptographic Engineer. February 2021 - present.
Cryptography Consultant. August 2019 - February 2021.

- Acted as tech lead for a small team to audit, prioritize, and implement changes to upgrade a threshold ECDSA library from proof-of-concept to production quality in Rust.
- Developed cryptographic APIs for distributed protocols in collaboration with product and system developers for use in efficient, scalable applications; design goals included abstracting over deployment decisions (e.g. network topology, database setup) while preventing cryptographic misuse.
- Wrote detailed specifications with implementation guidance for custom cryptographic protocols.
- Collaborated on the development of custom distributed cryptographic protocols, including evaluation and comparison of dependencies and informal security analysis.
- Led education efforts outside the cryptography division sharing knowledge about general cryptography engineering and principles and providing cryptography onboarding for new hires.
- As a consultant, designed and implemented a proof-of-concept application of a custom protocol using MPC, including integrating academic MPC libraries.

Microsoft Resarch, Cryptography and Privacy group, Seattle, WA USA (remote)
Research Intern. Hosted by Hao Chen. May - August 2020.

- Refactored monolithic PSI implementation to add abstraction layers between cryptographic dependencies (including OT, OT-extension, and OPRF). Implemented general-purpose PSI test suite.
- Built a deployment pipeline for secure computation applications to run on an existing developer platform. Improved accessibility of automated deployments by determining secure defaults.

Software & Application Innovation Lab at Boston University, Boston, MA USA
Research Intern. May - August 2019.
Implemented feature libraries and worked on a cryptographically secure protocol for generating preprocessing data in the JIFF framework for secure multi-party computation.

MIT Lincoln Laboratory, Lexington, MA USA
Research Intern. May - August 2014.

Google, New York City, NY USA
Engineering Practicum Intern. June - August 2013.

Publications

Refereed Conference Proceedings

SoK: General Purpose Frameworks for Secure Multi-Party Computation. Marcella Hastings, Brett Hemenway, Daniel Noble, and Steve Zdancewic. In *40th IEEE Symposium on Security and Privacy* (Oakland '19). May 2019.

The Proof is in the Pudding: Proofs of Work for Solving Discrete Logarithms. Marcella Hastings, Nadia Heninger, Eric Wustrow. In *Financial Cryptography and Data Security* (FC '19). February 2019.

Measuring Small Subgroup Attacks on Diffie-Hellman. Luke Valenta, David Adrian, Antonio Sanso, Shaanan Cohney, Joshua Fried, Marcella Hastings, J. Alex Halderman, Nadia Heninger. In *Network and Distributed System Security Symposium* (NDSS '17). February 2017.

Weak Keys Remain Widespread in Network Devices. Marcella Hastings, Joshua Fried, and Nadia Heninger. In *Proceedings of the 2016 ACM on Internet Measurement Conference* (IMC '16). November 2016.

Refereed Journals

Privacy Preserving Network Analytics. Marcella Hastings, Brett Hemenway Falk, Gerry Tsoukalas. In *Management Science* 69(9):5482-5500. 2022.

Invited Talks

General purpose frameworks for secure multi-party computation

DC Area Crypto Day, December 2018
Theory and Practice of Multi-Party Computation Workshops, June 2019
Real World Cryptography, January 2020

Service

Program Committees: FC 2020.

External Reviewing:

PETS 2017, 2018, 2019.
USENIX Security 2019.

Open-Source Software:

MPC-SoK frameworks repository (`github.com/MPC-SoK/frameworks`).
Canetti et al.'s protocol for threshold ECDSA signing (`github.com/boltlabs-inc/tss-ecdsa`).

Teaching

Teaching Assistant, University of Pennsylvania

CIS 331: Introduction to Networks and System Security, Spring 2017. CIS 556: Cryptography, Fall 2016. GEMS Computer Science Workshop, 2017.

Teaching Assistant, Tufts University

COMP 170: Theory of Computation, Spring 2015. COMP 50: Problem-Solving by Computer, Fall 2013. COMP 11: Introduction to Computer Science, Fall 2012 - Spring 2015.

Awards and Honors

The James Schmolze Award for Excellence in Computer Science, Tufts University, May 2015
The Class of 1942 Prize Scholarship, Tufts University, May 2015
Tau Beta Pi