

Marcella Hastings

---

#### CONTACT

Moore 102, 200 South 33rd Street, Philadelphia PA, 19104  
mhast@cis.upenn.edu  
marcellahastings.com

#### EDUCATION

**University of Pennsylvania**, Philadelphia, Pennsylvania USA  
M.S., Ph.D., Department of Computer Science, (*expected December 2020*)  
Advisor: Nadia Heninger

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

#### 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.

#### 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 (<https://github.com/MPC-SoK/frameworks>).

#### 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