Marcella Hastings marcellahastings@gmail.com marcellahastings.com

Work Experience

Galois, Inc, USA (remote)
Research Engineer. November 2023 - present.

- Led project to develop high-quality Cryptol specifications for 12+ NIST cryptography specs, including implementation, documentation and usability, developing readability standards, and education.
- Built and maintained CI (on GitLab and GitHub) for projects supporting Rust, Haskell, and custom formal verification pipelines. Improved performance of existing systems by 20% (caching, pipelining).
- Performed as a software developer on contracts, focusing on effectively architecting code, maintaining readable documentation, comprehensive testing, and preparing effective transitions to clients.

Bolt Labs Holdings, Inc, USA (remote)
Cryptographic Engineer. February 2021 - October 2023.
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.

Selected Open Source

cryptol-specs [https://github.com/GaloisInc/cryptol-specs/]
Developed and improved a wide variety of cryptographic specifications to improve readability and alignment with NIST documents. Improved modularity, test coverage, CI scope, and documentation throughout. Work done at Galois.

tss-ecdsa [github.com/boltlabs-inc/tss-ecdsa]
Improved a threshold ECDSA implementation, including auditing for correctness and code quality, abstracting internal APIs, adding tests, correcting security parameters, writing extensive documentation, and updating public API to be suitable for production deployments. Work done at Bolt Labs.

MPC frameworks [github.com/mpc-sok/frameworks]
Developed an open-source repository and wiki of Docker build environments to compile and run research software frameworks for secure multi-party computation (based on [1]). 400+ stars, 100+ forks on GitHub. Work done at University of Pennsylvania.

Education

University of Pennsylvania, Philadelphia, Pennsylvania USA
Ph.D., M.S., Department of Computer Science, February 2021. Advised by Nadia Heninger.

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

Selected Publications

Refereed Conference Proceedings

[1] SoK: General Purpose Compilers for Secure Multi-Party Computation. Marcella Hastings, Brett Hemenway, Daniel Noble, and Steve Zdancewic. In *40th IEEE Symposium on Security and Privacy*. May 2019.

[2] 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*. February 2019.