# IAN MCQUOID

@ ian.m.mcquoid(at)gmail.com    Oregon, USA    oreko.github.io    linkedin.com/in/ian-mcquoid

## EXPERIENCE

### Cryptography Research Intern

**MIT Lincoln Laboratory**

June 2022 — February 2023    Remote, USA

Perform research on the design and implementation of privacy preserving machine learning algorithms. Work in Python with Tensorflow and MPSPDZ using Git for version control.

### Cryptography Research Intern

**Cloudflare**

June 2021 — September 2021    Remote, USA

Perform research on authentication protocols and work on existing Javascript and Go libraries for cryptographic protocols. Work in an agile environment using Git for version control.

### Software Engineering Intern

**Mentor Graphics**

June 2019 — December 2019    Wilsonville, OR

Implement performance analysis paradigms and develop tools for analyzing static and JIT runtimes using VTune, Collect, and PAPI. Decrease the execution time of an internal tool by a factor of 1000. Work on a large codebase in C using perforce for version control.

### Software Engineering Intern

**Digimarc Corporation**

April 2018 — September 2018    Beaverton, OR

Follow object oriented and functional software engineering paradigms in Python and C++. Debug code on Linux, OSX, and Windows platforms. Work in an agile environment with a team of six people using Git for version control.

## PUBLICATIONS

### Conference Proceedings

- McQuoid, Ian, Mike Rosulek, and Jiayu Xu (2022). “How to Obfuscate MPC Inputs”. In: *TCC 2022: 20th Theory of Cryptography Conference*. Springer, pp. 151–180.
- McQuoid, Ian, Mike Rosulek, and Lawrence Roy (2021). “Batching Base Oblivious Transfers”. In: *Advances in Cryptology – ASIACRYPT 2021*. Springer.
- – (2020). “Minimal Symmetric PAKE and 1-out-of-N OT from Programmable-Once Public Functions”. In: *ACM CCS 2020: 27th Conference on Computer and Communications Security*. ACM Press, pp. 425–442.
- McQuoid, Ian, Trevor Swope, and Mike Rosulek (2019). “Characterizing Collision and Second-Preimage Resistance in Linicrypt”. In: *TCC 2019: 17th Theory of Cryptography Conference*. Springer, pp. 451–470.

## MY LIFE PHILOSOPHY

*“Learning is a process, not a goal. Everything and everyone is a source of knowledge.”*

## AWARDS

**Eagle Scout**
My project was in trail reconstruction on Mount McLoughlin

## STRENGTHS

Quick Learner    Eye for detail    Communicator

## LANGUAGES

C    C++    Python

## EDUCATION

### Ph.D. in Computer Science - Cryptography

**Oregon State University**

January 2020 – Ongoing

GPA: 4.00

### B.Sc. in Computer Science

**Oregon State University**

June 2019

GPA: 3.99

### B.Sc. in Mathematics

**Oregon State University**

June 2019

Overall GPA: 3.89