

# Eleanor McMurtry

MASTER'S CANDIDATE, APPLIED CRYPTOGRAPHY

on request | ✉ elem0@protonmail.com | 🏠 eleanorm.info | 📱 eleanor-em

## Summary

I am a recently-graduated Master of Science (Computer Science) student at the University of Melbourne, where I researched applied cryptography with Vanessa Teague. I have been a programmer for years, and am passionate about education, security, and privacy. Research interests include zero-knowledge proofs, post-quantum cryptography, and multiparty computation. This year I am due to begin my PhD in theoretical cryptography at ETH Zürich with Ueli Maurer.

## Education

### University of Melbourne

Victoria, Australia

M.Sc. (COMPUTER SCIENCE) (WITH DISTINCTION)

2019-2020

B.Sc. (MATHEMATICAL PHYSICS)

2015-2018

DIPLOMA IN INFORMATICS

2015-2018

## Experience

### University of Melbourne

Victoria, Australia

RESEARCH ASSISTANT

Jul 2019 - Present

- Working with Prof. Shanika Karunasekera to develop and deploy RAPID, a large distributed cloud-based system for data collection and analytics. The project allows large volumes of data (e.g. from social media) to be categorised by topic and analysed for patterns.
  - Responsibilities include finding and fixing issues, as well as developing new features and system monitoring scripts.
- Assisted the security research group with grant applications.
- Working with Dr Olya Ohrimenko on attacks against differentially private mechanism implementations.

### University of Melbourne

Victoria, Australia

HEAD TUTOR

Jul 2016 - Dec 2020

- Managed the tutoring team for a core subject (Object-Oriented Software Development) with hundreds of students, liaising between students, tutors, and lecturers.
- Developed major assignments for students, including specifications, marking criteria, and testing methodology.
- Delivered one to two lectures per semester on software tools and alternative paradigms while also teaching two to three tutorials per week.
- Tutor for various other subjects including Declarative Programming, Parallel & Multicore Computing, and Research Methods.

### CSIRO (Clayton campus)

Victoria, Australia

CASUAL IT OFFICER

Apr 2016-Apr 2017

- Worked with meteorologists to create interactive data visualisation tools for hurricane data.
- Wrote software to process large volumes of unstructured data and extract meaningful information.
- Used augmented reality to work with new data visualisation methods.

## Publications

Eleanor McMurtry, Olivier Pereira, Vanessa Teague. **When is a test not a proof?** *ESORICS (2020)*.

Eleanor McMurtry, Xavier Boyen, Chris Culnane, Kristian Gjøsteen, Thomas Haines, Ronald Rivest, Peter Ryan, Vanessa Teague. **Verifiable**

**Remote Voting with Paper Assurance.** *In Submission*.

Chris Culnane, Eleanor McMurtry, Robert Merkel, Vanessa Teague. **Tracing the challenges of COVIDSafe.** [Blog post](#).

## Honors & Awards

2020 **Best Technology**, Codebrew Hackathon

Victoria, Australia

2020 **Student Registration Grant**, IEEE Symposium on Security and Privacy

California, U.S.A.

2017 **Excellence in Tutoring Award**, School of Computing & Information Systems, Uni. of Melbourne

Victoria, Australia

## Presentation

### CSides

Canberra, Australia

SPEAKER

June 2020

- Presented an introduction to cryptography and formal notions of security.

- Presented an in-depth exploration of the COVIDSafe mobile app, focusing on the root causes of the issues with its application security.

## Projects

---

### **Cryptid & PaperVote**

UNIVERSITY OF MELBOURNE

*2019-2020*

- Cryptid (<https://github.com/eleanor-em/cryptid>) is a threshold ElGamal implementation in Rust, over Curve25519. It also implements various zero-knowledge proofs, including a shuffle proof based on that in Verificatum.
- PaperVote (<https://github.com/eleanor-em/papervote/>) is an implementation of a verifiable voting protocol using Cryptid, based around augmenting postal voting techniques.
- This project is related to Master's work and the paper "Verifiable Remote Voting with Paper Assurance".