Eleanor **McMurtry**

Software Developer, Educator, Cryptographer

☎ on request | ✉ elem0@protonmail.com | ⌂ lnor.net | eleanor-em

About me

An experienced software developer with a strong background in cryptography, both applied and academic. I have worked in many different environments and technologies to build reliable, secure, and user-friendly software. I am comfortable working on both the front- and back-end, and am fluent in Linux system administration. My experience in cryptography brings to the table knowledge of many common security pitfalls. Moreover, as an experienced educator I am able to share my knowledge to build a stronger team.

Languages: English (native), French and German (approx. B2)

Languages & technologies

Primary	Rust, Java, Linux, C, JavaScript, TypeScript, React
Secondary	C#, Python, Node.js, HTML & CSS, C++, Swift, Kotlin, Haskell, Docker, SQL

Experience

ETH Zurich

Zürich, Switzerland

Doctoral studies *Apr 2021-–present*

- Work in theoretical cryptography and composable security with Prof. Ueli Maurer.
- Developed skills in reading and synthesising complex technical documents at the forefront of cryptographic research.
- Supervised undergraduate and Master’s theses, forming close one-on-one mentoring relationships.
- Held weekly tutorial sessions for an undergraduate course in mathematics. Received excellent feedback on my teaching ability from students.

RightToAsk

Melbourne, Australia

Consultant *Jan 2021–Mar 2021*

- Project development for `RightToAsk`, an initiative to make it easy for voters to pose questions to their representatives while maintaining privacy using cryptographic protocols.
- Contracted at an early stage to explore the space and identify appropriate technologies for developing a high-security server and associated mobile app.
- Produced prototype software with detailed instructions for setting up an appropriate development environment, and navigating the intricate technology stack.
- Back-end development and cryptographic engineering with **Rust**, **C++**, **Python**, and **RabbitMQ**.
- Front-end development with **Xamarin** (**C#**) and **Swift**/**Kotlin**.

University of Melbourne

Melbourne, Australia

Research Assistant *Jul 2019–Jan 2021*

- Work with Prof. Shanika Karunasekera to develop and deploy RAPID, a 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.
  - Primary developer with responsibilities ranging from finding and fixing issues to developing new features and system monitoring tools across the full stack.
  - Back-end development with **Java**, **Apache Storm**, and **Apache Kafka**.
  - Front-end development with **React** and **TypeScript**.
  - Assisted with **system administration** and management.
- Work with Assoc. Prof. Olga Ohrimenko on developing attacks against differential privacy implementations.
  - Real-world attacks developed in **Python** against Opacus (a library for the **PyTorch** machine learning system) and Google Differential Privacy.
  - Work published as `Are We There Yet? Timing and Floating-Point Attacks on Differential Privacy Systems` in IEEE Symposium on Security and Privacy (2022).

University of Melbourne

Melbourne, Australia

Head Tutor *Jul 2016–Dec 2020*

- Managed the tutoring team for a core **object-oriented programming** subject with hundreds of students, liaising between students, tutors, and lecturers.
- Developed major assignments for students, including specifications, marking criteria, and testing methodology.
  - Developed `Bagel` for the major assignments, a game engine written in **Java** designed to make it easy for students to get started.
- Delivered one to two lectures per semester on software tools and alternative paradigms and taught two to three tutorials per week.
- Tutor for various other subjects including Declarative Programming (**Haskell**), Parallel & Multicore Computing (**C**, **HPC**), and Design of Algorithms (**C**).

CSIRO
Melbourne, Australia

Casual IT Officer
Apr 2016–Apr 2017

- Worked with meteorologists to create interactive data visualisation tools for hurricane data.
- Developed software using **Python** and **R** to process large volumes of unstructured data and extract meaningful information.
- Developed experimental data visualisation software for augmented reality using **C#** and **Unity**.

Education

University of Melbourne
Melbourne, Australia

M.Sc. in Computer Science (with Distinction)
2019–2020

`Thesis` in applied cryptography, designing a cryptographic protocol for verifiable postal voting, proving its security, and creating a proof-of-concept implementation in Rust. Part of this work was published as `When is a test not a proof?` in ESORICS (2020).

University of Melbourne
Melbourne, Australia

B.Sc. in Mathematical Physics
2015–2018

Completed concurrently with a Diploma in Informatics. Included a semester project evaluating the feasibility of a magneto-optical trap practical experiment for undergraduates.

Honors & Awards

2020	**Best Technology**, Codebrew Hackathon	*Melbourne, 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	*Melbourne, Australia*

Speaking

CSides
Canberra, Australia

Speaker
June 2020

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

metauni
The Internet

Seminar Presenter
2021-2022

- Presented a `seminar series` introducing attendees to foundational ideas in cryptography, composable security, and zero-knowledge proofs.

Selected Projects

PaperVote

University of Melbourne (Masters studies)
2019–2020

- `Cryptid` is a threshold ElGamal cryptosystem implementation in Rust. It also implements various zero-knowledge proofs, including a shuffle proof based on that in Verificatum.
- `PaperVote` is a proof-of-concept implementation of a verifiable postal voting protocol using Cryptid.

RoleCall (`GitHub`) (`Demo`)
2020

- A web application I developed in **React**/**TypeScript** and **Rust** to provide a simple map interface for tabletop role playing games with a focus on performance and avoiding unnecessary features. Development stopped due to a suitable alternative service becoming available.

Kanga (`GitHub`) (`Demo`)
2020

- An online execution environment for the `Roo` language written in **JavaScript**. The underlying compiler (**Haskell**) was developed during Master's coursework, with significant additional features implemented beyond the course requirements.