

Elizabeth van Oorschot

+1-613-698-4558 | evo.vanoorschot@gmail.com | elizabethvanoorschot.ca

 [elizabeth-van-oorschot](https://www.linkedin.com/in/elizabeth-van-oorschot) |  [lizz-zard.github.io](https://github.com/lizz-zard) |

EXPERIENCE

• Undergraduate Research Assistant

May 2024 - August 2024

Concordia University under Professor Jeremy Clark

Montreal, Canada

- Worked on a [handbook](#) for gadgets in the polynomial interactive oracle proof (Poly-IOP) model used by the succinct non-interactive argument of knowledge (SNARK) Plonk
- Main contributor to security proofs, commitment and polynomial level descriptions, and intuition sections
- Used Poly-IOP gadgets to devise a protocol for implementing a zero-knowledge call market auction
- Gained general cryptographic and blockchain background

• Junior Security Analyst

May 2023 - August 2023

Field Effect

Ottawa, Canada

- Worked on the Operational Development team in the area of network security
- Refactored code to improve efficiency in attack surface report generation
- Improved client awareness of security breaches by writing audience specific educational material and adding clarifying information to security alerts

EDUCATION

• McGill University

September 2022 - April 2026

B. Sc. Mathematics and Computer Science

Montreal, Canada

- GPA: 4.00/4.00

• Glebe Collegiate Institute

September 2018 - June 2022

Secondary Education

Ottawa, Canada

- GPA: 98.7/100 (top 6 senior classes)

PROJECTS

• Plonkbook: [Handbook on the Poly-IOP model used by Plonk]

May 2024 - August 2024

Joint work with Professor Jeremy Clark and Youwei Deng

plonkbook.org

- Wrote security proofs (Completeness, Soundness, Zero-Knowledge) for Poly-IOP gadgets
- Developed commitment and polynomial level descriptions of gadgets, as well as overviews of how they work in an intuition section for each

• Personal Website

August 2024

Hosted on Github Pages

elizabethvanoorschot.ca

SKILLS

- **Programming Languages:** Java, Python, C, MIPS assembly language
- **Other Background:** Linux/Bash; familiar with networking, circuits, blockchain, cryptography and security

HONOURS AND AWARDS

• Math and Physics Class of 1965 Prize

October 2024

McGill University

- Awarded to one math student and one physics student entering their penultimate year of study, on the basis of academic merit

• Undergraduate Student Research Award

May 2024 - August 2024

NSERC

- Funding for May to August 2024 undergraduate student research
- Recognition of research potential and academic aptitude in the sciences

• R.E. Powell Major Scholarship

September 2022 - May 2026

McGill University

- Major renewable scholarship at McGill University, conditional on maintaining high average

• Canadian National Champion (two consecutive years)

May 2021 and May 2022

Reach for the Top Trivia, Canada

- Captain of first in Canada high school trivia team (2022) and team member of first in Canada team (2021)