Elizabeth van Oorschot

+1-613-698-4558 | evo.vanoorschot@gmail.com | elizabethvanoorschot.ca
elizabeth-van-oorschot | lizz-zard.github |

Experience

- **Undergraduate Research Assistant (University of Waterloo)** *May 2025 - August 2025*
  NSERC USRA funded research with Professor Douglas Stebila Waterloo, Canada
  ◦ Research in post-quantum cryptography
- **Undergraduate Research Assistant (Concordia University)** *May 2024 - August 2024*
  NSERC USRA funded research with 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
- **Junior Security Analyst** *May 2023 - August 2023*
  Field Effect - Cybersecurity company Ottawa, Canada
  ◦ 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 and Talks

- **"Succinct Zero-Knowledge Proofs Using Polynomial Commitments"** *January 2025*
  Talk at Seminars in Undergraduate Mathematics in Montreal Conference slides
- **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:** C, OCaml, Java, Python, MIPS assembly language
◦ **Computer Background:** Linux/Bash; familiar with OS, networks, circuits, algorithm design, blockchain, cryptography and security
◦ **Mathematical Background:** Abstract and linear algebra, graph theory, combinatorics, calculus, probability

Honours and Awards

- **Math and Physics Class of 1965 Prize** *October 2024*
  McGill University
  ◦ Awarded on the basis of academic merit to one math student and one physics student entering their penultimate year of study
- **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)