Elizabeth van Oorschot

evo.vanoorschot@gmail.com | elizabethvanoorschot.ca | elizabeth-van-oorschot

Experience

- **Undergraduate Research Assistant (University of Waterloo)** *May 2025 - August 2025*
  NSERC USRA funded research with Professor Douglas Stebila Waterloo, Canada
  - Research in provable security and post-quantum cryptography
  - Devised and proved security of a variant of the Fujisaki-Okamoto transform that leverages confirmation codes to tie the functionality of a key encapsulation mechanism (KEM) to its security
- **Undergraduate Research Assistant (Concordia University)** *May 2024 - August 2024*
  NSERC USRA funded research with Professor Jeremy Clark Montreal, Canada
  - Wrote a handbook analyzing the mathematical gadgets in the polynomial interactive oracle proof (Poly-IOP) model that underpin the SNARK (succinct non-interactive argument of knowledge) called Plon
  - 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 clarifying 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

- **"Recognizing Faulty Implementations of PQ KEMs: Verifiable Decapsulation With(out) Algorithm Modifications"**
  Lewis Glabush, Felix Günther, Britta Hale, Kathrin Hövelmanns, Elizabeth van Oorschot, Douglas Stebila
  - Presentation submitted to Real World Crypto 2026 (decision pending)
- **"Succinct Zero-Knowledge Proofs Using Polynomial Commitments"** *January 2025*
  Elizabeth van Oorschot slides
  - 30 minute oral presentation at Seminars in Undergraduate Mathematics in Montreal 2025 Conference
- **Plonkbook: Handbook on the Poly-IOP model used by Plonk** *May 2024 - August 2024*
  Elizabeth van Oorschot, Youwei Deng, Jeremy Clark plonkbook.org
  - Handbook analyzing the mathematical operations used by the SNARK called Plonk

Skills

- **Programming Languages:** C, Python, OCaml, Java, MIPS assembly language
- **Computer Background:** Latex, Linux/Bash, OS, networks, circuits, artifical intelligence, algorithm design, blockchain, cryptography and security
- **Mathematical Background:** Linear algebra, abstract algebra, graph theory, analysis, calculus, probability

Honours and Awards

- **Sir Edward Beatty Memorial Scholarships in Mathematics** *October 2025*
  McGill University
  - Awarded in recognition of high academic merit to three students in Mathematics
- **Undergraduate Student Research Award** *May 2025 - August 2025*
  NSERC
  - Funding for May to August 2025 undergraduate student research at the University of Waterloo
- **Math and Physics Class of 1965 Prize** *October 2024*
  McGill University
  - Awarded on the basis of academic merit to one math 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 at Concordia University
- **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)