

Education

- Ongoing **Doctor of Philosophy**
Department of Computer Science
Supervised by Prof. Christophe Petit
Université Libre de Bruxelles
- 2020 – 2022 **Masters of Mathematics**, Thesis option
Department of Combinatorics and Optimization
Supervised by Prof. David Jao
University of Waterloo
- 2016 – 2020 **Honours Bachelor of Science**
Specialist Program in Mathematics, Comprehensive Stream
Graduated with High Distinction
University of Toronto

Awards

- | | |
|-----------|--|
| 2022-2026 | €30 721/a Fund for Research Training in Industry and Agriculture Grant |
| 2022 | €36 489 Université Libre de Bruxelles, Doctoral Scholarship (DECLINED) |
| 2021 | \$15 000 Queen Elizabeth II Graduate Scholarship in Science and Technology |
| 2021 | \$10 000 President's Graduate Scholarship, University of Waterloo |
| 2020 | \$2 000 Combinatorics and Optimization Department Award |
| 2020 | \$1 700 University of Waterloo Graduate Scholarship |
| 2020 | \$2 000 Math Domestic Graduate Student Award |
| 2020 | \$3 700 Graduate Research Studentship |
| 2018 | \$5 000 Canadian Queen Elizabeth II Diamond Jubilee Scholarship |
| 2016 | \$2 000 University of Toronto President's Entrance Scholarship |

Publications

Gustavo Banegas, **Valerie Gilchrist**, Benjamin Smith. *Efficient supersingularity testing over F_p and CSIDH key validation*. Mathematical Cryptology (MathCrypt 2022).

- Investigates algorithmic improvements to two supersingularity tests, in the context of CSIDH. Proposes a new algorithm for the state of the art, with a run-time improvement.
- Authors listed in alphabetical order.

Research Experience

Ongoing

Doctoral Research

Université Libre de Bruxelles

Worked under the supervision of Dr. Christophe Petit. Researched topics related to the cryptanalysis of post-quantum cryptosystems, with particular emphasis on isogeny-based systems.

Reviewed research papers on behalf of EuroCrypt 2023.

August 2023

Isogeny Graphs in Cryptography Workshop (Invited)

Banff International Research Station

Participated in brainstorming sessions for open problems in the field, and later worked in smaller groups to develop some of the ideas that were presented.

June 2023

Summer School on Real-World Crypto and Privacy

Vodice, Croatia

Was accepted into the summer school, hosted jointly by Radboud University, ETH Zurich, and University of Zagreb. Received partial funding from the school to attend, in the amount of a 450 euro fee waiver. Attended talks by industry professionals and academics in a wide variety of areas relating to cryptography and privacy.

Summer 2022 **Research Visit**

National Institute for Research in Digital Science and Technology (Inria)

Collaborated with Dr. Benjamin Smith and his team on projects related to isogeny-based cryptography including the use of radical isogenies in signature schemes and key validation techniques in key-exchange schemes. The visit was funded by both the University of Waterloo and Inria.

Published *Efficient supersingularity testing over F_p and CSIDH key validation* in the affiliate event of Crypto, MathCrypt. It was later published in a special edition of Mathematical Cryptology.

2020-2022

Master's Research

University of Waterloo

Researched isogeny-based cryptography under the supervision of Dr. David Jao. Explored different approaches of editing the signature scheme SQISign for use on off-blockchain transactions by studying already published adaptor signatures. The thesis was read and approved by Dr. David Jao, Dr. Douglas Stebila, and Dr. Alfred Menezes.

Reviewed research papers on behalf of AsiaCrypt 2021.

August 2021 **Isogeny Summer School**
University of Bristol

Attended an 11 week-long intensive summer school, lectured by more than 20 professionals and researchers working in the field. Topics spanned all areas relating to isogeny-based cryptography, including both implementation and theory concepts.

Teaching Experience

2020-2022 **Teaching Assistant**
University of Waterloo

Worked directly with professors to develop exam questions. Held weekly office hours and answered questions on the discussion forum for both undergraduate and graduate level students. Graded assignments and exams. Courses included:

- Applied Cryptography
- Public Key Cryptography
- Introduction to Combinatorics
- Introduction to Geometry

2017-2020 **Teaching Assistant**
University of Toronto

Lead weekly two hour and one hour tutorials with an average class size of 30 students. Wrote and graded quizzes/assignments. Invigilated and graded midterms and finals. Held weekly office hours. Courses included:

- *Calculus I for the Life Sciences*
- *Linear Algebra I for the Mathematical Sciences*
- *Calculus of Several Variables I*
- *Calculus of Several Variables II*
- *Algebraic Cryptography*

Performed grading duties for:

- *Introduction to General Relativity*
- *Introduction to Mathematical Logic*

Conferences and Invited Talks

2023 **Erasmus Mundus Cyberus**
Held Virtually

Gave an introduction to post-quantum cryptography as part of the Cyberus summer school for Masters students.

- 2023 **Isogeny Club**
Held Virtually
- Presented the talk *Computing rational isogenies from irrational kernel points* (video and slides available).
- 2022 **Isogeny Days (IsoCrypt)**
KU Leuven
- Presented on original research about supersingularity tests (video and slides available). Attended other technical talks. Participated in workshops, investigating new research problems.
- 2022 **MathCrypt (affiliate event of Crypto)**
University of California, Santa Barbara
- Presented on the accepted paper *Efficient supersingularity testing over F_p and CSIDH key validation* (video and slides available). Attended technical seminar talks.
- 2021 **Ottawa Math Conference**
Held virtually
- Presented on original research pertaining to an isogeny-based adaptor signature that uses SQISign as its underlying signature scheme.

Professional Experience

- 2018-2019 **Business Intelligence Work Study Student**
University of Toronto Scarborough Campus
- Regularly used Tableau and Microsoft Office programs.
- 2017 **Summer Student Data Analyst**
University of Toronto, Business Intelligence
- Regularly used programs such as Python, R, Tableau, VBA, and SQL.

Extracurricular and Volunteer Experience

- 2023 **Women in STEM Week at ULB**
Université Libre de Bruxelles
Gave talks to visiting school children to introduce them to the field of cryptography.
- 2020-2022 **Department of Combinatorics and Optimization Mentorship Program**
University of Waterloo
Worked with incoming graduate students to ease the transition into their programs.

- 2018-2019 **Association of Mathematics and Computer Science Students (AMACSS)**
University of Toronto Scarborough Campus
Held weekly office hours and exam review sessions for assigned courses.
- 2018 **Students Without Borders Internship Placement**
World University Service of Canada, Lilongwe, Malawi
Worked as a Knowledge Management Officer with a local NGO.

Languages

English (Native)

Spanish (Native)

French (Proficient, level B2+)