Valerie Gilchrist

Phone Number: (+33) 06 44 09 21 63
E-mail: valerie.gilchrist@ulb.be
vgilchri.github.io

Education

2022-2025	**Doctor of Philosophy** Department of Computer Science Supervised by Prof. Christophe Petit Defended on November 25, 2025 *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	€13 000 FNRS Various travel credits to attend academic events
2022-2026	€30 721/a Fund for Research Training in Industry and Agriculture Grant
2024	€4 000 ULB Faculté des Sciences travel credit
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 and preprints

Paul Frixons, **Valerie Gilchrist**, Péter Kutas, Simon-Philipp Merz, Christophe Petit, Lam L. Pham.
Another Look at the Quantum Security of the Vectorization Problem with Shifted Inputs.
Submitted. Available on eprint:2025/376.

- Studies the quantum security of a group action based hard problem. Presents a quantum algorithm from the literature for use in cryptography, showing an improvement in T-gate count and memory resources over the state-of-the-art security estimate.

Valerie Gilchrist, Laurane Marco, Christophe Petit, Gang Tang.
On the security of two blind signatures from code equivalence problems.
Communications in Cryptology, Volume 2, Issue 4 (2026).

- Studies two blind signatures whose security relies on code equivalence problems.
- One problem is shown to be polynomial time equivalent to LCE. The second problem is shown to have vulnerabilities to classical attacks.

Steven Galbraith, **Valerie Gilchrist**, Shai Levin, Ari Markowitz.
Further Connections Between Isogenies of Supersingular Curves and Bruhat-Tits Trees.
Submitted. Available on eprint:2024/1971.

- Studies the connection between the isogeny graph and the Bruhat-Tits tree.
- Makes explicit the correspondence between the Tate module labelling of the graph and the quaternion algebra labelling.

Steven D. Galbraith, **Valerie Gilchrist**, Damien Robert.
Improved algorithms for ascending isogeny volcanoes, and applications.
International Conference on Cryptology and Information Security in Latin America (LatinCrypt) 2025.

- Studies the worst-case complexity of the computation isogeny problem.
- Removes a heuristic assumption from the state-of-the-art, and improves the complexity in a special case.

Thomas Decru, Tako Boris Fouotsa, Paul Frixons, **Valerie Gilchrist**, Christophe Petit.
Attacking trapdoors from matrix products.
Communications in Cryptology, Volume 1, Issue 3, 2024.

- Considers a trapdoor that uses matrix products, proposed for use as encryption.
- Gives a classical attack that completely breaks one of the constructions, and analysis that suggests a significantly lower security level for the second construction.

Valerie Gilchrist, Laurane Marco, Christophe Petit, Gang Tang.
Solving the Tensor Isomorphism Problem for special orbits with low rank points: Cryptanalysis and repair of an Asiacrypt 2023 commitment scheme.
International Cryptology Conference (Crypto) 2024.

- Gives both distinguishing and computational polynomial time attacks on a previously published commitment scheme from tensors, completely breaking the security claims.
- Provides a repair by operating in a new, simpler framework.

Gustavo Banegas, **Valerie Gilchrist**, Anaëlle Le Dévéhat, Benjamin Smith.
Fast and Frobenius: Rational Isogeny Evaluation over Finite Fields.
International Conference on Cryptology and Information Security in Latin America (LatinCrypt) 2023.

- Improves runtimes of the state of the art for evaluating isogenies with both rational and irrational kernel groups.

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.

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 Crypto 2025, AfricaCrypt 2025, AsiaCrypt 2024, PQCrypto 2024, EuroCrypt 2023, and AsiaCrypt 2023. Served on the program committee for Public Key Cryptography (PKC) 2025.

August 2024 **Mathematics for post-quantum cryptanalysis**
Eötvös Loránd University and KU Leuven

Learned about the main areas of post-quantum cryptography and their mathematical foundations, as well as new emerging hardness assumptions. Presented a poster about original research (a cryptanalytic look at the Tensor Isomorphism Problem).

Spring 2024 **Research Visit**
University of Auckland

Collaborated with Dr. Steven Galbraith on projects related to isogeny-based cryptography. Project topics included computational number theory, and pairings-based cryptography. Spoke in two different seminar groups about original research.

August 2023 **Isogeny Graphs in Cryptography Workshop** (invited participant)
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. 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

2022-present **Teaching Assistant**
Université Libre de Bruxelles

Served as a teaching assistant for a variety of courses. Duties ranged from grading, giving tutorials/exercise sessions, writing exam questions, and supervising student project groups.
The majority of activities were conducted in French.
Courses included:

- Introduction to Python (for non computer science students)
- Third Year Projects course

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

2026 **Thematic Program (Isogeny cryptography)**
Okinawa Institute of Science and Technology (OIST)

Invited workshop participant. Participated in active research about the cryptanalysis of isogeny-based cryptography.

2025 **CatíoCrypto, affiliated with LatinCrypt** (invited speaker)

Gave an introductory class to isogeny-based cryptography (4 hours) to undergraduate and masters students. Lectures were entirely taught in Spanish.

2025 **Isogeny Days (IsoCrypt)** (invited speaker)
KU Leuven

Gave an expository talk about recent original research titled “The Quantum Security of the Vectorization Problem with Shifted Inputs.”

2024 **Rennes cryptography seminar** (invited speaker)
Université de Rennes

Gave a talk about recent research titled "Solving the Tensor Isomorphism Problem for special orbits".

2023 **SIAM Conference: Algebraic Geometry**
Eindhoven, Netherlands

Gave a talk in the post-quantum cryptography mini-symposium. Discussed original research about supersingularity testing of elliptic curves.

2023 **Erasmus Mundus Cyberus Summer School** (invited speaker)
Held Virtually

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

2023 **Isogeny Club** (invited speaker)
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.

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 Boarders 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+)

Italian (Basic, level A2)