



# LEONARDO COLÒ

NUMBER THEORY & CRYPTOGRAPHY

DOCTOR OF PHILOSOPHY IN MATHEMATICS

**Date of Birth:** 14 October 1994

**Nationality:** Italian

**Address:** 200 University Avenue W.,  
Mathematics and Computers (Office MC 5438),  
Waterloo, ON, N2L 3G1, Canada

**Email:** leo.colo.94@gmail.com

**Webpage:** <http://www.leonardocolo.com>

## SUMMARY

I am currently a Postdoc in the in the Department of Combinatorics and Optimization at the University of Waterloo under the mentorship of Prof. David Jao. My broad research interests lie at the crossroad between number theory and cryptography. In particular, I investigate various aspects of supersingular isogeny graphs and exploit their potential new cryptographic applications.

I am passionate about exploring the diverse applications of mathematics in cryptography and committed to advancing the field by developing innovative solutions and protocols that enhance security, privacy and efficiency.

## ACADEMIC POSITIONS

- **2023-2026 Postdoctoral Fellow.** University of Waterloo, ON Canada.
  - Research group of D. Jao and D. Stebila.
  - Funded by NSERC Alliance Quantum Consortia grant ALLRP 578463 - 22.
  - Program: *Accelerating the transition to quantum-resistant cryptography.*
- **2022-2023 ATER.** Aix-Marseille Université.
  - Attaché Temporaire d'Enseignement et de Recherche (1 year teaching contract).
  - Full time: 192h.
- **2021-2022 ATER.** Aix-Marseille Université.
  - Attaché Temporaire d'Enseignement et de Recherche (1 year teaching contract).
  - Full time: 192h.

## EDUCATION

- **2018-2022 PhD in Mathematics and Cryptography.** Aix-Marseille Université.
  - Advisor: *Prof. David Kohel.*
  - Thesis Title: *Oriented supersingular elliptic curves and class group actions.*
  - Number theory and cryptography.
- **2016-2018 Master Degree in Algebra and Number Theory.** ALGANT Master Program.
  - First year at Concordia University, Montréal (QC, Canada). **Cumulative GPA: 4.14/4.00**
  - Second year at Università degli Studi di Milano, Milano (Italy). **Grade: 110/110 cum Laude**
  - Thesis: *p-adic Abelian Integrals: from Theory to Practice*, supervised by Prof. Fabrizio Andreatta.
  - Algebraic & Algorithmic Number Theory, Algebraic Geometry, Rigid Geometry, Algebra.
- **2013-2016 Bachelor Degree in Mathematics.** Università degli studi di Milano.
  - Final Seminar: *Intersection of Ideals in a Multivariable Polynomial Ring.* **Grade: 110/110**
  - Courses on various aspects of mathematics, physics and computer science.
- **2008-2013 High School Diploma.** Liceo Scientifico Statale "Leonardo da Vinci", Milano (Italy).
  - Final research: *Mathematical models for the theory of conflicts.* **Grade: 100/100**
  - Training in both humanistic and scientific subjects.

## AWARDS

- Honors** ● Member of the Concordia University Chapter of the Golden Key International Honour Society.
- Scholarships** ●
  - ▶ "Progetto Eccellenze" awarded by Città di Pioltello, a.y. 2012/2013 & 2016/2017.
  - ▶ "Concordia International Tuition Award of Excellence" awarded by Concordia University, a.y. 2016/2017.
  - ▶ "Fondo per il sostegno dei giovani e per favorire la mobilità degli studenti" awarded by MIUR, a.y. 2013/2014.

## PUBLICATIONS

- 2026** ● **Supersingular isogeny graphs and Hecke modules with level structure.** arXiv  
With David Kohel.  
We study supersingular isogeny graphs with level structure and the associated Galois representations.
- 2026** ● **Weber modular curves and modular isogenies.** arXiv  
With David Kohel.  
We study Weber functions and the modular structures associated with them, with a view toward studying the isogeny graphs they define.
- 2025** ● **From orientations to  $\ell$ -adic period vectors.** arXiv  
We show how to relate orientations to homology classes on modular curves and to  $p$ -adic period invariants.
- 2022** ● **On a modular approach to the OSIDH protocol.** In preparation  
Avec David Kohel.  
We show how the use of modular curves equipped with level structure makes it possible to improve the complexity of the modular approach to the OSIDH protocol.
- 2020** ● **Orienting supersingular isogeny graphs.** arXiv  
Avec David Kohel. Journal of Mathematical Cryptology, vol. 14, no. 1, pp. 414 - 437  
We introduce a category of  $\mathcal{O}$ -oriented supersingular elliptic curves and study the structure of the associated graphs of  $\ell$ -isogenies.

## SELECTED TALKS

full list of talks at  
<https://leonardocolo.com/talks.html>

- Dec. 2025** ● **The modular symbol inversion problem.**  
Sèminaire ATI - Arithmétique et Théorie de l'Information (Marseille, France).
- Jul. 2024** ● **Supersingular isogeny graphs and Galois representations.**  
William Tutte Colloquium (Waterloo, Canada).
- Feb. 2023** ● **Oriented supersingular elliptic curves and class group actions.**  
Algebraic and combinatorial methods for Coding and Cryptography (Marseille, France).
- May 2021** ● **A modular approach to OSIDH.**  
AGC<sup>2</sup>T: Arithmetic, Geometry, Cryptography and Coding Theory (Marseille, France).
- Jun. 2019** ● **Orienting supersingular isogeny graphs.**  
Number-Theoretic Methods in Cryptology 2019 (Institut de Mathématiques de Jussieu, Paris, France).

## TEACHING EXPERIENCES

full list of courses at  
<https://leonardocolo.com/teaching.html>

- **2024-present** **Instructor.** University of Waterloo.
- **Jan. 2025** **Research froup facilitator.** CIMPA school, Kampala, Ouganda.
- **2021-2023** **Mission d'Enseignement ATER.** Aix-Marseille Université.
- **2019-2021** **Charges d'Enseignement pour Doctorant Contractuel.** Aix-Marseille Université.
- **2016-2017** **Instructor and Teaching Assistant.** Concordia University.
- **Mar-Jun 2016** **Trainee Teacher.** Liceo Scientifico Leonardo da Vinci, Milano.  
Internship supervised by Prof. Laura Chizzini.
- **Training** **Formation CIPE.** Aix-Marseille Université.  
40 hours of teaching training (formation pédagogique).

## WORKSHOPS

- **Aug. 2025** **Isogeny Graphs in Cryptography.** Banff International Research Station.  
Group Leader for the project "Class-group action signatures"

## SELECTED REFEREEING ACTIVITIES

- **2021** MathCrypt 2021 (Santa Barbara, USA).
- **2024** Algorithmic Number Theory Symposium XVI (Boston, USA).
- **2024** Eurocrypt 2025 (Madrid, Spain).
- **2025** Advances in Mathematics of Communications.

## ORGANIZATION ACTIVITIES

- **2025/2026** Reading group on Cryptography, University of Waterloo..
- **2024/2025** Crypto research group seminar, University of Waterloo..

## PROFESSIONAL DEVELOPMENT

- **2026** **CryptoWorks21.** University of Waterloo.
  - Training program in areas as cryptography, network security, quantum information standards, certification, intellectual property protection, and commercialization.
- **2025** **Information Security Specialist.** Fields Institute.
  - Fundamentals program.
  - Linux Operating System, Python Programming, Computer Networks, Mathematics for Cryptography.
- **2025** **Applied Cryptography.** Online course (Coursera), University of Colorado.
  - Modules: Cryptography and Information Theory, Symmetric Cryptography, Asymmetric Cryptography and Key Management, Cryptographic Hash and Integrity Protection.

## SELECTED SCIENTIFIC ACTIVITIES

### Participation research schools

- ▶ Spring school in Arithmetic statistics (Marseille, France), May 2023.
- ▶ Introduction to Symposium on arithmetic geometry and its applications (Marseille, France), February 2023.
- ▶ Spring master class "Cryptographie et codages à base des courbes et surfaces" (Marseille, France), April 2019
- ▶ Winter school on Mathematical foundations of asymmetric cryptography (Aussois, France), March 2019.
- ▶ ALGANT Summer school on Modular Forms (Padova, Italy), September 2017.

### Attended Conferences

- ▶ "Quantum Consortium Day", February 2025 (University of Toronto, Canada).
- ▶ "Algorithmic Number Theory Symposium - ANTS XVI", July 15–19, 2024 (Boston, USA)
- ▶ "Arithmetic Statistics", May 2023 (CIRM, Marseille, FRA).
- ▶ "Aix-Marseille Cyber Security Forum", April 2021 & May 2022 (Marseille, FRA).
- ▶ "Conférence de théorie des nombres Québec-Maine", October 2016 (Université Laval, Québec City, CAN).

### Reading groups

- ▶ Groupes de Travail at Aix-Marseille University, Marseille, FR.  
Rational Points on Curves over Finite Fields, Local fields, Quaternion algebras, Class field theory.
- ▶ Student seminars at McGill University, Montréal, CA.  
Modularity and the proof of Fermat's Last Theorem, Iwasawa Theory.

## LANGUAGES

### Italian

● Mother tongue.

### English

- Listening: **C1**      Reading: **C2**      Speaking: **C1**      Writing: **B2**
- ▶ June 2016. University of Cambridge ESOL Examinations: IELTS. **Grade 7.5 (CEFR C1)**
  - ▶ 2010/11. Language summer school in San Diego (USA).

### French

- Listening: **C1**      Reading: **C1**      Speaking: **C2**      Writing: **B2**
- ▶ 2019. 100 hours course organized by the doctoral school (Aix-Marseille Université).
  - ▶ June 2020. Intensive course (stage d'été) organized by SUFLE. **Level: Advanced**

## PROGRAMMING

### Familiar with

● C, HTML, CSS, Javascript, Matlab, Python, Sage, Magma,  $\LaTeX$ , Office Suites.

### Certifications

- ▶ HTML & CSS Level 1. CCA, Cambridge Certification Authority. May 2021.
- ▶ ECDL Certificate, European Computer Driving Licence. Mar. 2012.

## OTHER SKILLS

### Driving licence

● **Italy:** A2, B  
**Canada:** G

### Sport

- **Judo.** Activity at a competitive level.
  - ▶ Black Belt 1° Dan. Obtained by earning points in competitions (2019).
  - ▶ Participation to Italian and Canadian national championships.