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 5471), Waterloo, ON N2L 3G1, Canada
Email: lcolo@uwaterloo.ca
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.
- Funded by NSERC Alliance Quantum Consortia grant ALLRP 578463 - 22.
- Program: *Accelerating the transition to quantum-resistant cryptography*.

2021-2023 **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 over a Field.* **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. 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.
- "Progetto Eccellenze" awarded by Città di Pioltello, a.y. 2012/2013.
- "Borsa di Studio per gli studenti delle scuole secondarie di secondo grado" awarded by Città di Pioltello, a.y. 2011/2012.

PUBLICATIONS

In preparation **Formal group orientations.**
With David Kohel

Preprint **On a modular approach to the OSIDH protocol.**
With David Kohel

2020 **Orienting supersingular isogeny graphs.**
With David Kohel
Journal of Mathematical Cryptology, vol. 14.1, pp. 414 - 437
ePrint arXiv HAL

SELECTED TALKS

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

Oct. 2023 **Modular and formal orientations: beyond OSIDH.**
Isogeny Club.

Oriented supersingular elliptic curves and class group actions.
Mar. 2023 Séminaire LFANT - Lithe and fast algorithmic number theory (Bordeaux, France).
Feb. 2023 Algebraic and combinatorial methods for Coding and Cryptography (CIRM, Marseille, France).

A modular approach to OSIDH.
May 2022 Séminaire ATI - Arithmétique et Théorie de l'Information (Marseille, France).
May 2021 AGC^{2}T: Arithmetic, Geometry, Cryptography and Coding Theory (CIRM, Marseille, France).

Orienting supersingular isogeny graphs.
Jun. 2019 Séminaire CCA - Codage, Cryptologie, Algorithmes (Paris, France).
Jun. 2019 Number-Theoretic Methods in Cryptology 2019 (Institut de Mathématiques de Jussieu, Paris, France).
Jul. 2021 Isogeny-based cryptography school (Bristol, UK) - Online.

REVIEWS

CONFERENCES

2021 MathCrypt 2021 (Santa Barbara, USA).

SELECTED ACTIVITIES

Schools
- Spring school in Arithmetic statistics (Marseille, France), May 2023.
- Introduction to Symposium on arithmetic geometry and its applications (Marseille, France), February 2023.
- Winter school on Mathematical foundations of asymmetric cryptography (Aussois, France), March 2019.
- ALGANT Summer school on Modular Forms (Padova, Italy), September 2017.

Master class Spring master class "Cryptographie et codages à base des courbes et surfaces" (Marseille, France), April 2019.

Attended Conferences
- "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).

Working Seminars
- Groupe de Travail at Aix-Marseille University, Marseille, FR.
- Student seminars at McGill University, Montréal, CA.

TEACHING EXPERIENCES

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

a.y. 2021-2023 **Mission d'Enseignement ATER.** Aix-Marseille Université.

a.y. 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).

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).
- 2009. Language summer school in Malta.

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**

Spanish Listening: **B1** Reading: **B1** Speaking: **A2** Writing: **A2**

- Basic knowledge.
- 2005-2008: course in middle school.

PROGRAMMING

Familiar with C, HTML, CSS, Javascript, Matlab, Sage (Python), Magma, LaTeX, Office Suites.

Certifications

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

OTHER SKILLS

Driving licence A2, B.

Sport **Judo.** Activity at a competitive level.

- Black Belt 1° Dan. Obtained by earning points in competitions (2019).
- Participation to Italian national championships.