ALESSIO CAMINATA

Date of birth: 21/12/1987 | Place of birth: Genova, Italy

WORKING EXPERIENCE

Ricercatore a tempo determinato di tipo B (tenure-track) *November 2023 - Present*
Università di Genova, Italy

Ricercatore a tempo determinato di tipo A *October 2020 - October 2023*
Università di Genova, Italy

Maître assistant *October 2018 - September 2020*
Université de Neuchâtel, Switzerland

Marie Skłodowska-Curie Individual Fellow *March 2017 - September 2018*
Universitat de Barcelona, Spain

Assistant post-doctorant *March 2016 - February 2017*
Université de Neuchâtel, Switzerland

EDUCATION

"Doctor rerum naturalium" in Mathematics *February 2016*
Universität Osnabrück, Germany

Master's degree in Mathemathics *July 2011*
Università di Genova, Italy

Bachelor's degree in Mathemathics *July 2009*
Università di Genova, Italy

SCIENTIFIC PUBLICATIONS

- *A new multivariate primitive from CCZ equivalence* (with Marco Calderini and Irene Villa), in **Journal of Cryptology**, vol. 38, no. 25, 2025.
- *Quadratic Modelings of Syndrome Decoding* (with Ryann Cartor, Alessio Meneghetti, Rocco Mora, and Alex Pellegrini), in Niederhagen, R., Saarinen, MJ.O. (eds) **Post-Quantum Cryptography, PQCrypto 2025**, Lecture Notes in Computer Science, vol 15577, pp. 35–70, 2025.
- *Simplices osculating rational normal curves* (with Enrico Carlini and Luca Schaffler), in **Vietnam Journal of Mathematics**, 2024.
- *Structure of CSS and CSS-T Quantum Codes* (with Elena Berardini and Alberto Ravagnani), in **Designs, Codes and Cryptography**, vol. 92, pp. 2801–2823, 2024.
- *Determinantal varieties from point configurations on hypersurfaces* (with Han-Bom Moon and Luca Schaffler), in **International Mathematics Research Notices**, vol. 2023, no. 22, pp. 19743–19772, 2023.
- *Multidegrees, prime ideals, and non-standard gradings* (with Yairon Cid-Ruiz and Aldo Conca), in **Advances in Mathematics**, vol. 435, Part A, 2023.
- *The complexity of solving Weil restriction systems* (with Michela Ceria and Elisa Gorla) in **Journal of Algebra**, vol. 621, pp. 116–133, 2023.
- *Solving degree, last fall degree, and related invariants* (with Elisa Gorla) in **Journal of Symbolic Computation**, vol. 114, pp. 322–335, 2023.
- *The complexity of MinRank* (with Elisa Gorla) **WiNE III: Research Directions in Number Theory**, A. Cojocaru, S. Ionica and E. Lorenzo Garcia Eds., Lecture Notes in Computer Science, pp. 163–169, Springer, 2021.
- *A Pascal's theorem for rational normal curves* (with Luca Schaffler) in **Bulletin of the London Mathematical Society**, vol. 53, no. 5, pp. 1470–1485, 2021.
- *Nearly Gorenstein quotient singularities* (with Francesco Strazzanti) in **Beiträge zur Algebra und Geometrie**, vol. 62, no. 4, pp. 857–870, 2021.

- *Point configurations, phylogenetic trees, and dissimilarity vectors* (with Noah Giansiracusa, Han-Bom Moon, and Luca Schaffler) in **Proceedings of the National Academy of Sciences of the United States of America (PNAS)**, vol. 118, no. 12, March 23, 2021.
- *Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra* (with Elisa Gorla) in **Arithmetic of Finite Fields, 8th International Workshop**, J.C. Bajard and A. Topuzoglu Eds, Lecture Notes in Computer Science, 12542 LNCS, pp. 3–36, Springer 2021.
- *F-signature function of quotient singularities* (with Alessandro De Stefani) in **Journal of Algebra**, vol. 523, pp. 311–341, 2019.
- *Differential symmetric signature in high dimension* (with Holger Brenner) in **Proceedings of the American Mathematical Society**, vol. 147, no. 10, pp. 4147–4159, 2019.
- *Symmetric signature of cyclic quotient singularities* (with Lukas Katthän) in **Journal of Commutative Algebra**, vol. 11, no. 2, pp. 163–174, 2019.
- *Equations for point configurations to lie on a rational normal curve* (with Noah Giansiracusa, Han-Bom Moon, and Luca Schaffler) in **Advances in Mathematics**, vol. 340, pp. 653–683, 2018.
- *Generalized Hilbert-Kunz function in graded dimension two* (with Holger Brenner), in **Nagoya Mathematical Journal**, vol. 230, pp. 1–17, 2018.
- *The symmetric signature* (with Holger Brenner) in **Communications in Algebra**, vol. 45, no. 9, pp. 3730–3756, 2017.
- *Cohomological dimension and arithmetical rank of some determinantal ideals* (with Davide Bolognini, Antonio Macchia, and Maral Mostafazadehfard), in **Le Matematiche**, vol. 70, no. 1, pp. 273–300, 2015.

PREPRINTS

- *Cryptanalysis of a multivariate CCZ scheme* (with Elisa Gorla, Madison Mabe, Martina Vigorito, Irene Villa) to appear in **Designs, Codes and Cryptography**.
- *Hilbert-Kunz series, F-signature series, and weak p-fractals* (with Francesco Zerman) he Landscape of Commutative Algebra, editors M. Rossi, N.V. Trung, B. Ulrich, and J. Verma, to appear in the **Lecture Note Series of the London Mathematical Society**, Cambridge University Press.
- *F-signature functions of diagonal hypersurfaces* (with Samuel Shideler, Kevin Tucker, and Francesco Zerman).

GRANTS (PI)

- **PRIN PNRR 2022**. Awarded from the Italian Ministry of University and Research. Research project entitled "Mathematical Primitives for Post Quantum Digital Signatures", funded with €223,262 for the period 11/2023 – 28/2026, grant number P2022J4HRR.
- **Curiosity Driven Grant**. Grant awarded from Università di Genova within the Programme NextGEneration EU. Research project entitled "Algebraic Cryptanalysis of Rainbow", funded with €66,500 for the period 11/2022 – 10/2024.
- **Fondi di Ricerca di Ateneo**. Grant awarded from the Department of Mathematics. Research project entitled "Algebra commutativa: singolarità, deformazioni, e aspetti computazionali", funded with €14,000 for the period 03/2022 – 02/2024.
- **Marie Skłodowska-Curie Action: Individual Fellowship**. European Union's Horizon 2020 Research and Innovation Programme (H2020-MSCA-IF-2015), grant agreement no. 701807. Research project entitled "Frobenius related invariants and singularities", funded with €158,122 for the period 03/2017 – 02/2019.

GRANTS (MEMBERSHIP)

- **PRIN 2022**. Awarded from the Italian Ministry of University and Research. Research project entitled "Unirationality, Hilbert schemes, and singularities", funded with €213,925 for the period 02/2025 – 02/2027, grant number 2022K48YYP. PI: Giovanni Staglianò.

- **INdAM - GNSAGA Grant**. Awarded from the *Istituto Nazionale di Alta Matematica Francesco Severi*. Research project entitled "New theoretical perspectives via Gröbner bases", funded with €2.500 for the period 03/2023 - 02/2024. PI: Alessio D'Alì.
- **PRIN 2020**. Awarded from the Italian Ministry of University and Research. Research project entitled "Squarefree Gröbner degenerations, special varieties and related topics", funded with €535,920 for the period 01/2022 – 12/2024, grant number 2020355B8Y. PI: Matteo Varbaro.
- **Collaborate@ICERM**. Grant to pursue a joint research project at the ICERM of Brown University, USA in January 2023. Research project entitled "Point Configurations on Projective Varieties". Other participants: Noah Giansiracusa, Han-Bom Moon, and Luca Schaffler.
- **Àlgebra i Geometria**. Awarded from the *Agència de Gestió d'Ajuts Universitaris i de Recerca* (AGAUR) della Generalitat de Catalunya, funded with €44.480 for the period 01/2017 – 09/2021, grant number 2017SGR585. PI: Rosa Maria Miró Roig.

HABILITATIONS

- **Habilitation to "Professore di I fascia"** (Full Professor), area 01/A2 Algebra and Geometry, awarded by the Italian Ministry of University and Research, 2024.
- **Habilitation to "Professore di II fascia"** (Associate Professor), area 01/A2 Algebra and Geometry, awarded by the Italian Ministry of University and Research, 2022.
- **Habilitation to "Professor lector"** (Assistant Professor), awarded by the Agency of Quality of the Universities of Catalunya (AQU), 2020.

SELECTED INVITED TALKS

- Notions of Singularity in Different Characteristics, Banff Research Station, Canada, 10/2025.
- CIFRIS25 – Third National Conference, Roma, Italy, 09/2025.
- Workshop on the mathematics of post-quantum cryptography, Zürich, Switzerland, 06/2025.
- Algebra seminar, Trento, Italy, 03/2025.
- AMS–MAA Joint Mathematics Meetings, Seattle, USA, 01/2025.
- Nonlinear Algebra, Max Planck Institute, Leipzig, Germany, 12/2024.
- CrypTOgraphy Days, Torino, Italy, 05/2024.
- Workshop on Commutative Algebra and Algebraic Geometry in Prime Characteristics, ICTP Trieste, Italy, 05/2023.
- Workshop on Commutative Algebra and Algebraic Geometry, Catania, Italy, 09/2022.
- International Conference on Applications of Computer Algebra 2022, Istanbul, Turkey, 08/2022.
- Commutative Algebra, D-Modules and Singularities intertwined, Miraflores de la Sierra, Spain, 06/2022.
- Geometry Seminar Roma Tre, Rome, Italy, 05/2022.
- ACCESS, Algebraic Coding and Cryptography on the East Coast, virtual, 02/2022.
- GTM: Some Topics in Commutative Algebra and Algebraic Geometry, Torino, Italy, 09/2021.
- Cryptography and Coding Theory, First Annual Conference of the UMI, virtual, 09/2021.
- International Conference on Applications of Computer Algebra 2021, virtual, 07/2021.
- Algebra and Geometry, seminar, Ghent University, Belgium, 05/2021.
- AMS–MAA Joint Mathematics Meetings, Washington, USA, 01/2021.
- Groups, Arithmetic and Algebraic Geometry, seminar, EPF Lausanne, Switzerland, 04/2019.
- Coding Theory and Cryptography, seminar, Universität Zürich, Switzerland, 03/2018.
- Topics in Topology and Singularities, conference, Castellón de la Plana, Spain, 12/2017.
- Workshop on algebra devoted to Peter Schenzel, conference, Osnabrück, Germany, 10/2017.
- Algebraic Geometry, seminar, Fordham University, New York City, USA, 07/2017.
- Algebra and Geometry, seminar, KTH Stockholm, Sweden, 05/2017.
- Combinatorial Structures in Geometry, conference, Osnabrück, Germany, 08/2016.
- Giornate di Geometria Algebrica ed Argomenti Correlati XIII, conference, Catania, Italy, 05/2016
- Incontro di Algebra Commutativa, conference, Genova, Italy, 10/2015.

- Combinatorial and Experimental Methods in Commutative Algebra and Related Fields, conference, Osnabrück, Germany, 10/2015.

INVITED LECTURES

- *Multivariate Cryptography and Polynomial Systems*, 4 lectures, CoCoA School 2025, Genova, Italy, 07/2025.
- *Introduction à la cryptographie post-quantum*, 2 lectures, Colloque 2024 - Commission Romande de Mathématique, Champery, Switzerland, 09/2024.
- *Polynomial systems in post-quantum cryptography*, 5 lectures, IMUB, Barcelona, Spain, 03-04/2024.

EVENTS ORGANIZED

- **Modules & Rings: Recent Developments in Commutative Algebra. A conference in honor of Marilina Rossi**, Genova, Italy, 06/2025.
- **Young Cryptographers in Genova 2023 & 2024**, two conferences, Genova, Italy, 11/2023 and 11/2024.
- **Applications of Algebraic Geometry to Post-Quantum Cryptology**, session at SIAM Conference on Applied Algebraic Geometry 2023, Eindhoven, The Netherlands, 07/2023.
- **Algebra & Geometry Seminar**, weekly seminar of the Università di Genova, Italy, AY 2021-22 and AY 2022-23.
- **Polynomial Equations in Cryptography and Coding Theory** and **Applications of Algebraic Geometry to Cryptology**, sessions at SIAM Conference on Applied Algebraic Geometry 2019, Bern, Switzerland, 07/2019.
- **Frobenius Action in Commutative Algebra: Recent Developments**, conference, Barcelona, Spain, 01/2019.
- **Algebraic Geometry Seminar**, weekly joint seminar of the universities UB, UAB, and UPC of Barcelona, Spain, AY 2017-18.

MENTORING

- **Post-docs:** Irene Villa (Università di Genova, 2023–24).
- **PhD Students:** Andrea Sanguineti (Università di Genova, since 2022).
- **Master Students:** Christian Luyet (Université de Neuchâtel, 2020), Barbara Betti, Silvia Sconza (Università di Genova, 2022), Matteo Bertuzzo, Emanuele Di Giandomenico, Evelina Lanteri (Università di Genova, 2023), Massimo Ostuzzi (Università di Padova, 2023), Janet Geraci, Matteo Raffo, Simone Trebiani (Università di Genova, 2024), Mattia Cipro, Federico Raffo (Università di Genova, 2025).

TEACHING

- **Lecturer** of the following courses taught at Università di Genova, Italy: Algebra e Logica per Informatica (AY 2020-21, AY 2021-22, AY 2022-23, AY 2023-24, AY 2024-25), Teoria dei Codici e Crittografia (AY 2020-21 AY 2021-22), Teoria dei Codici (AY 2022-23, AY 2023-24), Crittografia (AY 2023-24, AY 2025-26).
- **Teaching Assistant** of the following courses taught at Università di Genova, Italy: Algebra 1 (AY 2024-25, AY 2015-26), Algebra 2 (AY 2015-26).
- **Lecturer** of the following courses taught at Université de Neuchâtel, Switzerland: Applied elliptic curves (AY 2019-20), Introduction à l'analyse fonctionnelle (AY 2018-19 and AY 2019-20), Algebraic curves (AY 2018-19), Cryptography (AY 2016-17).
- **Lecturer** of the following course taught at Universitat de Barcelona, Spain: Local Algebra (AY 2017-18).
- **Teaching Assistant** of the following courses taught at Universität Osnabrück, Germany : Lineare Algebra und analytische Geometrie I (AY 2015-16), Analysis II (AY 2014-15), Analysis III (AY

2015-16 and AY 2014-15), Local Cohomology and Toric Varieties (AY 2014-15), Mathematik für Anwender I (AY 2013-14, AY 2012-13, and AY 2011-12), Mathematik für Anwender II (AY 2013-14 and AY 2012-13), Vector Bundles (AY 2013-14), Algebraische Kurven (AY 2011-12).

MISCELLANEOUS

- **Invited Research Visits** at the following institutions: Universitat de Barcelona, Spain (03/2024–04/2024), Università di Roma Tre, Italy (05/2022), Università di Catania, Italy (11/2019), Fordham University, New York City, USA (07/2017), KTH, Stockholm, Sweden (05/2017), FMO, Oberwolfach, Germany (12/2016).
- **Expert Evaluator of Proposals** for the Horizon 2020 Marie Skłodowska-Curie Actions 2019 and 2020.
- **Project Reviewer** for the French "Agence Nationale de la Recherche" 2025.
- **Member of the Editorial Board** of "De Cifris Koine" book series published by De Cifris Press, focused on cryptography and related topics.
- **Member of the PhD Committee** of the following candidates: Roberta Barbi (Université de Neuchâtel, 2019), Stefano Canino (Politecnico di Torino, 2024), Giulia Gaggero (Université de Neuchâtel, 2024).
- **Member of the Program Committee** of the Workshop on Post-Quantum Cryptography PQ-Cifris 2022 (Università di Trento, 2022).
- **Referee** for Archiv der Mathematik, Beiträge zur Algebra und Geometrie, Communications in Algebra, Finite Fields and Their Applications, Journal of Algebra, Journal of Algebra and its Applications, Journal of Mathematical Cryptology, Journal of Pure and Applied Algebra, Proceedings of the American Mathematical Society, and SIAM Journal on Applied Algebra and Geometry (SIAGA).