

## ALLEGATO B

**UNIVERSITÀ DEGLI STUDI DI MILANO**

selezione pubblica per n.\_1 posto/i di Ricercatore a tempo determinato ai sensi dell'art.24,

comma 3, lettera b) della Legge 240/2010 per il settore concorsuale \_\_\_\_01/A2 Geometria \_\_\_\_\_ e Algebra,

settore scientifico-disciplinare \_\_\_\_\_MAT/03 - Geometria\_\_\_\_ presso il Dipartimento di \_\_\_\_\_MATEMATICA "FEDERIGO

ENRIQUES" \_\_\_\_\_,

(avviso bando pubblicato sulla G.U. n. \_\_. 46 del 11/06/2021 \_\_\_\_\_) Codice concorso \_4773\_

## **[Nome e cognome] CURRICULUM VITAE**

**(N.B. IL CURRICULUM NON DEVE ECCEDERE LE 30 PAGINE E DEVE CONTENERE GLI ELEMENTI CHE IL CANDIDATO RITIENE UTILI AI FINI DELLA VALUTAZIONE.**

**LE VOCI INSERITE NEL FACSIMILE SONO A TITOLO PURAMENTE ESEMPLIFICATIVO E POSSONO ESSERE SOSTITUITE, MODIFICATE O INTEGRATE)**

### **INFORMAZIONI PERSONALI (NON INSERIRE INDIRIZZO PRIVATO E TELEFONO FISSO O CELLULARE)**

<b>COGNOME</b>	<b>CERIA</b>
<b>NOME</b>	<b>MICHELA</b>
<b>DATA DI NASCITA</b>	[ 03, 07, 1984 ]

# Michela Ceria

**About Me** Born on 03/07/84, Biella (IT). Non-tenure track researcher, Polytechnic of Bari.

## Academic positions

**22/12/2020 – now** Non-tenure track researcher, Dept. of Mechanics, Mathematics and Management; Polytechnic of Bari (IT) Art. 24, c. 3, lett. a) Law 240, 30/12/2010

**1/05/2018 – 21/12/2020** Postdoc at Dept. of Computer Science, Univ. of Milan (IT). Art.22–Law 240, 30/12/2010

**26/04/2017 – 25/04/2018** Postdoc at Dept. of Mathematics, Univ. of Trento (IT). Art.22–Law 240, 30/12/2010

**07/04/2015 – 06/04/2017** Postdoc at Dept. of Engineering and Computer Science, Univ. of Trento (IT). Art.22–Law 240, 30/12/2010

## Awards, Scholarships and grants

**French qualification to the function of *Maître de Conférences*** *Mathematics* (11/02/2015 – 31/12/2019, n. 15225277843; 31/01/2019 – 31/12/2023, n. 19225277843), *Applied Mathematics* (04/02/2015 – 31/12/2019, n. 15226277843), *Computer Science* 19/02/2021, n. 21227277843.

**2011–2013 PhD scholarship** Funded by INdAM (National Institution of High Mathematics).

**2017–2018 Grant** ISCRA-CINECA, IsC50\_OGBC4EC, HP10C3HFL2, “Optimization of Groebner Basis computations for ECDLP”, with F.Pintore, M.Sala and A.Visconti

## Research Interests (Keywords)

**Combinatorial aspects of Computational Algebra; Commutative and noncommutative Groebner bases; Coding Theory and Cryptography; Computational Algebraic Geometry and Commutative Algebra;  $q$ -matroids theory, designs and rank metric codes; Finite geometry.**

## Publications

**2021** *Bits, bytes and friends* (book), accepted by the scientific committee of the “Cryptography” series of Aracne eds. With G.Rinaldo, M.Sala

**2021** *Why you cannot even hope to use Ore algebras in Cryptography*, *Applicable Algebra in Engineering, Communication and Computing*, DOI: 10.1007/s00200-021-00493-9, With T.Mora, A.Visconti.

**2020** *A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS*. *Mathematics* 2020, 8 (10), 1782. DOI: 10.3390/math8101782 With C.Lepore, A.Visconti, U.Pratap Rao, K.Arvinbhai Shah, and L.Zanolini

**2020** *Combinatorial decompositions for monomial ideals*, *Journal of Symbolic Computation*, Volume 104, May–June 2021, Pages 630–652 DOI:10.1016/j.jsc.2020.09.004

**2020** *Toward involutive bases over effective rings*, Special issue of *Applicable Algebra in Engineering, Communication and Computing*, concerning “Algebraic Geometry from an Algorithmic point of View”, 31, 359–387. DOI: 10.1007/s00200-020-00448-6. With T.Mora

**2020** *Sublime Experience: New Strategies for Measuring the Aesthetic Impact of the Sublime*, In: Emmer M., Abate M. (eds) *Imagine Math 7*. Springer, Cham. DOI: 10.1007/978-3-030-42653-8\_11, with M.Mazzocut-Mis, A.Visconti, H.Tahayori

- 2020** *Why you cannot even hope to use Gröbner bases in cryptography: an eternal golden braid of failures*, Special issue of Applicable Algebra in Engineering, Communication and Computing, concerning "Computer Algebra and application to combinatorics, coding theory and cryptography", 31, pages 235–252. Doi: 10.1007/s00200-020-00428-w With B.Barkee, T.Moriarty, A.Visconti.
- 2020** *HELP: a sparse error locator polynomial for BCH codes*, Special issue of Applicable Algebra in Engineering, Communication and Computing, concerning "Computer Algebra and application to combinatorics, coding theory and cryptography", 31, pages 215–233. Doi: 10.1007/s00200-020-00427-x With T.Mora, M.Sala
- 2019** *Zech Tableaux as tools for sparse decoding*. Rend. Semin. Mat. Vol. 78, 1 (2020), 43 – 56 ISSN: 0373-1243 With T.Mora, M.Sala.
- 2019** *Bar Code vs Janet tree*. Atti della Accademia Peloritana dei Pericolanti, Classe di Scienze Fisiche, Matematiche e Naturali VOL 97, NO 2 (2019) Doi: 10.1478/AAPP.972A6
- 2019** *Measuring Performances of a White-box Approach in the IoT Context*. Symmetry 2019, 11(8), 1000; Doi: 10.3390/sym11081000 With D.Albricci, A.Shakiba, A.Visconti, F. Cioschi, N.Fornari
- 2019** *Applications of Bar Code to involutive divisions and a greedy algorithm for complete sets. (extended abstract)* International Conference Polynomial Computer Algebra '2019 St. Petersburg, Russia April 15–20, 2019 International Euler Institute – ISBN 978-5-96511-1234-0
- 2019** *Weak involutive bases over effective rings (extended abstract)* International Conference Polynomial Computer Algebra '2019 St. Petersburg, Russia April 15–20, 2019 International Euler Institute – ISBN 978-5-96511-1234-0 With T.Mora
- 2019** *Bar code: a visual representation for finite sets of terms and its applications* Mathematics in Computer Science, 14(2), 497–513 (2020), online in 2019 doi:10.1007/s11786-019-00425-4
- 2019** *A general framework for Noetherian well ordered polynomial reductions* Journal of Symbolic Computation, Vol. 95, P. 100–133 ISSN: 0747-7171, Doi: 10.1016/j.jsc.2019.02.002 With T.Mora, M.Roggero
- 2019** *Bar code for monomial ideals*. Journal of Symbolic Computation, Doi: 10.1016/j.jsc.2018.06.012 vol. 91, p. 30–56, ISSN: 0747-7171
- 2018** *Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game (abstract)* Doi: 10.15304/978841695487 In 24th Conference on Applications of Computer Algebra – ACA 2018: Proceedings, Applications of Computer Algebra, Santiago de Compostela, Spain, June 18–22, 2018. With T.Mora
- 2018** *Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game (extended abstract)* International Conference Polynomial Computer Algebra '2018 St. Petersburg, Russia April 16–21, 2018 International Euler Institute – ISBN 978-5-9651-1141-1 With T.Mora
- 2018** *Efficient computation of squarefree separator polynomials (extended abstract)* Doi:10.1007/978-3-319-96418-8\_12 In: Davenport J., Kauers M., Labahn G., Urban J. (eds) Mathematical Software – ICMS 2018. Lecture Notes in Computer Science, vol 10931p. 98–104, Springer, ISBN: 9783319964171, ISSN: 1611-3349, South Bend, 2018, with T.Mora, A.Visconti.
- 2017** *Buchberger-Zacharias Theory of Multivariate Ore Extensions*. Doi: 10.1016/j.jpaa.2017.02.011 Journal of Pure and Applied Algebra, vol. 221, p. 2974–3026, ISSN: 0022-4049. With T. Mora
- 2017** *Bitcoin, la moneta virtuale per transazioni reali*, Interlex, may 2017. With M.Sala
- 2017** *Buchberger-Weispfenning Theory for Effective Associative Rings*. Doi: 10.1016/j.jsc.2016.11.008 Journal of Symbolic Computation, vol. 83, p. 112–146, ISSN: 0747-7171. With T.Mora
- 2016** *Bitcoin e Blockchain*, with F.Pintore, M.Sala. Aused Informa, 98.
- 2016** *A computational approach to the theory of adjoints*. Doi: 10.1478/AAPP.942A7 Atti della Accademia Peloritana dei Pericolanti, Classe di Scienze Fisiche, Matematiche e Naturali, vol. 94, p. 1–14, ISSN: 1825-1242.
- 2015** *Term-ordering free involutive bases* Doi: 10.1016/j.jsc.2014.09.005, Journal of Symbolic Computation, vol. 68, p. 87–108, ISSN: 0747-7171, with T.Mora, M.Roggero

**2014** *A proof of the “Axis of Evil theorem” for distinct points. Rendiconti del Seminario Matematico*, vol. 72, p. 213–233, ISSN: 0373–1243 (2014).

## Other accepted works

**2019** *Bar Code and Janet-like division (extended abstract)*, accepted for a talk at ACA2019.

**2019** *Weak Involutive bases over effective rings (extended abstract)*, accepted for a talk at ACA2019 With T.Mora.

**2019** *HELP: the knight gambit for efficient decoding of BCH codes (extended abstract)*, accepted for a talk at ACA2019. With T.Mora, M.Sala.

**2019** *Why you cannot even hope to use Gröbner bases in cryptography: an eternal golden braid of failures (extended abstract)*, accepted for a talk at ACA2019. With B.Barkee, T.Moriarty, A.Visconti.

**2019** *Combinatorial decompositions for monomial ideals (extended abstract)*, accepted for the poster presentation at MEGA2019.

**2018** *Combinatorics of ideals of points: a Cerlienco–Mureddu-like approach for an iterative lex game* Accepted for a talk at ACA 2018, PCA 2018. With T.Mora.

**2017** *On the discrete logarithm problem for prime-field elliptic curves* Accepted for a computation presentation at MEGA 2017. With A.Amadori, F.Pintore, M.Sala

## Submitted works

**2021** *On near-MDS codes and caps*, with A. Cossidente, G. Marino, F. Pavese

**2021** *Secret sharing schemes from hypersurfaces over finite fields*, with A.Aguglia and L. Giuizzi

**2021** *Weighted Subspace Designs from  $q$ -Polymatroids*, with E. Byrne, R. Jurrius, S. Ionica.

**2021** *Optimizing the key-pair generation phase of McEliece cryptosystem*, with A. De Piccoli, M. Tiziani, A. Visconti

**2021** *Construction of new  $q$ -cryptomorphisms*. with E. Byrne and R. Jurrius

**2020** *Efficient cryptanalysis over multivariate Ore extensions* With T. Moriarty and A.Visconti

**2020** *Bar Code and Janet-like division*

## Available in Arxiv

**2019** *Macaulay, Lazard and the Syndrome Variety* arXiv:1910.13189 [math.CO].

## In preparation

**Paper** *Degroebnerization and its applications: a new approach for data modelling* With T. Mora and A. Visconti

**Paper** *Constructions of new matroids and designs over  $GF(q)$* , accepted (01/09/2020), but withdrawn (25/06/2021) by *Women in Numbers Europe III: Research Directions in Number Theory. Papers from the Workshop (WIN-E3) held at La Hublais, Cesson-Sévigné (France), August 26–30, 2019. Edited by Alina Cojocaru, Sorina Ionica and Elisa Lorenzo García. Association for Women in Mathematics Series. Springer.* With E.Byrne, S.Ionica, R.Jurrius, E.Saçikara

**Paper** *Applications of Bar Code to involutive divisions and a greedy algorithm for complete sets.*

**Paper** *A trojan Diffie–Hellman-like protocol based on proof of gullibility*, with, A.De Piccoli, T.Moriarty and A.Visconti.

**Paper** *Half error locator polynomials for efficient decoding of binary cyclic codes*

**Paper** *Combinatorics of ideals of points: a Cerlienco–Mureddu-like approach for an iterative lex game.* With T.Mora

**Paper** *Towards involutive bases for effective algebras*

**Paper** *A variant of the iterative Moeller algorithm for giving Pommaret basis and its factorization*

## Distributed software

**2012** *JMBTest.lib: a J-marked basis tester* Library available from Singular 3-1-6:

<https://www.singular.uni-kl.de/index.php/singular-download.html>

**2012** *JMSConst.lib: a J-marked schemes constructor* Library available from Singular 3-1-6:

<https://www.singular.uni-kl.de/index.php/singular-download.html>

## Organized Conferences

**Annual congress** In the organizing committee for the Annual conference organized by the group CRITTOGRAFIA E CODICI (National Mathematical Union) and by De Componendis Cifris.

**ACA202(1)** Organizer (with T.Mora and A- Leroy) of the session Effective Ideal Theory in Commutative and non-Commutative Rings and its Applications. Online, July 2021.

**Widecom2019** Local Chair and member of the Technical Committee for the conference Widecom2019 – 11-13 Feb. 2019

**One-day workshops** Contribution to the organization of

- the one-day workshop on *Blockchain and Innovative Applications*, 10/02/2017
- the one-day workshop on *Cryptographic Aspects of Cloud and Distributed Computing*, 28/10/2016

**MEGA 2015** Contribution to the local organization of the conference MEGA 2015, Univ. of Trento, Italy; 15-19 June 2015.

**Miniworkshop Coding Theory and Cryptography** 13-14 Oct. 2014, Univ of Turin. Organization, with C.Marcolla.

## Visiting

**Neuchâtel** 10-12-2019 – 13-12-2019 I have been invited to Univ. of Neuchâtel by Prof. E. Gorla for research purpose and for delivering two seminars, one for the *research seminar on coding theory and cryptography* and the second for the *algebra seminar* (joint with Freiburg).

**Rennes** 26-08-2019 – 30-08-2019 Participation (completely funded) to the project WINE3 Workshop – Women in Numbers Europe 3 (3rd edition of the European WIN Workshop) In particular participation to the project by E. Byrne (University College Dublin) & R. Jurrius (The Netherlands Defense Academy) Title: q-Analogues in Combinatorics.

**Linz** 10-12-2018 – 15-12-2018 Invited for a seminar to the Univ. of Linz by Prof. M. Kauers.

**Kaiserslautern** During the period May-November 2012, I made short visits to *Univ. of Kaiserslautern* (Germany) and worked with Prof. W. Decker and H. Schoenemann. I implemented two libraries for the software Singular, which have been integrated in version 3-1-6 of the software. <http://www.singular.uni-kl.de/index.php/singular-devteams.html>. Moreover, I followed some courses on computational algebraic geometry.

## Referee (from 22-09-2016 on)

**Journals and conferences** I have been a referee for the journals *AAECC* (Applicable Algebra in Engineering, Communication and Computing), *JSC* (Journal of Symbolic Computation), *Mathematische Nachrichten*, *Mathematics*, *Advances in Mathematics of Communications*, *Security and Communication Networks*, *Theoretical Computer Science and Internet of Things: Engineering Cyber Physical Human Systems*; moreover I have been a referee for the conferences *ISSAC* (International Symposium on Symbolic and Algebraic Computation), *MEGA* (International conference On Effective Methods in Algebraic Geometry), *ITASEC 2020* and *WTSC* (Workshop on Trusted Smart Contracts).

## Reviews

**Zentralblatt Math 2012-today** 5 papers. **Mathematical Reviews 2017-today** 4 papers.

## Research groups

**European Women in Mathematics (2019-)** In 2020: part of the Corona Crisis Working Group

**UMI National Mathematical Union (2018-)** In 2020: among the proposers of the Cryptography and Coding Theory group

## [De Componendis Cifris National association in Cryptography \(Autum 2017-\)](#)

## [GNSAGA National Group for Algebraic and Geometrical structures and their Applications \(2012-\)](#)

### References

[Prof. T. Mora](#) Univ. of Genoa – 5919@unige.it

[Prof. B. Buchberger](#) RISC, Johannes Kepler University – bruno.buchberger@risc.jku.at

### Students

**Bachelor** Thesis co-advisor for four students with Prof. P. Valabrega and for six students with Prof. A. Visconti. External advisor with Prof T. Mora for two students.

**Master** Master Thesis co-advisor for five students with Prof. M. Sala (one in collaboration with Dr. J. Shokrollahi of Bosh GmbH); Master Thesis co-advisor for one student with Dr. G. Rinaldo and for a student with Professor A. Visconti. Thesis opponent for 4 students.

**Tutoring 10-04-2015 — 25-04-2018** I have been tutor of 14 students, studying in the Major *Coding Theory and Cryptography* (now called *Cryptography*) of the Master of Degree in Mathematics at Univ. of Trento, helping them with their study plans, average grade and in deciding about their internships in companies.

### Conferences, Schools, Seminars (invited speaker)

**Seminar Mar. 05 2021** Joint PolSys SpecFun Seminar, Sorbonne University, Paris (online). Title: Combinatorics of ideal of points and Half Error Locator polynomials.

**Seminar Dec. 11 2020** Séminaire de l'équipe CASC Univ. Grenoble-Alpes (in French). Title: Dégroëbnérisation: théorie et applications

**Seminar Nov. 26 2020** Séminaire Limousin de Calcul Formel en VISIO (in French). Title: Degroebnerisation et ses applications

**Seminar Nov. 24 2020** Seminar at the MAX Computer Algebra seminar, École polytechnique, Palaiseau. Title: Degroebnerization and error correcting codes: Half Error Locator Polynomial.

**Conference Oct. 12-17, 2020** Invited speaker at PCA2020. Title[1]: Groebner bases and error correcting codes: from Cooper Philosophy to Degrobnerization. Title[2]: Bar Code and involutiveness: Janet and Janet-like divisions.

**Conference July 13-16, 2020** Invited speaker to the session “Gröbner Bases in Theory and Practice” of ICMS 2020, Braunschweig, Germany. Title: Do It Yourself: Buchberger and Janet Base solver effective rings Part 3: What happens to involutive bases?

**Seminar 21 May 2020** *De Cifris Augustae Taurinorum in webinar*. Title: Why you should not even think to use Ore algebras in Cryptography

**Seminar 9 Apr. 2020** Invited for a seminar (online, in French) at the *séminaire Mathématiques Discrètes, Codes et Cryptographie*, Univ. of Paris 8. Title: *Bases de Gröbner, degroebnerisation et leurs applications à la théorie des codes et à la cryptographie*

**Seminars 10-13 Dec. 2019** Univ. of Neuchâtel. Title [1]: *Half error locator polynomials for efficient decoding of binary cyclic codes*. [2]: *Combinatorics of ideals of points: Groebner escaliers, separator polynomials and applications to Algebraic Statistics*.

**Seminar 8 Nov. 2019** I have been invited by Prof. Ulmer at Univ. of Rennes for a seminar. Title: *Half error locator polynomials for efficient decoding of binary cyclic codes*.

**Seminar 6 Jun. 2019** Invited by Univ. of Milano Bicocca. Title: *Efficient computation of squarefree separator polynomials and applications to algebraic statistics*.

**Seminar 13 Dec. 2018** Invited by Univ. of Linz. Title: *DIY for Groebner bases: multivariate Ore extensions and effective rings*.



**Seminar 5 Dec. 2018** Invited by Univ. of Genoa. Title: *DIY for Groebner bases: multivariate Ore extensions*.

**Seminar 4 Dec. 2018** Invited by Univ. of Genoa. Title: *Bitcoin, blockchain and their applications*.

**Seminar 27 Mar. 2018** Invited by CTI Liguria for a seminar at Palazzo Ducale, Genoa. Title: *La crittografia dietro Bitcoin e blockchain*.

**Seminar 20 Dec. 2017** Invited for a seminar at Univ. of Genoa. Title: *Combinatorics of involutive divisions*.

**Seminar 19 Dec. 2017** Invited for a seminar at Univ. of Genoa. Title: *Bitcoin, Blockchain e loro Applicazioni*.

**Conference 26-27 Oct. 2017** Invited speaker to the *2nd Number Theory Meeting - Turin*, Polytechnic of Turin Title: *Groebner bases and ECDLP: Involution*.

**Conference 29-30 May 2017** Invited speaker at *Theory and Computation in Algebra and Algebraic Geometry with a dedication to Paolo Valabrega on the occasion of his 70(+2)th Birthday*, Univ. of Turin  
Title: *Combinatorics of involutive divisions*

**Conference 4-7 Jun. 2014** Invited speaker at the conference *Giornate di Geometria Algebrica e Argomenti Correlati XII*, Salone d'Onore del Castello del Valentino, Turin. Title: *Basi involutive "Term-ordering free"*

## Selected Conferences, Schools, Seminars (speaker/poster)

**Conference 14-15 Jun.2021** Poster at AlCoVE: an Algebraic Combinatorics Virtual Expedition (online). Title: *Constructions of new  $q$ -cryptomorphisms*.

**Conference 7-11 June 2021** Speaker at MEGA2021 . Title: *Degroebnerization and its applications: a new approach for data modelling*.

**Conference 28 May 2021** Speaker at Giornata INdAM Unità di Ricerca di Bari 2021 MATEMATICA E INDUSTRIA con lo sguardo della Prof.ssa Rosa Maria Mininni. Title: *Why you cannot even hope to use Ore algebras in Cryptography*

**Conference 19-24 Apr.2021** Speaker at PCA2021 (online). Title: *Degroebnerization and its applications: a new approach for data modelling*

**Conference 15-16 Jun.2020** Poster at AlCoVE: an Algebraic Combinatorics Virtual Expedition (online). Title: *Constructions of new matroids and designs over  $\mathbb{G}_f(q)$*

**Conference 2-7 Sept.2019** Speaker at *Congresso UMI - Pavia, Italy*. Title: *Bar Code: a visual representation for finite sets of terms and its applications*

**Conference 16-20 July 2019** Speaker at *ACA 2019 - Montréal, Canada*. Title [1]: *Bar Code and Janet-like division* [2]: *HELP: the knight gambit for efficient decoding of BCH codes*

**Conference 24-27 June 2019** Speaker at *NCRA VI - Lens, France*. Title: *Why you should not even think to use Ore algebras in Cryptography*

**Conference 16-21 June 2019** Poster presentation at *MEGA2019 - Madrid, Spain*. Title: *Combinatorial decompositions for monomial ideals*

**Conference 15-20 Apr. 2019** Speaker at *PCA2019 - St.Petersburg, Russia*. Title: *Applications of Bar Code to involutive divisions and a greedy algorithm for complete sets*.

**Conference 11-13 Febr. 2019** Tutorial Speaker at *Widecom2019 - Milan, Italy*. Title: *Efficient cryptographic algorithms for securing passwords*.

**Summer School Aug. 2018** Participation to the poster session of *AEC 2018 - RISC, Linz, Austria*. Title: *Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game*.

**Conference 24-27 July 2018** Participation as speaker to *ICMS 2018 - Notre Dame, Indiana, USA*. Title: *Efficient computation of squarefree separator polynomials*.

**Conference 18-22 June 2018** Participation as speaker to *ACA 2018 – session Algorithms for zero-dimensional ideals* – Santiago de Compostela – Spain. Title: *Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game*.

**Conference 2-7 Apr. 2018** Participant to the poster session of the conference *Symmetry and Computation*, CIRM – Luminy – Marseille. Title: *Combinatorics of involutive divisions*

**Conference 12-16 June 2017** Participation as speaker to *MEGA 2017. Effective methods in Algebraic Geometry*, Univ. of Nice, France. Title: *Bar Code for monomial ideals*

**Summer School and Conference 1 – 10 July 2015** Speaker at the conference *Current Trends on Groebner Bases*, Osaka, Japan. Title: *A unifying form for noetherian polynomial reductions*. Participation to the summer school.

**Conference 3- 7 June 2013** Participation to the poster session of the convention *MEGA 2013. Effective methods in Algebraic Geometry*, Univ. of Frankfurt, Germany. Title: *JMBTest.lib and JMSConst.lib: Singular Tools for J-Marked Schemes*.

**Summer School 24-28 June 2013** *EACA'S Second International School On Computer Algebra and Applications*, Univ. of Valladolid, Spain. Seminar titled: *Bar-codes for monomial ideals*. Participation to courses.

**Seminar Dec. 2012** Polytechnic of Turin Title: *L'Asse del Male* (The Axis-of-Evil Theorem).

**Summer School 1-13 Oct. 2012** *Algebra for Secure and Reliable Communication Modeling*, Institute of Physics and Mathematics of the Univ. of Michoacán, Mexico. Lecturer of a seminar titled: *The Axis-of-Evil Theorem*. Participation to courses.

**Conference 17-21 Sept. 2012** Participation as a speaker to the convention *MAP 2012 – Mathematics, Algorithms and Proofs*, Univ. of Konstanz, Germany. Title: *The Axis-of-Evil algorithm*. Participation to the 'Young Researchers' Session' with a brief talk on my research activities.

**Summer School July-Aug. 2012** *PHD School on Groebner Bases, Curves, Codes and Cryptography*, Univ. of Trento. Seminar titled: *A Bar-Code algorithm for the 'Axis of Evil' Theorem*. Participation to courses.

**Summer school Oct. 2011** *International School on Computational Commutative Algebra and Algebraic Geometry*, Villa Pace-Univ. of Messina. Seminar titled: *Classification of Adjoint Curves*. Participation to courses.

## Teaching Experience – University courses

**Apr.-May 2020** PhD course for the Dept. of Computer Science, Univ. of Genoa "Blockchain 101", with M. Ribaudo

**Supplementary course; 21 and 23 May 2018** Invited by Univ. of Genoa, within the course "Additional Useful Knowledge", Master in Computer Science. *A crash course in Bitcoin and Blockchain [part 1 and 2]*.

**18/09/2017 – 16/02/2018** Master Degree in Mathematics, Univ. of Trento: *Advanced Coding Theory and Cryptography* with M.Sala and CryptoLabTN.

**14/09/2015 – 12/02/2016 and 14/09/2016 – 17/02/2017** Master Degree in Mathematics, Univ. of Trento: *Algebraic Cryptography*, with M.Sala and CryptoLabTN.

**2016** PhD in Mathematics, Univ. of Trento: *Groebner Bases applied to Cryptography and Coding Theory*, with E.Bellini, M.Piva and M.Sala

**2013–2014** Bachelor in Engineering, Polytechnic of Turin, *Geometry*, with G.Casnati.

**2011–2013** Bachelor in Engineering, Polytechnic of Turin, *Geometry*, with C.Massaza.

## Teaching Experience – courses for professionals

**May 2018** Lecturer for the course *Post-Quantum Cryptography* for the part on multivariate post-quantum cryptography. Scientific coordination: M.Sala.

**Nov. 2017** Lecturer for the course *Monero: the dark side of cryptocurrencies* Prof.: M.Sala.

**Oct. 2017** Lecturer for the course *Bitcoin, Blockchain and their new frontiers in Milan* Prof.: M.Sala.



**May 2017** Lecturer for the course *Bitcoin, Blockchain and their new frontiers in Trento* Prof.: M.Sala.

**Nov. 2016** Assistant Lecturer for the courses *Bitcoin, Blockchain and their new frontiers in Milan*, *Bitcoin, Blockchain and their new frontiers in Rome*. Prof.: M.Sala.

**Sept. 2016** Assistant Lecturer for the course *Bitcoin, Blockchain and their new frontiers II*, Univ. of Trento Prof.: M.Sala.

**May 2016 – May 2017** Assistant Lecturer for the course *Bitcoin, Blockchain and their new frontiers*, Univ. of Trento Prof.: M.Sala.

## Teaching Experience – e-learning and courses' coordination

**Course coordination 2018/2019** Coordination (*Professore a contratto*) for the blended course in Computer Science for the faculty of Linguistic Mediation.

**E-learning 2015 – 2018** *Applications of Cryptography to Security and Privacy* and *BoAB: Bitcoin and other Applications of Blockchain*, with M.Sala.

## Teaching Experience – experience at school

**November 2014** Liceo Istituto Comprensivo S. Francesco d'Assisi – Biella Brief mathematics substitute teaching.

**Summer 2014** Liceo Giuseppe & Quintino Sella – Classico Linguistico Artistico Mathematics recovery course.

## Editorial activity

I am going to be editor for a special issue of AAEECC, together with M. Sala (Univ. of Trento) and A. Bracciali (Univ. of Stirling). Such issue, titled "Crypto-assets: from algebraic cryptography to cryptocurrencies, blockchain technology, smart contracts and DeFi tokens" has been approved by the Managing Board.

## Education

**2011–2013 Univ. of Turin, Italy** *PhD in Mathematics*, Defence:14/02/2014. Title of PhD Thesis: *Combinatorial structure of monomial ideals*. Prof.: M.G. Marinari, T. Mora, M. Roggero.

**2007–2010 Univ. of Turin, Italy** *Master degree in Mathematics* Defence on 20/07/2010 with grade 110/110 cum laude and mention.

Title of MSc Thesis: *Conductor and adjoints of algebraic curves*. Prof.: M. Roggero and P. Valabrega.

**2003–2007 Univ. of Turin, Italy** *Bachelor degree in Mathematics* Faculty of Mathematical, Physical and Natural Science, Univ. of Turin · Bachelor degree obtained on 27/04/ 2007 with grade 104/110.

Title of Bachelor Thesis: *Matroids and parking functions*. Prof.: M. Roggero.

## Foreign languages

**Italian** Mother tongue; **English** Good, IELTS (Academic), got in Sept. 2010, grade 7; **French**

Scholastic, B1 MC Graw Hill certificate got online; **Japanese** Scholastic.

## Software Development Skills

**OS:** Linux (Ubuntu), Microsoft Windows, Mac OS X, Android. **Programming:** C/C++ (basic notions), Singular, Magma. **Softwares:** Singular, Cocoa, Maple, Magma. **E-learning:** Moodle,

Sakai, Google Classroom. **Videoconference:** Zoom, BBB, Skype, Google Meet.

## Other information

**Advisory Board** I contributed to the creation of an *Advisory Board* of companies in Trento. These companies financed stages and scholarships for students and iterfaced with the Department, highlighting the specific knowledge they would need for people to work within them.

**Hopf Algebras course** followed the Hopf algebra Course held by Prof. Ardizzoni to the PhD School in Mathematics at Univ. of Turin.

**Lie Algebras course** followed the Lie algebra Course held by Prof. De Graaf to the PhD School in Mathematics at Univ. of Trento.

**Diffusion:** Researchers' night (Turin and Trento), instructor for olympic games in Mathematics.  
Bari, 09/07/2021

Data

09/07/2021

Luogo

Bari