

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 a) della Legge 240/2010 per il settore concorsuale 01/B1 - Informatica, settore scientifico-disciplinare INF/01 - Informatica presso il Dipartimento di Informatica "Giovanni degli Antoni", (avviso bando pubblicato sulla G.U. n. 96 del 06/12/2019) Codice concorso 4242

**[Michela Ceria]
CURRICULUM VITAE**

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

COGNOME	CERIA
NOME	MICHELA
DATA DI NASCITA	03/07/1984

**INSERIRE IL PROPRIO CURRICULUM
(non eccedente le 30 pagine)**

Michela Ceria

About Me Born in Biella, Italy; 3 July 1984.

Postdoc at the Department of Computer Science - University of Milan, Italy, from may 2018: *Advanced methods and technologies in Computer Science*.

Academic positions

1 May 2018 - · University of Milan, Italy ·

Department of Computer Science · *Postdoc position*: Advanced methods and technologies in Computer Science.

26 April 2017 - 25 April 2018. · University of Trento, Italy ·

Department of Mathematics · *Postdoc position*: Algebraic Cryptography and Theory of Cyclic Codes.

07 April 2015 - 06 April 2017 · University of Trento, Italy ·

Department of Engineering and Computer Science · *Postdoc position*: Algebraic Cryptography for Online Courses

Awards, Scholarships and grants

French qualification to the function of Maître de Conférences

Mathematics (11/02/2015 - 31/12/2019, number 15225277843; 31/01/2019 - 31/12/2023, number 19225277843) *Applied Mathematics* (04/02/2015 - 31/12/2019, number 15226277843).

2011-2013 · PhD scholarship

Three-year PhD Scholarship, funded by INdAM (National Institution of High Mathematics). INdAM Tutor for the scholarship: Prof. A.Verra (University Roma Tre).

Mobility fundings

I got fundings by INdAM (National Institute of high mathematics) to participate to the conferences Current trends on Groebner bases, ICMS2018, PCA2019, ACA2019

May-November 2012 · Regional fundings

Regional fundings for the visiting period in Kaiserslautern (Germany).

Research Interests

Combinatorial aspects of Computational Algebra

Commutative and noncommutative Groebner bases

Coding Theory and Cryptography

Computational Algebraic Geometry and Commutative Algebra

For more information see the enclosed Research Statement.

Publications

2019

Zech Tableaux as tools for sparse decoding. accepted for publications in Rendiconti del Seminario Matematico. Authors: M. CERIA, 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:<http://dx.doi.org/10.1478/AAPP.972A6> Author: M. CERIA.

2019

Bar code: a visual representation for finite sets of terms and its applications Math.Comput.Sci. (2019) doi:10.1007/s11786-019-00425-4 Author: M.CERIA

2019

Measuring Performances of a White-box Approach in the IoT Context. Symmetry 2019, 11(8), 1000; <https://doi.org/10.3390/sym11081000> Authors: D. ALBRICCI, M. CERIA, 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 Author: M. CERIA

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 Author: M. CERIA, T. MORA

2019

A general framework for Noetherian well ordered polynomial reductions *Journal of Symbolic Computation*, ISSN: 0747-7171, <https://doi.org/10.1016/j.jsc.2019.02.002> Authors: M. CERIA, T. MORA, M. ROGGERO

2019

Bar code for monomial ideals. *Journal of Symbolic Computation*, DOI:<https://doi.org/10.1016/j.jsc.2018.06.012> vol. 91, p. 30-56, ISSN: 0747-7171, Author: M. CERIA

2018

Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game (abstract) DOI: <http://dx.doi.org/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. Authors: M. CERIA, 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 Authors: M. CERIA, T. MORA

2018

Efficient computation of squarefree separator polynomials (extended abstract) DOI:https://doi.org/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, Authors: M. CERIA, T. MORA, A. VISCONTI.

2017

Buchberger-Zacharias Theory of Multivariate Ore Extensions. DOI: <https://doi.org/10.1016/j.jpaa.2017.02.011> *Journal of Pure and Applied Algebra*, vol. 221, p. 2974-3026, ISSN: 0022-4049. Authors: M. CERIA, T. MORA

2017

Bitcoin, la moneta virtuale per transazioni reali, Interlex, may 2017. Authors: M. CERIA, M.SALA

2017

Buchberger-Weispfenning Theory for Effective Associative Rings. DOI:<https://doi.org/10.1016/j.jsc.2016.11.008> *Journal of Symbolic Computation*, vol. 83, p. 112-146, ISSN: 0747-7171. Authors: M. CERIA, T.MORA

2016

Bitcoin e Blockchain, Authors: M. CERIA, F. PINTORE, M. SALA Aused Informa, 98.

2016

A computational approach to the theory of adjoints. DOI: <http://dx.doi.org/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. Author: M. CERIA

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, Authors: M. CERIA, 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) Author: M. CERIA

Other accepted works

2019

Bar Code and Janet-like division (extended abstract), accepted for a talk at ACA2019 Authors: M. CERIA.

2019

Weak Involutive bases over effective rings (extended abstract), accepted for a talk at ACA2019 Authors: M. CERIA, T. MORA.

2019

HELP: the knight gambit for efficient decoding of BCH codes (extended abstract), accepted for a talk at ACA2019 Authors: M. CERIA, 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. Authors: B. BARKEE, M. CERIA, T. MORIARTY, A. VISCONTI.

2019

Combinatorial decompositions for monomial ideals (extended abstract), accepted for the poster presentation at MEGA2019. Authors: M. CERIA.

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 Authors: M. CERIA, T. MORA.

2017

On the discrete logarithm problem for prime-field elliptic curves Accepted for a computation presentation at MEGA 2017. Authors: A. AMADORI, M. CERIA, F. PINTORE, M. SALA

Submitted works

2019

Weak Involutive bases over effective rings, Authors: M. CERIA, T. MORA

2019

A trojan Diffie-Hellman-like protocol based on proof of gullibility, Authors: M. CERIA, A. DE PICCOLI, T. MORIARTY and A. VISCONTI.

2019

Why you cannot even hope to use Gröbner bases in cryptography: an eternal golden braid of failures, Authors: B. BARKEE, M. CERIA, T. MORIARTY, A. VISCONTI.

2019

Bar Code and Janet-like division Author: M. CERIA

2019

HELP: a sparse error locator polynomial for BCH codes Authors: M. CERIA, T. MORA, M. SALA .

2019

Sublime Experience: new strategies for measuring the aesthetic impact of the sublime Authors: Maddalena Mazzocut-Mis, Andrea Visconti, Hooman Tahayori and Michela Ceria

2019

Combinatorial decompositions for monomial ideals , Author: M. CERIA

2019

A performance-based approach to compare the Blockchain consensus procedures: PoW vs PoS vs Pure PoS. Authors: C. LEPORE, M.CERIA, A. VISCONTI, U. PRATAP RAO, K. ARVINDBHAI SHAH, and L. ZANOLINI

Available in Arxiv

2017

Combinatorics of involutive Divisions arXiv:1707.02452 [math.AC] Author: M. CERIA

In preparation

Book

Bits, bytes and friends Authors: M. CERIA, G. RINALDO and M. SALA

Paper

Macaulay, Lazard and the Syndrome Variety Authors: M. CERIA.

Paper

Half error locator polynomials for efficient decoding of binary cyclic codes Authors: M. CERIA.

Paper

Applications of Bar Code to involutive divisions and a greedy algorithm for complete sets., Author: M. CERIA

Paper

Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game. Authors: M. CERIA, T. MORA

Paper

Towards involutive bases for effective algebras, Authors: M. CERIA, probably in cooperation with T. MORA

Paper

A variant of the iterative Moeller algorithm for giving Pommaret basis and its factorization, Author: M. CERIA

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> Author: M. CERIA

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> Author: M. CERIA

Submitted software

AffMarkedSchemes.lib Prototype library for Singular which performs Affine Marked Schemes computation. *Submitted to Singular Team.* Author: M. CERIA

Organized Conferences

Widecom2019

Local Chair and member of the Technical Committee for the conference Widecom2019 - 11-13 February 2019

One-day workshops

As assistant of Prof. M. Sala, I contributed 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

As assistant of Prof. M. Sala, I contributed to the local organization of the international conference MEGA 2015, University of Trento, Italy; June 15 – 19, 2015.

Miniworkshop Coding Theory and Cryptography

Organization of the miniworkshop *Coding Theory and Cryptography*, 13th and 14th October 2014, University of Turin. In collaboration with Doctor Chiara MARCOLLA (University of Trento).

Visiting

Neuchâtel

10-12-2019 – 13-12-2019 I have been invited to University 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*.

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. A paper will be submitted to a referenced proceedings based on the project.

Linz

10-12-2018 – 15-12-2018 Invited for a seminar and for research purpose to the University of Linz by Prof. M. Kauers.

Kaiserslautern

During the period May-November 2012, I made short visits to *University 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*, *Advances in Mathematics of Communications*, *Security and Communication Networks* 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) and *WTSC* (Workshop on Trusted Smart Contracts).

Reviews

Zentralblatt Math · 2012-Today

Reviewed papers:

- C. Chen, J.H. Davenport, M.M Maza, B. Xia, R. Xiao, *Computing with semi-algebraic sets: relaxation techniques and effective boundaries*. *J. Symb. Comput.* 52, 72-96 (2013).
C. Dönch, *Characterization of relative Gröbner bases*, *J. Symb. Comput.* 55, 19-29 (2013).
C. Bopp, *Syzygies of 5-Gonal Canonical Curves*, *Documenta Mathematica* 20 (2015) 1055–1069.

Mathematical Reviews · 2017-Today

Reviewed papers:

- V. Levandovskyy et al., *A factorization algorithm for G-algebras and its applications*, *J. Symbolic Comput.* 85 (2018)
Huishi Li, *An elimination lemma for algebras with PBW bases*, *Communications in Algebra* 2018, VOL. 46, NO. 8, 3520–3532 <https://doi.org/10.1080/00927872.2018.1424863>
Li, Zijia, Josef Schicho, and Hans-Peter Schröcker. *Factorization of motion polynomials*. *Journal of Symbolic Computation* 92 (2019): 190-202.

Research groups

European Women in Mathematics (2019 -)

UMI · National Mathematical Union (2018 -)

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

University of Genoa - 5919@unige.it

Prof. B. Buchberger

Research Institute for Symbolic Computation (RISC) Johannes Kepler University - bruno.buchberger@risc.jku.at

Students

Bachelor

Thesis co-advisor for five students with Prof. A. Visconti. External advisor with Prof T. Mora for two students.

Master

Master Thesis co-advisor for four 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.

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 University of Trento, helping them with their study plans, average grade and in deciding about their internships in companies.

Conferences, Schools, Seminars (invited speaker)

Seminars · 10-13 December 2019

University of Neuchâtel. Title of the seminar [1]: *Half error locator polynomials for efficient decoding of binary cyclic codes*. Title of the seminar [2]: *Combinatorics of ideals of points: Groebner escaliers, separator polynomials and applications to Algebraic Statistics*.

Seminar · 8 November 2019

I have been invited by Prof. Ulmer at University of Rennes for a seminar. Title of the seminar: *Half error locator polynomials for efficient decoding of binary cyclic codes*.

<https://irmar.univ-rennes1.fr/seminaire/genre/geometrie-et-algebre-effectives>

Seminar · 6 June 2019

Invited by University of Milano Bicocca. Title of the talk: *Efficient computation of square-free separator polynomials and applications to algebraic statistics*.

<https://www.matapp.unimib.it/it/eventi/efficient-computation-squarefree-separator-polynomials-and-applications-algebraic-statistics>

Seminar · 13 December 2018

Invited by University of Linz. Title of the talk: *DIY for Groebner bases: multivariate Ore extensions and effective rings*. <http://www.algebra.uni-linz.ac.at/talks/schedule.php>

Seminar · 5 December 2018

Invited by University of Genoa. Title of the talk: *DIY for Groebner bases: multivariate Ore extensions*. <https://commalge.tumblr.com/post/180718172787/algebrageometry-seminar>

Seminar · 4 December 2018

Invited by University of Genoa. Title of the talk: *Bitcoin, blockchain and their applications*.

Seminar · 21 and 23 May 2018

Invited by University of Genoa. Title of the talks: *A crash course in Bitcoin and Blockchain [part 1 and 2]*.

Seminar · 27 March 2018

Invited by CTI Liguria for a seminar at Palazzo Ducale, Genoa. Title of the talk: *La crittografia dietro Bitcoin e blockchain*.

Seminar · 20 December 2017

Invited for a seminar at University of Genoa. Title of the talk: *Combinatorics of involutive divisions*.

Seminar · 19 December 2017

Invited for a seminar at University of Genoa. Title of the talk: *Bitcoin, Blockchain e loro Applicazioni*.

Conference · 26-27 October 2017

Invited speaker to the *2nd Number Theory Meeting - Turin*, Polytechnic of Turin Title of the seminar: *Groebner bases and ECDLP: Involution*.

http://ntmeeting.polito.it/2nd_Number_Theory_Meeting.html

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*, University of Turin

Title of the talk: *Combinatorics of involutive divisions*

<http://www.theoryandcomputation.unito.it/node/4>

Conference · 4-7 June 2014

Invited speaker at the conference *Giornate di Geometria Algebrica e Argomenti Correlati XII*, Salone d'Onore del Castello del Valentino, Turin.

Title of the talk: *Basi involutive "Term-ordering free"* (Term-ordering free involutive bases).

<http://ricerca.mat.uniroma3.it/users/lopez/GGAACXII/Conferenzieri.html>

Conferences, Schools, Seminars (speaker/poster)

Conference · 2-7 September 2019

Speaker at Congresso UMI - Pavia, Italy. Title of the talk: *Bar Code: a visual representation for finite sets of terms and its applications* <http://umi.dm.unibo.it/congresso2019/>

Conference · 16-20 July 2019

Speaker at ACA 2019 - Montréal, Canada. Title of the talk [1]: *Bar Code and Janet-like division* Title of the talk [2]: *HELP: the knight gambit for efficient decoding of BCH codes* <http://aca2019.etsmtl.ca/>

Conference · 24-27 June 2019

Speaker at NCRA VI - Lens, France. Title of the talk: *Why you should not even think to use Ore algebras in Cryptography* <http://leroy.perso.math.cnrs.fr/Congres2019/Main2019.HTML>

Conference · 16-21 June 2019

Poster presentation at MEGA2019 - Madrid, Spain. Title of the poster: *Combinatorial decompositions for monomial ideals* <http://eventos.ucm.es/12097/detail/mega-2019.html>

Conference · 15-20 April 2019

Speaker at PCA2019 - St.Petersburg, Russia. Title of the talk: *Applications of Bar Code to involutive divisions and a greedy algorithm for complete sets.* <https://pca-pdmi.ru/2019/>

Conference · 11-13 February 2019

Tutorial Speaker at Widecom2019 - Milan, Italy. Title of the talk: *Efficient cryptographic algorithms for securing passwords.* <http://www.widecomconference.org/nsittest.co.nf/index.html>

Summer School · August 2018

Participation to the poster session of AEC 2018 - RISC, Linz, Austria. Title of the poster: *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 of the talk: *Efficient computation of squarefree separator polynomials.* <http://icms-conference.org/2018/ICMS2018Schedule.pdf>

Conference · 18-22 June 2018

Participation as speaker to ACA 2018 - session *Algorithms for zero-dimensional ideals* - Santiago de Compostela - Spain. Title of the talk: *Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game.* https://www.unilim.fr/pages_perso/vincent.neiger/aca18/

Conference · 2-7 April 2018

Participant to the poster session of the conference *Symmetry and Computation*, CIRM - Luminy - Marseille. Title of the poster: *Combinatorics of involutive divisions* <https://www.cirm-math.fr/ProgWeebly/Renc1772/Prog1772.pdf>

Seminar · September 2017

Findomestic, Florence. Lecturer of a seminar titled: *Introduzione alla tecnologia blockchain ed alle sue principali applicazioni* (Introduction to blockchain technology and its main applications).

Conference · 12-16 June 2017

Participation as speaker to MEGA 2017. *Effective methods in Algebraic Geometry*, University of Nice, France. Title of the talk: *Bar Code for monomial ideals* <https://mega2017.inria.fr/>

Seminar · 4 November 2016

Speaker to the miniworkshop *Seminari di Teoria dei Numeri* Title of the seminar: *Half Error Locator Polynomial for binary cyclic codes.* <https://www.dipmatematica.unito.it/do/home.pl/View?doc=teorianumeri.html>

Seminar · April 2016

SGS, Verona Lecturer of a seminar titled: *E-Voting e Blockchain.*

Seminar · May 2016

Polytechnic of Turin Title of the talk: *Crittografia e sicurezza del sistema Bancomat* (Cryptography and security of the Bancomat system).

Summer School · July 2015 ·

Participation to the poster session of the summer school *AEC, 2nd Algorithmic and Enumerative Combinatorics Summer School 2015* Title of the poster: *Bar Codes and Strongly Stable Ideals* . Participation to the summer school.

Summer School and Conference · 1 - 10 July 2015

Speaker at the conference *Current Trends on Groebner Bases*, Osaka, Japan. Title of the talk: *A unifying form for noetherian polynomial reductions*. Funded by INdAM. Participation to the summer school.

Miniworkshop · 13-14 October 2014

Speaker at the miniworkshop *Coding Theory and Cryptography*, Department of Mathematics, University of Turin. Title of the talk: *Polinomi locatori sparsi per codici ciclici binari* (Sparse locator polynomials for binary cyclic codes).

<https://www.unito.it/eventi/miniworkshop-coding-theory-and-cryptography>

Seminar · April 2014

Polytechnic of Turin. Title of the talk: *Basi involutive "Term-ordering free"* (Term-ordering free involutive bases).

Conference · 3- 7 June 2013

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

<https://www.math.uni-frankfurt.de/mega2013/program.shtml>

Summer School · 24-28 June 2013

EACA'S Second International School On Computer Algebra and Applications, University of Valladolid, Spain. Lecturer of a seminar titled: *Bar-codes for monomial ideals*. Participation to courses.

Seminar · December 2012

Polytechnic of Turin Title of the talk: *L'Asse del Male* (The Axis-of-Evil Theorem).

Summer School · 1-13 October 2012

Algebra for Secure and Reliable Communication Modeling, Institute of Physics and Mathematics of the University of Michoacán, Mexico. Lecturer of a seminar titled: *The Axis-of-Evil Theorem*. Participation to courses.

Conference · 17-21 September 2012

Participation as a speaker to the convention *MAP 2012 - Mathematics, Algorithms and Proofs*, University of Konstanz, Germany. Title of the seminar: *The Axis-of-Evil algorithm*. Participation to the 'Young Researchers' Session' with a brief talk on my research activities. https://cms.uni-konstanz.de/fi_leadadmin/archive/map2012/schedule-and-slides/index.html

Summer School · July-August 2012

PHD School on Groebner Bases, Curves, Codes and Cryptography, University of Trento. Lecturer of a seminar titled: *A Bar-Code algorithm for the 'Axis of Evil' Theorem*. Participation to courses.

Summer school · October 2011

International School on Computational Commutative Algebra and Algebraic Geometry, Villa Pace-University of Messina. Lecturer of a seminar titled: *Classification of Adjoint Curves*. Participation to courses.

Followed Conferences and Schools

Conference · June 2017

Fq13 - The 13th International Conference on Finite Fields and their Applications, Gaeta.

Conference · April 2015

The Ninth International Workshop on Coding and Cryptography 2015 , Paris.

Conference · March 2012

Geometria delle varietà algebriche in honour of Professor A.Conte, Department of Mathematics, University of Turin.

Conference · April 2011

Participation to the *Commutative Days in Turin, a meeting in honour of Silvio Greco on the occasion of his 70th birthday*, Department of Mathematics, Polytechnic of Turin.

Conference · October 2011

Participation to the *Mathematica 5th User Group Meeting*, Department of Mathematics, University of Turin.

Teaching Experience - University courses

18.09.2017 - 16.02.2018 ·

Master Degree in Mathematics · Lecturer for the Advanced Coding Theory and Cryptography course taught on the second year of the Master Degree in Mathematics, Major in Coding Theory and Cryptography, University of Trento. Professor: M. Sala.

14.09.2015 - 12.02.2016 and 14.09.2016 - 17.02.2017 ·

Master Degree in Mathematics · Lecturer for the Algebraic Cryptography course taught on the first year of the Master Degree in Mathematics, Major in Coding Theory and Cryptography, University of Trento Professor: M. Sala.

2016

PhD in Mathematics Assistant Lecturer for the PhD course *Groebner Bases applied to Cryptography and Coding Theory*, University of Trento Professor: M. Sala.

<https://www.unitn.it/drmath/43/manifesto-studies> (see Manifesto 2015/2016)

2013–2014 ·

Bachelor in Engineering Lecturer for the Geometry course taught on the first year of the bachelor in Engineering, Politecnico di Torino. Professor: G. Casnati.

2011–2013 ·

Bachelor in Engineering Lecturer for the Geometry course taught on the first year of the bachelor in Engineering, Politecnico di Torino. Professor: 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.

November 2017

Lecturer for the course *Monero: the dark side of cryptocurrencies* Professor: M. Sala.

October 2017 ·

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

May 2017 ·

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

November 2016

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

September 2016 ·

Assistant Lecturer for the course *Bitcoin, Blockchain and their new frontiers II*, University of Trento Professor: M. Sala.

May 2016 - May 2017 ·

Assistant Lecturer for the course *Bitcoin, Blockchain and their new frontiers*, University of Trento Professor: 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

I assisted Prof. Massimiliano Sala in the preparation of the teaching material and in the organization of the two one-day face-to-face events of the EIT online course *Applications of Cryptography to Security and Privacy* and in the preparation of the teaching material for the online course *BoAB: Bitcoin and other Applications of Blockchain*. I have maintained the online platform of the latter course and done the tutoring for the participants until April 2018.

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.

Education

2011-2013 · University of Turin, Italy

PhD in Mathematics, XXVI cycle, University of Turin. · Scientific field MAT02-Algebra. PhD degree obtained on 14/02/2014 (University of Turin).

Title of PhD Thesis: *Combinatorial structure of monomial ideals*.

Description: In the thesis we study *monomial ideals* from a combinatorial point of view, mainly dealing with their Groebner escalier. Many links with coding theory and enumerative combinatorics are provided. Moreover, the code of some related software is attached to the thesis.

Developed with Professors: M.G. Marinari, T. Mora, M. Roggero.

2007-2010 · University of Turin, Italy

Master degree in Mathematics · Class: 45/S (class of Mathematics Masters of Science, D.M. 509/1999), Faculty of Mathematical, Physical and Natural Science, University of Turin Master degree obtained on 20/07/2010 with grade 110/110 cum laude and mention.

Title of MSc Thesis: *Conductor and adjoints of algebraic curves*.

Description: The thesis focuses on the several definitions of *adjoint curve*, distinguishing them and highlighting their reciprocal relationships. Additionally, a software classifying adjoint curves is developed and its pseudocode attached to the thesis, with some significant examples.

Developed with Professors: M. Roggero and P. Valabrega.

2003-2007 · University of Turin, Italy

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

Title of Bachelor Thesis: *Matroids and parking functions*.

Description: This thesis deals with graph theory and, more precisely, with the theory of *matroids*. After a theoretical overview, it gives a practical application, examining its connection with *parking functions*.

Developed with Professor M. Roggero.

Foreign languages

Italian

Mothertongue

English

Good

International English Language Testing System (Academic), got in September 2010 with 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
- Microsoft Office
- Outlook
- Thunderbird
- Internet Explorer
- Mozilla Firefox
- Chrome/Chromium
- Safari
- Adobe reader
- Opera

E-learning

- Moodle
- Sakai
- Google Classroom

Other information

Lie Algebras course

followed the Lie algebra Course held by Prof. De Graaf to the PhD School in Mathematics at University of Trento.

Researchers' night

I participated to the italian researcher's night both in Turin and in Trento.

Milano, 26/12/2019

Data

26/12/2019

Luogo

Biella