

# C.V. of Massimiliano Sala

## 1 Personal Details

- Massimiliano Sala, born in Milan (ITALY), 1969.
- Full Professor, Head of CryptoLabTN, Univ. of Trento
- e-mail `maxsalacodes@gmail.com`.

## 2 Degrees

- “Laurea in Matematica”, Univ. of Pisa, 1995.  
“The Fibrewise Homotopy Group of Simple Products of Spheres”,  
F. Bardelli (Pisa) and R. Piccinini (Newfoundland)
- Ph.D. in Mathematics, Univ. of Milan, 2001.  
“On some Algebraic Methods for Coding Theory”, C. Traverso (Pisa)

## 3 Summary

Funded research projects coordinated: 5

University courses lectured: 35

Conferences/Workshops organized: 17

Talks at formal conferences and workshops: 35

Other invited scientific talks: 31

Master’s theses supervised: 68

Ph.D. theses supervised: **15**

Ph.D. theses under supervision: 7

Papers in journals (published/accepted): 33

Papers not published yet: 15

Papers in refereed proceedings: 20

## 4 Career History

### 4.1 Overview

“BCRI” is an acronym for “Boole Centre for Research in Informatics”.

“UCC” is an acronym for “University College Cork”.

“CPR” is an acronym for “Consorzio Pisa Ricerche”

“RC” is an acronym for “Rientro dei Cervelli”, which is a special non-permanent academic position similar to a Research Professorship in UK/Ireland.

01/1996–12/1996	Junior Research Officer	Dept. of Defence
01/1997–01/2001	PhD student	Univ. of Milan
06/2001–08/2002	Senior Research Fellow	CPR (Pisa)
12/2002–02/2003	Visiting Researcher	BCRI- UCC
01/2003–09/2003	Post-doc	University of Pisa
<b>09/2003–07/2007</b>	Senior Research Fellow	BCRI- UCC
01/2007–07/2007	Visiting Professor	Univ. of Trento
07/2007–04/2008	Temporary Professor	Univ. of Trento
05/2008–10/2011	RC Professor	Univ. of Trento
11/2011–10/2015	Associate Professor	Univ. of Trento
<b>11/2015–ongoing</b>	Full Professor	Univ. of Trento

Simultaneously, I have given courses in several Universities, with positions similar to a Contract Lecturer/Professor, summarized as follows:

- Univ. of Milan-Bicocca: 2002, 2003, 2004, 2005, 2006.
- University of Milan: 2002, 2004, 2006.
- UCC: 2004.
- University of Pisa: 2005.
- University of Florence: 2006.

### 4.2 Details

01/96–12/96, **Junior Research Officer, Italian Dept. of Defence**

After a successful competition, I spent a training period in the academy of the Italian Navy. I was appointed Navy officer and my official title was “Guardiamarina con compiti di ricerca” (junior officer with research duties).

I was working in a Defence Research Centre, ‘ ‘ORMEDIFE”. I did some mathematics related work for the needs of the Department of Defence.

06/01–08/02, **Senior Research Fellow, CPR**

I was working at CPR, which is a research centre, founded by the university institutions of Pisa and large private companies, whose institutional mission is applied and industrial research.

I was in charge of carrying out an industrial research project jointly with PIAGGIO, the leading motorcycle engine manufacturer in Europe, to create an artificial intelligence system able to optimize the engine production process. I selected and hired my staff (three graduates), organized their training and subsequently led the group. The project was successfully completed and we got a 1 million euro award (50% for PIAGGIO and 50% for CPR) from the Italian Department for Research and Innovation. One of my staff was a Master's student and I was her supervisor. The thesis was successfully defended.

**12/02-02/03, Visiting Researcher, BCRI- UCC Cork**

My main duty was to pursue research in coding theory, particularly algebraic coding theory and Low Density Parity Check codes. My research work was within the group led by Prof. Patrick Fitzpatrick. I assisted the final stage of two Ph.D. theses, being part of the internal defence committee and helping finalizing both. Also, I gave some talks in the Codes seminar series.

**01/03-09/03, Post-doc Research Fellow, Univ. of Pisa**

My main duty was to pursue research in commutative algebra, computational algebra, coding theory and cryptography. As well as in their mutual interaction. My research work was within the group led by Prof. Carlo Traverso.

**09/2003-07/2007, Senior Research Fellow, BCRI- UCC Cork**

I have pursued research in commutative and computational algebra, with emphasis on applications to coding theory and cryptography, working in collaboration with Prof. P. Fitzpatrick, but also leading research on my own or together with my postgrad students.

I have a close collaboration with Dr. Marnane (Elec. Elect. Eng.) and Dr. Popovici (Microelectronics) providing mathematical support to the design of chips for efficient coding/decoding in many channels, including wireless, sensor communications, etc. .

I have been supervising several postgrad students (Master's and Ph.D.) in UCC, jointly with either Prof. Fitzpatrick or Dr. Marnane or Dr. Popovici. I have been supervising many postgrad students in Italy (Florence, Pisa, Milan, Trento) and I have arranged for most of them to spend internships with the Boole Centre and /or with large companies.

I have been involved in the organization of the BCRI Workshops in "Coding and Cryptography" (2004, 2005, 2006) and other similar activities, like the Codes seminar series, both helping in organizing the seminar schedule and giving talks when appropriate.

**01/2007-07/2007, Visiting Professor, Univ. of Trento**

I taught two courses for undergrads: "Algebraic Coding Theory" (42 hours) and "Discrete Fourier Transform" (42 hours). I have collaborated with prof. A Caranti on applications of group theory to cryptography.

07/2007--05/2008, **Temporary Professor, Univ. of Trento**

I taught two courses for undergrads: "Algebraic Coding Theory" (42 h) and "Advanced Algebraic Coding Theory" (42 h) and supervised several theses.

05/2008--10/2011, **RC Professor Univ. of Trento.**

I won a competition (or better, the university won it) and I have research funds, courses to teach and postgrads to supervise. The position expired in october 2011.

**11/2011– 10/2015, Associate Professor - Univ. of Trento.**

I have served as an Associate Professor in Algebra, with the Department of Mathematics of the University of Trento.

**11/2015– ongoing, Full Professor - Univ. of Trento.**

This is my present position.

### **Temporary Lectureships**

01/2002–10/2002, **Lecturer (Master's), Univ. of Milan-Bicocca**

I taught the course "Coding Theory and Cryptography" (30 hours) to graduate students attending a Master's programme entitled "Master in Applied and Industrial Mathematics" (ca. 20 students). I designed also the course programme and assessment method.

01/2003–10/2003, **Lecturer (Master's), Univ. of Milan-Bicocca**

Similar to the previous (30 hours). I revised the assessment method and supervised four Master's theses.

03/2005--05/2005, **Lecturer (Master's), Univ. of Milan-Bicocca**

Similar to the previous (30 hours). I also supervised one thesis.

01/2004–10/2004, **Lecturer (Master's), Univ. of Milan-Bicocca**

Similar to the previous (30 hours). I revised the assessment method and I have supervised three Master's theses.

05/2006–07/2006, **Lecturer (Master's), Univ. of Milan-Bicocca**

Similar to the previous (30 hours). Moreover, I supervised one thesis.

11/02–12/02, **Lecturer (PhD), Univ. of Milan**

I taught the course "Coding Theory" (30 hours) to Ph.D. students (ca. 10 students). I prepared a written examination plus an oral examination.

12/03–09/04, **Lecturer (PhD), Univ. of Milan**

I taught the course "Coding Theory" (45 hours) to Ph.D. students (ca. 10 students). I have assessed the students with written and oral examinations.

02/06-- 05/06, **Contract Part-time Lecturer, Univ. of Milan**

I taught a course "Symmetric Cryptography" (10 hours) to PhD students.

09/04-08/05, Lecturer (undergrad), Dept. of Math., UCC

I taught the course “Ring and Field Theory” to about 15 undergrads, mostly at their third or fourth year (Mathematics).

01/05-09/05, Lecturer (undergrad), Univ. of Pisa

I taught the course (15 hours) of “Coding Theory and Groebner bases” to undergrads, at their third/fourth/fifth year (Mathematics).

02/06-- 05/06, Lecturer(PhD), Univ. of Florence

I taught the course “Coding Theory” (30 hours) to Ph.D. students.

## 5 Teaching

### Courses that I have lectured at university level (35)

1. “Coding Theory and Cryptography”, (2002), to graduate students attending a Master’s programme entitled “Master in Applied and Industrial Mathematics” (ca. 20 students). I gave 30 lectures.
2. “Coding Theory and Cryptography”, (2003-2004-2005-2006-2007), five courses like the previous.
3. “Coding Theory”, (2002), to Ph.D. students in Milan (ca. 10 students). I gave 30 lectures.
4. “Coding Theory”, (2003-2004), to Ph.D. students in Milan (ca. 10 students). I gave 45 lectures.
5. “Ring and Field Theory”, (2004-2005), to 14 undergrads, mostly at their third or fourth year of Mathematics, UCC Cork (34 hours).
6. “Coding Theory and Groebner bases”, (2004-2005), to undergrads in Pisa. 15 hours of teaching.
7. “Symmetric Cryptography”, (2006), to Ph.D. students in Milan, 10 hours.
8. “Coding and Cryptography”, (2006), to Ph.D. students in Florence, 30 hours.
9. “Algebraic Coding Theory”, (2007), to undergrads in Trento (ca. 10 students). I gave 42 lectures.
10. “Discrete Fourier Transform”, (2007), to undergrads in Trento (3 students). I gave 42 lectures.
11. “Algebraic Coding Theory”, (2008), to undergrads in Trento (ca. 3 students). I gave 42 lectures.
12. “Advanced Coding Theory”, (2008), to postgrads in Trento (ca. 8 students). I gave 42 lectures.

13. “Algebraic Coding Theory”, (2009), to undergrads in Trento (ca. 4 students). I gave 42 lectures.
14. “Advanced Coding Theory”, (2009), to postgrads in Trento (ca. 4 students). I gave 42 lectures.
15. “Groebner bases, geometric codes and order domains”, (2009) within an international Ph.D. school in Trento (12 hours).
16. “Classical and Advanced Coding Theory”, (2009), to undergrads and postgrads in Trento (ca. 8 students). I gave 84 lectures.
17. “Block ciphers and their security”, (2010), international Ph.D. course in Trento (40 hours).
18. “Classical and Advanced Coding Theory”, (2010), to undergrads and postgrads in Trento (ca. 10 students). I gave 84 lectures.
19. “Differential Advanced Cryptanalysis”, (2010), course for postgrads in Trento (40 hours).
20. “Mathematical Evaluation of the Security of a Block Cipher”, (2011), for postgrads in Trento (40 hours).
21. “Mathematical Evaluation of the Security of Stream Ciphers”, (2011), for postgrads in Trento (40 hours).
22. “Classical and Advanced Coding Theory”, (2011), to undergrads and postgrads in Trento (ca. 15 students). I gave 84 lectures.
23. “Boolean functions and their applications to cryptography”, (2012), international Ph.D. course in Trento (40 hours).
24. “Groebner Bases, Curves, Codes and Cryptography”, (2012), international Ph.D. course taught with M. Elia, T. Mora, M. Giulietti and C. Fontanari in Trento (40 hours).
25. “Classical and Advanced Coding Theory”, (2012), to undergrads and postgrads in Trento (ca. 25 students). I gave 84 lectures.
26. “Laboratories of Applied Maths”, (2012), BSC students in Mathematics in Trento. 28 lectures and 90 students.
27. “Cryptography”, (2012), to undergrads and postgrads in Trento (ca. 35 students). I gave 42 lectures.
28. “Cryptography”, (2013), to undergrads and postgrads in Trento (ca. 35 students). I gave 42 lectures.
29. “Laboratories of Applied Maths”, (2013), BSC students in Mathematics in Trento. 28 lectures and 90 students.

30. “Advanced Coding Theory and Cryptography”, (2013), to undergrads and postgrads in Trento (ca. 15 students). I gave 42 lectures.
31. “Coding Theory and Applications”, (2013), Master’s students in Mathematics (ca. 20 students). 42 lectures
32. “Weaknesses of block ciphers: recent attacks and countermeasures”, (2013), for postgrads in Trento (40 hours).
33. “Random sources in cryptography and cryptanalysis: requirements and critical aspects”, (2013), for postgrads in Trento (40 hours).
34. “Laboratories of Applied Maths”, (2014), BSC students in Mathematics in Trento. 28 lectures and 90 students.
35. “Complexity in Cryptography”, (2014), PHD students in Trento. 10 lectures and 8 students.
36. Currently lecturing three courses at the Master’s students in Mathematics: “Coding Theory and Applications”, “Cryptography”, “Advanced Coding Theory and Cryptography”. Currently lecturing a blended course at EIT Educational “Applied Cryptography”.

### **Activities in course development**

In Trento we have a Major in Coding and Cryptography within the Master’s degree in Mathematics. Since 2008 I have been heavily involved in the organization of this Major, taking up responsibility in 2011.

We have reshaped the Major year after year, adapting the course programmes, introducing new courses to strengthen the students’ preparation and setting up more than ten internships every year for them, including several international internships. In 2014 we split the Major in two branches, according to the students’ plans for their period after their degree. One is for students interested in working as cryptographers in companies (called “stage-oriented”) and the other is for students aiming at research at a PHD level (called “research-oriented”).

## 6 Research

### 6.1 Research interests

My main research interest lies in the applications of algebra to coding theory and cryptography. In my PHD thesis I presented an approach to the study of cyclic codes, by representing its words as points in an affine variety. In the thesis this was used only to compute the distance, but later it was improved to compute the weight distribution and even the coset weight distribution. A variation to that method allowed to compute the general error locator polynomial, whose existence for any cyclic code was proved for the first time. A more developed version of our variety has been developed to solve similar problems for  $n$ -th root codes, which form a large subclass of linear codes. Some recent advances along this line resulted in the determination of multidimensional version of general error locator polynomials for any affine-variety code and hence for any linear code. Again, it is possible to adapt the multidimensional locators to determine the weight distribution and the distance. In particular, by an application of intrinsic geometrical properties of the Hermitian curves we have obtained the first-ever explicit expressions for the number of small-weight codewords in families of Hermitian codes.

Apart from the research line coming out of my PHD thesis, I have been investigating several other research areas, including: block ciphers, stream cipher, Boolean functions, S-Boxes, LDPC codes, security proofs for protocols and algorithms, attribute-based encryption, homomorphic encryption, non-linear codes, elliptic curves and other number-theoretic cryptosystems.

Finally, I want to mention that I have collaborated also with researchers from outside the academia, as summarized in Subsection 6.5, especially with large companies in need of mathematical study of codes/decoding. Several of my former students have spent internships in their research centres.



## 6.2 Talks

“Best poster prize” at the Conference “Symbolic Computational Algebra 2002”, Univ. of West. Ont. Ontario (Canada), sponsored by Ontario Res. Cent. for Comp. Alg. and Fields Institute.

### Talks outside conferences (31)

1. 2001, “Secure and safe communications, coding theory, mathematical foundations of error correction”, Appl. Math. seminar series, Dept. of Math., Univ. of Milan, Milan, ITALY.
2. 2001, “Safe communications and coding theory”, Math. seminar series, Dept. of Math. and Appl., Univ. of Milan-Bicocca, Milan, ITALY.
3. 2002, “On the syndrome variety for cyclic codes”, Commutative Algebra group seminar series, Dept. of Math., Univ. of Pisa, Pisa, ITALY.
4. 2002, “On the McEliece-Niederreiter Cryptosystem”, Appl. Math. seminar series, Dept. of Math., Univ. of Milan, Milan, ITALY.
5. 2002, “Solutions of polynomial systems on any field and Groebner bases”, Appl. Math. seminar series, UCC, Cork, IRELAND.
6. 2003, “On general error locator polynomials for cyclic codes”, School of Math. Sciences Colloquium, UCC, Cork, IRELAND.
7. 2003, “An introduction to LDPC codes”, CODES seminar series, UCC, Cork, IRELAND.
8. 2003, “On the sum-product algorithm and optimal decoding of linear codes- Part I”, CODES seminar series, UCC, Cork, IRELAND.
9. 2003, “On the sum-product algorithm and optimal decoding of linear codes- Part II”, CODES seminar series, UCC, Cork, IRELAND.
10. 2004, “Protecting data: how to get a train and arrive safe and sound”, MathSoc Seminars, UCC, Cork, IRELAND.
11. 2004, “Digital Watermarking from an Information Theory point of view”, CODES seminar series, UCC, Cork, IRELAND.
12. 2004, “Bounds on the distance of cyclic codes”, IMA Summer School in Coding and Cryptography, Univ. of Notre Dame, USA.
13. 2004, “Probabilistic algorithms for upper bounds on the distance of cyclic codes”, CODES seminar series, UCC Cork, IRELAND.
14. 2005, “A mixed ”graph theory”-algebra approach to LDPC codes”, UCD, Dublin, IRELAND.

15. 2005, “General error locator polynomials for cyclic codes”, Algebra and Geometry seminar series, Univ. of Genoa, Genoa, ITALY.
16. 2006, “The syndrome variety and decoding of cyclic codes”, seminar, Univ. of Trento, Trento, ITALY.
17. 2006, “Cyclic codes: decoding and distance bounding”, CCA seminar series, ENSTA, Paris, FRANCE.
18. 2007, “Towards a moduli space for codes.”, seminar, Univ. of Torino, Torino, ITALY.
19. 2008, “Intersections of Hermitian curves and minimum weight words” seminar, Univ. of Torino, Torino, ITALY.
20. 2008, “On Boolean functions and Groebner bases”, seminar, Univ. of Torino, Torino, ITALY.
21. 2010, “Cryptography and weak group representations”, seminar, Univ. of Torino, Torino, ITALY.
22. 2010, “An intrinsic weakness of the AES and other translation-based ciphers”, Université de Méditerranée, Marseille, FRANCE.
23. 2010, “The small weight words of some Hermitian codes”, Université de Méditerranée, Marseille, FRANCE.
24. 2010, “On Boolean function and non-linearity”, Université de Méditerranée, Marseille, FRANCE.
25. 2011, “On the provable security of some cryptographic primitives”, Univ. of Torino, Torino, ITALY.
26. 2013, “Bitcoin: the digital currency of the future”, Univ. of Verona, Verona, ITALY.
27. 2013, “On the provable security of block ciphers from their components”, Univ. of Verona, Verona, ITALY.
28. 2013, “Bitcoin: the digital currency of the future”, Univ. of Bolzano, Bolzano, ITALY.
29. 2014, “On the Hermitian curve and its intersections with some conics”, University of Messina, Messina, ITALY.
30. 2014, “A bound on the size of systematic codes”, University of Perugia, Perugia, ITALY.
31. 2014, “CryptoLabTN: some real-life projects in Cryptography”, Marche Polytechnic University, Ancona, ITALY.

### Talks given at conferences, workshops and other official events (35)

1. 2002, "Using the syndrome variety to study cyclic codes", *Workshop on Applications of Commutative Algebra*, Catania, ITALY.
2. 2003, "Bound on minimum weight codewords for BCH codes with  $d=5$ ", *BCRI Workshop on Coding and Cryptography*, Cork, IRELAND.
3. 2003, "Recent trends in coding theory" (key-note presentation), *MIRIAM Coding and Cryptography Workshop*, Univ. of Milan, ITALY.
4. 2004, "Efficient low-density parity-check decoding", *The Irish Signal and Systems Conference*, (with L. Marnane and \*R. Bresnan), Dublin, IRELAND.
5. 2005, "On a class of quasi-cyclic LDPC codes", *MEGA05, (Effective Methods in Algebraic Geometry)*, (with \*M. Rossi), Alghero, ITALY.
6. 2005, "A bound for the distance of cyclic codes which is sometimes stronger than the Roos bound", *MEGA05 (Effective Methods in Algebraic Geometry)*, (with \*E. Betti), Alghero, ITALY.
7. 2005, "On the distance of non-linear codes", *MEGA05 (Effective Methods in Algebraic Geometry)*, (with \*E. Guerrini), Alghero, ITALY.
8. 2006, "A theory for the distance of cyclic codes", *Workshop D1: Groebner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics*, Linz, AUSTRIA.
9. 2006, "Relations between bounds on the distance of cyclic codes and FGLM decoding", *Workshop D1: Groebner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics*, Linz, AUSTRIA.
10. 2006, "Symmetric Cryptography, provable security, and group theory", *Fourth International Conference on Information, joint MFCSIT06*, Cork, IRELAND.
11. 2007, "An algebraic approach to the classification of some non-linear codes", *WCC2007 (International Workshop on Coding and Cryptography)*, (with \*E. Guerrini), Paris, FRANCE.
12. 2007, "An algebraic description of Boolean functions", *WCC2007 (International Workshop on Coding and Cryptography)*, (with \*I. Simonetti), Paris, FRANCE.
13. 2007, "General error locator polynomials for  $n$ th-root codes", *WCC2007*, (with \*M. Giorgetti), Paris, FRANCE.

14. 2007, “Improved decoding of affine-variety codes”, *The Claude Shannon Workshop on Coding, Cryptography*, Cork, IRELAND.
15. 2008, “An approach to a linear approximation of the AES”, *The Claude Shannon Workshop on Coding, Cryptography*, Cork, IRELAND.
16. 2009, “Optimal binary codes with 4 codewords are linear”, *Workshop on Groebner bases and Geometric codes*, Trento, ITALY.
17. 2009, “On translation-based cryptosystems and their security”, *Workshop on block ciphers and their security*, Trento, ITALY.
18. 2011, “On the weights of affine-variety codes and some Hermitian codes”, WCC 2011 (*International Workshop on Coding and Cryptography*), (with \*C. Marcolla and \*M. Pellegrini), Paris, FRANCE.
19. 2011, “Attacks and security of systems: comparisons and conclusions” *Public key Cryptography: beyond RSA*, Univ. of Torino, Torino, ITALY.
20. 2011, “On the provable security of BEAR and LION schemes”, *The Claude Shannon Workshop on Coding, Cryptography*, Cork, IRELAND.
21. 2012, “Hand-written signature and homomorphic encryption”, *SAGA Workshop*, Trento, ITALY.
22. 2013, “Some bounds on the size of codes”, WCC 2013 (*International Workshop on Coding and Cryptography*), (with \*E. Bellini and \*E. Guerrini), Bergen, NORWAY.
23. 2013, “On the Hermitian curve and its intersections with some conics”, MEGA 2013 (*Effective Methods in Algebraic Geometry*), (with \*C. Marcolla and M. Pellegrini), Frankfurt am Main, GERMANY.
24. 2013, “Generalized AG codes as evaluation codes”, CAI 2013 (*5th International Conference on Algebraic Informatics*), (with \*M. Calderini), Porquerolles Island, FRANCE.
25. 2013, “A new bound for cyclic codes beating the Roos bound”, CAI 2013 (*5th International Conference on Algebraic Informatics*), (with \*M. Piva), Porquerolles Island, FRANCE.
26. 2014, “Boolean functions and trapdoors in block ciphers”, *International Workshop on Boolean Functions and Their Applications*, Sorendal, NORWAY.
27. 2014, “Some security bounds for the DGHV scheme”, YACC 2014 (*Yet Another Conference on Cryptography*), (with \*F. Marinelli, R. Aragona and C. Marcolla), Porquerolles Island, FRANCE.

28. 2014, “Low-Weight Common Multiples of Binary Primitive Polynomials through Discrete Logarithms”, *YACC 2014 (Yet Another Conference on Cryptography)*, (with P. Peterlongo and \*C. Tinnirello), Porquerolles I., FRANCE.
29. 2014, “Implementation and improvement of the Partial Sum Attack on 6-round AES”, *WCS 2014 (Workshop on Communication Security)*, (with \*F. Aldà, R. Aragona, L. Nicolodi), Ancona, ITALY.
30. **2015**, “A Discrete Logarithm-based Approach to Compute Low-Weight Multiples of Binary Polynomials”, *MEGA 2015 (Effective Methods in Algebraic Geometry)*, (with P. Peterlongo and \*C. Tinnirello), Trento, ITALY.
31. 2015, “Algorithmic approach using polynomial systems for the nonlinearity of Boolean functions”, *MEGA 2015 (Effective Methods in Algebraic Geometry)*, (with E. Bellini and T. Mora), Trento, ITALY.
32. 2015, “Key-Policy Multi-Authority Attribute-Based Encryption”, *CAI 2015, (6th International Conference on Algebraic Informatics)*, (with \* R. Longo and C. Marcolla), Stuttgart, GERMANY.
33. 2015, “Attacking BEAR and LION schemes in a realistic scenario”, *CAI 2015, (6th International Conference on Algebraic Informatics)*, (with M. Pizzato and M. Piva), Stuttgart, GERMANY.
34. 2015, “On differential uniformity of maps that may hide an algebraic trapdoor”, *CAI 2015, (6th International Conference on Algebraic Informatics)*, (with M. Pizzato and M. Piva), Stuttgart, GERMANY.
35. 2015, “On an algebraic trapdoor”, *XX Congresso dell’UMI*, (with R. Aragona), Siena, ITALY.

### 6.3 Other research activities

#### Organization of Conferences and Workshops (17)

I was an organizer for the following conferences:

- “BCRI Workshop on Coding and Cryptography” (2003,2004,2005,2006) Cork, IRELAND,
- “MIRIAM Coding and Cryptography Workshop” (2003) Milan, ITALY,
- “Cryptography and Computer Algebra”, workshop, (2008), Pisa, ITALY,
- “Workshop on Groebner bases and Geometric codes” (2009), Trento, ITALY,
- “Workshop on block ciphers and their security”, (2009), Trento, ITALY,
- “First Cryptography Workshop Bunny TN”, (2011), Trento, ITALY,
- “Second Cryptography Workshop Bunny TN”, (2011), Trento, ITALY,
- “Workshop on Applied Math”, (2011), Trento, ITALY.
- “Third Cryptography Workshop Bunny TN”, (2012), Trento, ITALY,
- “Fourth Cryptography Workshop Bunny TN”, (2013), Trento, ITALY,
- “Fifth Cryptography Workshop Bunny TN”, (2014), Trento, ITALY,
- “MEGA 2015 (Effective Methods in Algebraic Geometry)”, (2015), Trento, ITALY,
- “Sixth Cryptography Workshop Bunny TN”, (2015), Trento, ITALY,

I acted as main organizer for the Coding session of the following conferences:

- “Workshop D1: Groebner Bases in Cryptography, “Coding Theory, and Algebraic Combinatorics”, (2006), Linz, AUSTRIA,
- “4th International Conference on Information, joint MFCSIT06”, (2006), Cork, IRELAND.

#### Other activities

In June 2004 I served as Senior Mentor at the Institute for Mathematics and its Applications (IMA) summer graduate program in mathematics, for the Coding and Cryptography school held at the Univ. of Notre Dame (USA).

I have acted as the Managing Editor of a Springer book: “Groebner Bases, Coding and Cryptography”, published in (2009), containing 17 chapters by some leading scientists of this growing area.

## 6.4 Funded projects

I have led the research involved in the following projects:

- 2005, *Complexity issues in algebraic Coding Theory and Cryptography*, STMicroelectronics
- 2008, *Algebraic cryptography and coding*, Italian MIUR (Ministry of Education, Universities and Research)
- 2012, *Data encryption for handwritten signature verification*, Corvallis
- 2012, *Encryption for biometrics signatures*, PayBay Network
- 2013, *Homomorphic encryption*, Telsy

The total funding for the previous projects was: 311K euros.

I have also been involved in other successful project proposals, for a total of ten projects and a total amount of more than 3 millions euros.

## 6.5 Industrial research

- In 1999-2000, collaboration with **Ansaldo Segnalamento Ferroviario** on codes for railway signalling system.
- In 2001-2002, collaboration with **Piaggio** on optimization of engine production planning.
- In 2003-2007, collaboration with **STMicroelectronics** on codes/cryptography.
- In 2008-2009, collaboration with **Easycardservices** and **Safepay** on money transfer via Internet.
- In 2009-2010, collaboration with **IDT** on codes for hard-disks.

In 2010-2012:

- collaboration with **SGS - Banco Popolare** on security assesment of ciphers.
- collaboration with **iTwin** on security assesment of ciphers.

In 2011-ongoing, short courses for companies in cryptography and cryptanalysis.

In 2010-2012 collaboration with **Telsy** on cryptography.

In 2012-2013:

- collaboration with **Corvallis Infracom** on handwritten signature verification.
- collaboration with **PayBay Networks** on an authentication model based on biometric signatures.
- collaboration with **Poste Italiane and PayBay Networks** on security issues in TITAN, a new advanced e-payment system.
- collaboration with **IKS** on an innovative project for transaction signing in online banking.

In 2013-2014:

- collaboration with **Consorzio Bancomat** on interbank cryptography.
- collaboration with **AliasLab** on cryptography for on-line banking.
- collaboration with **Banco Popolare** on mobile banking.

**Previous non-academic consultancy work**

In 1997-2000, network programming for Internet providers. In 1998, teaching of courses for large Italian companies: “Java Programming”, “Designing WWW services”, “Internet Security”. In 1999, teaching of an IFOA course (Milan): “C programming”. In 1997-2002, designing security policies for internet providers.



## 6.6 Research supervision

Master's theses supervised<sup>1</sup> (68):

1. Lucia Berardi, Dept. of Math., Univ. of Milan-Bicocca, 2001,  
*Some applications of neural networks*
2. \* Leonarda Mangieri, Dept. of Math., Univ. of Milan-Bicocca, 2003,  
*Implementations of coding-decoding procedures for a Number Theory family of Space-Time codes*
3. \* Francesca Villani, Dept. of Math., Univ. of Milan-Bicocca, 2003,  
*Modes of Operation for a Block Cipher*
4. Marta Giorgetti, Dept. of Math., Univ. of Milan-Bicocca, 2003,  
*An investigation of LDPC decoding for Goppa codes*
5. Jennifer Manginelli, Dept. of Math., Univ. of Milan-Bicocca, 2003,  
*An investigation of LDPC decoding for Goppa codes*
6. Richard Bresnan, Dept. of Elec. Eng., UCC Cork, 2004,  
*Novel code construction and decoding techniques for LDPC codes*
7. Marta Rossi, Dept. of Math., Univ. of Milan-Bicocca, 2004,  
*Construction of quasi-cyclic LDPC codes*
8. \* Emanuela Orsini, Dept. of Math., Univ. of Milan-Bicocca, 2004,  
*Metodi algebrici per la costruzione di matrici di parit per LDPCC*
9. \* Simone Nava, Dept. of Math., Univ. of Milan-Bicocca, 2004,  
*Metodi algebrici per la costruzione di matrici di parit per LDPCC*
10. Emanuele Betti, Dept. of Math., Univ. of Pisa, 2005,  
*Un'interpretazione algebrica della distanza dei codici ciclici*
11. \* Anna Rimoldi, Dept. of Math., Univ. of Milan-Bicocca, 2005,  
*Coppersmith's algorithm with Fitzpatrick's techniques*
12. Eleonora Guerrini, Dept. of Math., Univ. of Pisa, 2005,  
*Distanza e ottimalit in codici non lineari*
13. \* Ilaria Simonetti, Dept. of Math., Univ. of Milan-Bicocca, 2005,  
*Crittosistemi polinomiali*
14. James McDonagh, Dept. of Microelectronics, UCC Cork, 2006,  
*LDPC Codes Using Quasi-Cyclic Encoding*
15. Tony O'Halloran, Dept. of Microelectronics, UCC Cork, 2006,  
*Forward Error Correction techniques for use in Wireless Sensor Network*

---

<sup>1</sup>The symbol "\*" denotes an internship period in a company.

16. \* Paola Stagliano, Dept. of Math., Univ. of Milan-Bicocca, 2006,  
*Sistemi crittografici ed il problema della fattorizzazione*
17. Valeria Bodrone, Dept. of Math., Univ. of Torino, 2007,  
*Basi di Groebner e codici correttori*
18. Chiara Marcolla, Dept. of Math., Univ. of Trento, 2009,  
*Parole di peso piccolo dei Codici Hermitiani*
19. Lara Maines, Dept. of Math., Univ. of Trento, 2009,  
*Una debole rappresentazione del gruppo simmetrico*
20. Marco Pizzato, Dept. of Math., Univ. of Trento, 2009.  
*The Jacobian Conjecture*
21. \* Marco Frego, Dept. of Math., Univ. of Trento, 2010.  
*Probabilit'errore in decodifica e bound relativi*
22. \* Matteo Piva, Dept. of Math., Univ. of Trento, 2010,  
*Decoding error probability with a new bound*
23. \* Daniele Giovannini, Dept. of Math., Univ. of Trento, 2011,  
*A mathematical overview of modern Stream Ciphers*
24. \* Valentina Pulice, Dept. of Math., Univ. of Trento, 2011,  
*A Security Classification of Boolean Functions*
25. \* Stefano Martin, Dept. of Math., Univ. of Trento, 2011,  
*Construction and evaluation of Block Ciphers*
26. Stefania Vanzetti, Dept. of Math., Univ. of Torino, 2011.  
*Attacchi ai sistemi crittografici basati sul logaritmo discreto: il caso delle curve iperellittiche*
27. Alberto Ravagnani, Dept. of Math., Univ. of Trento, 2012.  
*On Goppa Codes on the Hermitian Curve*
28. \* Chiara Pellegrini, Dept. of Math., Univ. of Trento, 2012.  
*Signature Verification Algorithms and Algebraic Homomorphic Encryption*
29. \* Giada Sciarretta, Dept. of Math., Univ. of Trento, 2012.  
*Biometric Signature Protection and Decoding Algorithm Analysis*
30. \* Valentina Da Rold, Dept. of Math., Univ. of Trento, 2012.  
*Biometric Signature Protection with Channel Analysis*
31. Martina Curto, Dept. of Math., Univ. of Trento, 2013.  
*Intersections between Hermitian Curve and Parabolas. Their Application to Hermitian Codes*
32. \* Daniel Pinter, Dept. of Math., Univ. of Trento, 2013.  
*Cryptographic Application of Number Theory to Online Banking*

33. Francesco Aldá, Dept. of Math., Univ. of Trento, 2013.  
*The Partial Sum Attack on 6-round reduced AES: Implementation and improvement*
34. \* Alessio Meneghetti, Dept. of Math., Univ. of Trento, 2013.  
*Algebraic post-processing and non-binary entropy extractors*
35. Nadir Cordioli, Dept. of Math., Univ. of Trento, 2013.  
*Euclidean Algorithm and Fitzpatrick's Algorithm: A Comparison Beyond Distance*
36. \* Simona Dimase, Dept. of Math., Univ. of Trento, 2014.  
*Cryptanalysis of GSM stream ciphers*
37. \* Beatrice Ridolfi, Dept. of Math., Univ. of Trento, 2014.  
*Cryptanalysis of Bluetooth stream cipher*
38. Daniele Maccauro, Dept. of Math., Univ. of Perugia, 2014.  
*On some algebraic properties of Boolean functions*
39. Cecilia Boschini, Dept. of Math., Univ. of Trento, 2014.  
*NTWO: a post quantum cipher*
40. Aaron Gaio, Dept. of Math., Univ. of Trento, 2014.  
*Some Teaching Experience in Computational Algebra*
41. \* Francesco Gozzini, Dept. of Math., Univ. of Trento, 2014.  
*RLWE-based Somewhat Homomorphic Encryption, with an application to the Symmetric Searchable Encryption problem*
42. \* Franca Marinelli, Dept. of Math., Univ. of Trento, 2014.  
*Somewhat Homomorphic Encryption with some security bounds*
43. Federico Giacon, Dept. of Math., Univ. of Padova, 2014.  
*Revising RS-ABE, an encryption scheme for user revocation and attribute-based access*
44. \* Riccardo Longo, Dept. of Math., Univ. of Trento, 2014.  
*Attribute Based Encryption with Algebraic Methods*
45. \* Giulia Traverso, Dept. of Math., Univ. of Trento, 2014.  
*On some modern applications of cryptography*
46. \* Giulia Perina, Dept. of Math., Univ. of Trento, 2014.  
*Cryptographic algorithms for the iPhone*
47. \* Ambra Valenti, Dept. of Math., Univ. of Trento, 2014.  
*Algebraic generation of pseudorandom numbers*
48. \* Giulia Benedetti, Dept. of Math., Univ. of Trento, 2014.  
*Algebraic weakness of the Dual Elliptic Curve PRNG*

49. \* Piera Galber, Dept. of Math., Univ. of Trento, 2014.  
*Algebraic coding in Blue-ray technology*
50. \* Gloria Massera, Dept. of Math., Univ. of Trento, 2015.  
*LDPC Codes in Quantum Key distribution*
51. \* Marco Iavernaro, Dept. of Math., Univ. of Trento, 2015.  
*On some cryptographic properties of vectorial Boolean functions*
52. Irene Villa, Dept. of Math., Univ. of Trento, 2015.  
*On Boolean functions in even dimension*
53. \* Marco Martinoli, Dept. of Math., Univ. of Trento, 2015.  
*Glitch propagation model and cryptography*
54. \* Lucia Berardi, Dept. of Math., Univ. of Trento, 2015.  
*Cryptographic properties of PGP*
55. \* Roberta Barbi, Dept. of Math., Univ. of Trento, 2015.  
*Polynomial interpolation over finite fields and applications to list decoding of Reed-Solomon codes*
56. \* Pasqua Valentina Mauri, Dept. of Math., Univ. of Trento, 2016.  
*PKI and IBE: authentication method and algebraic background*
57. \* Francesco De Vito, Dept. of Math., Univ. of Trento, 2016.  
*An application of Edwards elliptic curves to Ripple protocol*
58. \* Marta Salvaterra, Dept. of Math., Univ. of Trento, 2016.  
*On Bitcoin and the security of ECDSA digital signature*
59. \* Valentina Calzavara, Dept. of Math., Univ. of Trento, 2016.  
*Cryptographic significance of key wrapping*
60. \* Andrea Zanini, Dept. of Math., Univ. of Trento, 2016.  
*On Message Authentication Codes and related mathematical problems*
61. \* Patrick Harasser, Dept. of Math., Univ. of Trento, 2016.  
*Cover Attacks on Hyperelliptic Curve Cryptography*
62. \* Silvia Berlanda, Dept. of Math., Univ. of Trento, 2016.  
*Cryptographic protection for shared processed data on an untrusted platform*

63. \* Roberto Roscino, Dept. of Math., Univ. of Trento, 2016.  
*XMSST A post-quantum signature for the QKDS public channel authentication*
64. \* Alessandro Amadori, Dept. of Math., Univ. of Trento, 2016.  
*On summation polynomial for elliptic curves*
65. \* Carlo Brunetta, Dept. of Math., Univ. of Trento, 2016.  
*On some computational aspects for hidden sums in Boolean functions*
66. \* Alessandro Budroni, Dept. of Math., Univ. of Trento, 2017.  
*Hash maps in pairing-based cryptography*
67. \* Manni Sara, Dept. of Math., Univ. of Trento, 2017.  
*Symmetric authentication methods for entities: a proof of security for NKerberos*
68. \* Iliaria Zappatore, Dept. of Math., Univ. of Trento, 2017.  
*Primitivity of generalized translation based block ciphers*

**Ph.D. theses** under supervision, Dept. of Math., Univ. of Trento, (7):

- Riccardo Longo,
- Roberto Civino,
- Matteo Bonini,
- Giordano Santilli,
- Augustine Musukwa,
- Daniele Taufer,
- Carla Mascia.

**Ph.D. theses** already supervised (15):

- Marta Giorgetti, Dept. of Math., Univ. of Milan, 2007,  
*“On some algebraic interpretations of classical codes”*
- Emanuela Orsini, Dept. of Math., Univ. of Milan, 2008,  
*“On the decoding and distance problems for algebraic codes”*
- Christian Spagnol, Dept. of Elec. Eng., UCC Cork, 2008,  
*“Aspects of LDPC codes for hardware implementation”*
- Ilaria Simonetti, Dept. of Math., Univ. of Milan, 2009,  
*“On some applications of commutative algebra to  
Boolean functions and their non-linearity”*
- Eleonora Guerrini, Dept. of Math., Univ. of Trento, 2009,  
*“Systematic codes and polynomial ideals”*
- Anna Rimoldi, Dept. of Math., Univ. of Trento, 2009,  
*“On algebraic and statistical properties of AES-like ciphers”*
- Chiara Marcolla, Dept. of Math., Univ. of Trento, 2013,  
*“On structure and decoding of Hermitian codes”*
- Matteo Piva, Dept. of Math., Univ. of Trento, 2014.  
*“Algebraic methods for the distance of cyclic codes”*
- Martino Borello, Dept. of Math., Univ. of Milan-Bicocca, 2014,  
*“Automorphism groups of self-dual binary linear codes”*
- Emanuele Bellini, Dept. of Math., Univ. of Trento, 2015,  
*“Computational techniques for nonlinear codes and Boolean functions”*
- Marco Calderini, Dept. of Math., Univ. of Trento, 2015,  
*“On Boolean functions, symmetric cryptography and algebraic  
coding theory”*
- Federico Pintore, Dept. of Math., Univ. of Trento, 2015,  
*“Binary quadratic forms, elliptic curves and Schoof’s algorithm”*
- Claudia Tinnirello, Dept. of Math., Univ. of Trento, 2016,  
*Cyclic codes: Low-Weight Codewords and Locators*
- Marco Pellegrini, Dept. of Math., Univ. of Florence, 2016,  
*On the Weight Distribution of Hermitian Codes*
- Alessio Meneghetti, Dept. of Math., Univ. of Trento, 2017,  
*Optimal Codes and Entropy Extractors*

## 6.7 Publications

I will use a “\*” to identify an author as one of my (former) students.

### Articles published or accepted (Journals) (33)

1. “A linear programming estimate of the weight distribution of BCH(255,k)”, *IEEE Transactions on Information Theory*, 2000, vol. 46, p. 2235–2237 (with A. Tamponi).
2. “Groebner bases and distance of cyclic codes”, *Applicable Algebra in Engineering, Communication and Computing*, 2002, vol. 13, p. 137–162.
3. “Upper bounds on the dual distance of BCH(255,k)”, *Design, Codes and Cryptography*, 2003, vol. 30, p. 159–168.
4. “On the Gröbner bases of some symmetric systems and their application to coding theory”, *Journal of Symbolic Computation*, 2003, vol. 35, p. 177–194 (with T. Mora).
5. “Correcting errors and erasures via the syndrome variety”, *Journal of Pure and Applied Algebra*, 2005, vol. 200, p. 191–226 (with \*E. Orsini).
6. “On the Groebner basis of a family of quasi-cyclic LDPC codes”, *Bulletin of the Iranian Mathematical Society*, 2005, vol. 31, p. 13–32, (with \*M. Giorgetti, \*M. Rossi).
7. “A new bound for the minimum distance of a cyclic code from its defining set”, *IEEE Transactions on Information Theory*, 2006, vol. 52, p. 3700–3706 (with \*E. Betti).
8. “General error locator polynomials for binary cyclic codes with  $t \leq 2$  and  $n < 63$ ”, *IEEE Transactions on Information Theory*, 2007, vol. 53, p. 1095–1107 (with \*E. Orsini).
9. “Abelian regular subgroups of the affine group and radical rings”, *Publicationes Mathematicae Debrecen*, 2006, vol. 69, p. 297–308 (with A. Caranti, F. Dalla Volta).
10. “Groebner basis techniques to compute weight distributions of shortened cyclic codes”, *Journal of Algebra and its Applications*, 2007, vol. 6, p. 403–414.
11. “Error Resilient Data Transport in Sensor Network Applications: A Generic Perspective”, *International Journal of Circuit Theory and Applications*, 2009, vol. 37, p. 377–396 (with R. Agarwal, E. Popovici, B. O’Flynn).

12. "Computing the distance distribution of systematic non-linear codes", *Journal of Algebra and its Applications*, 2010, vol. 9, p. 241–256, (with \*E. Guerrini, \*E. Orsini).
13. "On some block ciphers and imprimitive groups", *Applicable Algebra in Engineering, Communication and Computing*, 2009, vol. 20, p. 339–350 (with A. Caranti, F. Dalla Volta).
14. "A commutative algebra approach to linear codes", *Journal of Algebra*, 2009, vol. 321, no. 8, p. 2259–2286 (with \*M. Giorgetti).
15. "An application of the O’Nan-Scott theorem to the group generated by the round functions of an AES-like cipher", *Design, Codes and Cryptography*, 2009, vol. 52, p. 293–301 (with A. Caranti, F. Dalla Volta).
16. "On the provable security of BEAR and LION schemes", *Applicable Algebra in Engineering, Communication and Computing*, 2011, vol. 22, p. 413–423 (with \*L. Maines, \*M. Piva, \*A. Rimoldi).
17. "On weakly APN functions and 4-bit S-Boxes", *Finite Fields and their Applications*, 2012, vol. 18, p. 522–528 (with C. Fontanari, \*V. Pulice, \*A. Rimoldi).
18. "Improved decoding of affine-variety codes", *Journal of Pure and Applied Algebra*, 2012, vol. 216, pp. 1533–1565 (with \*E. Orsini, \*C. Marcolla).
19. "Postulation of general quintuple fat point schemes in  $P^3$ ", *Journal of Algebra*, 2012, vol. 363, p. 113–139 (with E. Ballico, M. C. Brambilla, F. Caruso).
20. "On the evaluation of multivariate polynomials over finite fields", *Journal of Symbolic Computation*, 2013, vol. 50, p. 255–262 (with E. Ballico, M. Elia).
21. "On the group generated by the round functions of translation based ciphers over arbitrary finite fields", *Finite Fields and their Applications*, 2014, vol. 25, p. 293–305 (with R. Aragona, A. Caranti, F. Dalla Volta).
22. "Some Bounds on the Size of Codes", *IEEE Transactions on Information Theory*, 2014, vol. 60, p. 1475–1480 (with E. Guerrini, \*E. Bellini).
23. "On the Hermitian curve and its intersections with some conics", *Finite Fields and their Applications*, 2014, vol. 28, p. 166–187 (with \*C. Marcolla, \*M. Pellegrini).
24. "Some security bounds for the key sizes of DGHV scheme", *Applicable Algebra in Engineering, Communication and Computing*, 2014, vol. 25, pp. 383–392 (with \*F. Marinelli, R. Aragona, C. Marcolla)



25. “On the small weights codewords of some Hermitian codes”,  
*Journal of Symbolic Computation*, 2016, vol. 73, p. 27–45  
(with \*C. Marcolla, \*M. Pellegrini).
26. “The group generated by the round functions of a GOST-like cipher”,  
*Annali di Matematica Pura e Applicata*, 2017, vol. 196, p. 1–17 (2017)  
(with R. Aragona, A. Caranti).
27. “A Discrete Logarithm-based Approach to Compute Low-Weight Multiples of Binary Polynomials”, *Finite Fields and their Applications*, 2016, vol. 38, p. 57–71 (with \*C. Tinnirello, P. Peterlongo).
28. “On weak differential uniformity of vectorial Boolean functions as a cryptographic criterion”,  
*Applicable Algebra in Engineering, Communication and Computing*, 2016, vol. 27, p. 359–372 (with R. Aragona, \*M. Calderini, \*D. Maccauro)
29. “On optimal nonlinear systematic codes”,  
*IEEE Transactions on Information Theory*, 2016, vol. 62, p. 3103–3112  
(with E. Guerrini, \*A. Meneghetti)
30. “Several proofs of security for a tokenization algorithm”,  
*Applicable Algebra in Engineering, Communication and Computing*, 2017, *to appear* (with R. Aragona, \*R. Longo) AAEECC.
31. “On the shape of the general error locator polynomial for cyclic codes”,  
*IEEE Transactions on Information Theory*, 2017, *to appear*  
(with F. Caruso, E. Orsini, \*C. Tinnirello)
32. “A note on APN permutations in even dimension”  
*Finite Fields and Their Applications*, 2017, vol. 46, p. 1–16  
(with M. Calderini and \*I. Villa).
33. “A note on an infeasible linearization of some block ciphers”,  
*Journal of Discrete Mathematical Sciences and Cryptography*, 2017, *to appear* (with R. Aragona and A. Rimoldi).

**Articles published (refereed Conference Proceedings) (20)**

1. “Efficient low-density parity-check decoding”,  
*Proc. of The Irish Signal and Systems Conference 2004*, 2004, p. 613–618  
(with L. Marnane and \*R. Bresnan).
2. “Symmetric Cryptography, provable security, and group theory”,  
*Proc. of International Conference on Information and MFCST06*, 2006, p. 279–282.
3. “An algebraic description of Boolean functions”,  
*Proc. of Int. Workshop on Coding and Cryptography 2007, WCC2007*, p. 343–349 (with \*I. Simonetti).

4. “An algebraic approach to the classification of some non-linear codes”,  
*Proc. of Int. Workshop on Coding and Cryptography 2007, WCC2007*,  
p. 177–185 (with \*E. Guerrini).
5. “General error locator polynomials for nth-root codes”,  
*Proc. of Int. Workshop on Coding and Cryptography 2007, WCC2007*,  
p. 167–176 (with \*M. Giorgetti).
6. “Low Cost Error Recovery in Delay-Intolerant Wireless Sensor Networks”,  
*Proc. of ECCTD*, 2007, p. 699–702, DOI: 10.1109/ECCTD.2007.4529692  
(with R. Agarwal, E. Popovici, B. O’Flynn).
7. “Efficient Construction and Implementation of Short LDPC Codes for  
Wireless Sensor Networks”,  
*Proc. of ECCTD*, 2007, p. 703–706, DOI: 10.1109/ECCTD.2007.4529693  
(with \*J. McDonagh, E. Popovici, \*A. O’Hallmhair, V. Katewa).
8. “On the weights of affine-variety codes and some Hermitian codes”, *Proc.  
of Int. Workshop on Coding and Cryptography 2011, WCC2011*,  
p. 273–282 (with \*C. Marcolla, \*M. Pellegrini).
9. “Some bounds on the size of codes”,  
*Proc. of Int. Workshop on Coding and Cryptography 2013, WCC2013*,  
p. 158–166 (with \*E. Bellini, \*E. Guerrini).
10. “Generalized AG codes as evaluation codes”,  
CAI2013, *Springer LNCS*, 2013, vol. 8080, p. 74–82 (with \*M. Calderini).
11. “A new bound for cyclic codes beating the Roos bound”,  
CAI2013, *Springer LNCS*, 2013, vol. 8080, p. 101–112 (with \*M. Piva).
12. “Some security bounds for the DGHV scheme”,  
*Proc. of YACC2014*, p. 10  
(with \*F. Marinelli, R. Aragona and C. Marcolla),
13. “Low-Weight Common Multiples of Binary Primitive Polynomials through  
Discrete Logarithms”,  
*Proc. of YACC2014*, p. 10, (with P. Peterlongo and \*C. Tinnirello).
14. “Implementation and improvement of the Partial Sum Attack on 6-round AES”,  
WCS2014, *Springer LNEE*, 2015, vol. 358, p. 181–195  
(with \*F. Alda, R. Aragona and L. Nicolodi).
15. “A Real Life Project in Cryptography: Assessment of RSA Keys”,  
WCS2014, *Springer LNEE*, 2015, vol. 358, p. 197–203  
(with R. Aragona and \*F. Gozzini).
16. ”Encoding in the DTMF channel for two-channel authentication”  
WCS2014, *Springer LNEE*, 2015, vol. 358, p. 205–212  
(with \*A. Meneghetti, P. Peterlongo).

17. “Geometric features for hand-written signatures”,  
*Springer Proc. Math. Stat.*, 2014, vol. 84, p. 117–134  
(with \*C. Pellegrini, A. Rimoldi).
18. “Key-Policy Multi-Authority Attribute-Based Encryption”,  
CAI2015, *Springer LNCS*, 2015, vol. 9270, p. 152–164  
(with \*R. Longo, C. Marcolla).
19. “Attacking BEAR and LION schemes in a realistic scenario”,  
CAI2015, *Springer LNCS*, 2015, vol. 9270, p. 189–195  
(with M. Pizzato, M. Piva).
20. “On differential uniformity of maps that may hide an algebraic trapdoor”,  
CAI2015, *Springer LNCS*, 2015, vol. 9270, p. 70–78  
(with \*M. Calderini).

**Preprints not yet published (15)**

1. arXiv:1011.2644  
”Do AES encryptions act randomly?” (with A. Rimoldi and E. Bertolazzi).
2. arXiv:1411.7681  
”The role of Boolean functions in hiding sums as trapdoors for some block ciphers” (with R. Aragona and \*M. Calderini).
3. arXiv:1006.5894,  
”A possible intrinsic weakness of AES and other cryptosystems”  
(with \*A. Rimoldi and I. Toli).
4. arXiv:0906.3410,  
”Quasi-cyclic LDPC codes with high girth”  
(with \*C. Spagnol and \*M. Rossi).
5. arXiv:0806.1763,  
”Permutation equivalent maximal irreducible Goppa codes”  
(with F. Dalla Volta and \*M. Giorgetti).
6. BCRI - UCC preprint no. 57,  
”A classification of MDS binary systematic codes”  
(with \*E. Guerrini).
7. BCRI - UCC preprint no. 60,  
”M-Channel Paraunitary Multirate Filter Bank Factorisation over Fields of Characteristic Two” (with M. Lucey and C. C. Murphy).
8. BCRI - UCC preprint no. 7,  
”A lower bound on the distance of cyclic codes” (with F. Ponchio).
9. BCRI - UCC preprint no. 62,  
”A theory for distance bounding cyclic codes” (with \*E. Betti).

10. BCRI - UCC preprint no. 48,  
“An approach to create coprime polynomial pairs”  
(\*A. Rimoldi and P. Fragneto).
11. arXiv:1404.2741  
“Nonlinearity of Boolean functions: an algorithmic approach based on multivariate polynomials” (with \*E. Bellini and I. Simonetti).
12. arXiv:1505.00542  
“A deterministic algorithm for the distance and weight distribution of binary nonlinear codes” (with \*E. Bellini).
13. arXiv:1502.01494  
“Code generator matrices as entropy extractors”  
(with A. Tomasi and \*A. Meneghetti).
14. <https://eprint.iacr.org/2016/262>,  
“Collaborative Multi-Authority Key-Policy Attribute-Based Encryption for Shorter Keys and Parameters” (with C. Marcolla and R. \*Longo).
15. arXiv:1603.06635  
“A proof of security for a key-policy RS-ABE scheme”  
(with \*F. Giacon and R. Aragona).

I am also preparing two text-books:

- “Coding Theory and Cryptography: an Algebraic Introduction”, from my notes on postgrad courses on this subject.
- “Groebner bases, affine-variety codes and order domains”.

## 7 Administration

I have served in the Managing Board of the Master’s programme “MAMI”, which was annually held in the Dept. of Math. of the Univ. of Milan-Bicocca (<http://www.matapp.unimib.it/russo/mami/#organizzazione>). I have contributed to develop the curricula for this programme, in particular proposing new courses and assessing the industrial interest of others.

I have directed the Laboratory of Industrial Mathematics and Cryptography in the Dept. of Math. of the Univ. of Trento since 2010. With 2 secretaries, four postdocs and about 5 PHD students every year, plus about 10 Master’s thesis annually, it is a rather engaging activity.