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: 20

University courses lectured: 59
Conferences/Workshops organized: 22
Talks at formal conferences and workshops: 40
Other invited scientific talks: 35

Master's theses supervised: 75
Ph.D. theses supervised: **17**
Ph.D. theses under supervision: 5

Papers in journals (published/accepted): 40
Papers not published yet: 14
Papers in refereed proceedings: 25

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
09/2003–07/2007	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
11/2015–ongoing	Full Professor	Univ. of Trento

Simultanously, 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 Transfom" (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 had research funds, courses to lecture 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. I founded the Laboratory of Cryptography and I took responsability for internships and placement of all Mathematics students (BSC and MSC).

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

This is my present position. I have continued to head the Laboratory of Cryptography and to have responsability for internships and placement.
I am also serving as delegate of the Department for the relationship with private companies and private-funded research.

Temporary Lectureships

- University of Milan-Bicocca
  01/2002-10/2002, Lecturer (Master's)
  01/2003-10/2003, Lecturer (Master's)
  I also supervised four Master's theses.
  03/2005--05/2005, Lecturer (Master's)
  I also supervised one thesis.
  01/2004-10/2004, Lecturer (Master's)
  I also supervised three Master's theses.
  05/2006-07/2006, Lecturer (Master's)
  Moreover, I supervised one thesis.

- University of Milan
  11/02-12/02, Lecturer (PhD)
  12/03-09/04, Lecturer (PhD)
  02/06-- 05/06, Contract Part-time Lecturer (PhD)

- others
  09/04-08/05, Lecturer (BSC), University College Cork.
  01/05-09/05, Lecturer (BSC), University of Pisa.
  02/06-- 05/06, Lecturer(PhD), University of Florence.

5 Academic Lecturing

Courses that I have lectured at university level (59)

1. "Coding Theory and Cryptography", Univ. of Milano-Bicocca (2002),
   MSC students in "Applied and Industrial Mathematics"
   (ca 30 lectures and 20 students).

2. "Coding Theory", Univ. of Milan (2002),
   Ph.D. students in Mathematics (ca 30 lectures and ca 10 students).

3. "Coding Theory and Cryptography", Univ. of Milano-Bicocca (2003),
   MSC students in "Applied and Industrial Mathematics"
   (ca 30 lectures and 20 students).

4. "Coding Theory", Univ. of Milan (2003-2004),
   Ph.D. students in Mathematics (ca 40 lectures and ca 10 students).

5. "Coding Theory and Cryptography", Univ. of Milano-Bicocca (2004),
   MSC students in "Applied and Industrial Mathematics"
   (ca 30 lectures and 20 students).

6. "Ring and Field Theory", Univ. College Cork UCC (2004-2005),
   BSC and MSC students in Mathematics (ca 30 lectures).

7. "Coding Theory and Groebner bases", Univ. of Pisa (2004-2005),
   BSC students in Mathematics (ca 15 lectures).

8. "Coding Theory and Cryptography", Univ. of Milano-Bicocca (2005),
   MSC students in "Applied and Industrial Mathematics"
   (ca 30 lectures and 20 students).

9. "Coding Theory and Cryptography", Univ. of Milano-Bicocca (2006),
   MSC students in "Applied and Industrial Mathematics"
   (ca 30 lectures and 20 students).

10. "Symmetric Cryptography", Univ. of Milan (2006),
    Ph.D. students in Mathematics (ca 10 lectures).

11. "Coding and Cryptography", Univ. of Florence (2006),
    Ph.D. students in Mathematics (ca 30 lectures).

12. "Coding Theory and Cryptography", Univ. of Milano-Bicocca (2007),
    MSC students in "Applied and Industrial Mathematics"
    (ca 30 lectures and 20 students).

13. "Algebraic Coding Theory", Univ. of Trento (2007),
    BSC students in Mathematics (ca 40 lectures and ca 10 students).

14. “Discrete Fourier Transform”, Univ. of Trento (2007),
BSC students in Mathematics (ca 40 lectures).

15. “Algebraic Coding Theory”, Univ. of Trento (2008),
BSC students in Mathematics (ca 40 lectures).

16. “Advanced Coding Theory”, Univ. of Trento (2008),
MSC students in Mathematics (ca 40 lectures and ca 10 students).

17. “Algebraic Coding Theory”, Univ. of Trento (2009),
BSC students in Mathematics (ca 40 lectures).

18. “Advanced Coding Theory”, Univ. of Trento (2009),
MSC students in Mathematics (ca 40 lectures).

19. “Groebner bases, geometric codes and order domains”,
Univ of Trento (2009),
within an international Ph.D. school (ca 10 lectures).

20. “Classical and Advanced Coding Theory”, Univ. of Trento (2009),
BSC and MSC students in Maths (ca 80 lectures and ca 10 students).

21. “Block ciphers and their security”, Univ. of Trento (2010),
international Ph.D. course (ca 40 lectures).

22. “Classical and Advanced Coding Theory”, Univ. of Trento (2010),
BSC and MSC students in Maths (ca 80 lectures and ca 10 students).

23. “Differential Advanced Cryptanalysis”,
Univ. of Trento (2010), (ca 40 lectures).
MSC graduates in Matematics, Computer Science and Engineering.

24. “Mathematical Evaluation of the Security of a Block Cipher”,
Univ. of Trento (2011), (ca 40 lectures).
MSC graduates in Matematics, Computer Science and Engineering.

25. “Mathematical Evaluation of the Security of Stream Ciphers”,
Univ. of Trento (2011), (ca 40 lectures).
MSC graduates in Matematics, Computer Science and Engineering.

26. “Classical and Advanced Coding Theory”, Univ. of Trento (2011),
BSC and MSC students in Maths. (ca 80 lectures and ca 20 students).

27. “Boolean functions and their applications to cryptography”, (2012)
Univ. of Trento, international Ph.D. course in Trento (ca 40 lectures).

28. “Groebner Bases, Curves, Codes and Cryptography”,
Univ. of Trento (2012), international Ph.D. course, jointly held with
M. Elia, T. Mora, M. Giulietti and C. Fontanari.

29. “Classical and Advanced Coding Theory”, Univ. of Trento (2012),
BSC and MSC students in Maths (ca 80 lectures and ca 30 students).

30. “Laboratories of Applied Maths”, Univ. of Trento (2012),
BSC students in Mathematics (ca 30 lectures and 90 students).

31. “Cryptography”, Univ. of Trento (2012),
BSC and MSC students in Maths (ca 40 lectures and ca 35 students).

32. “Cryptography”, Univ. of Trento (2013),
BSC and MSC students in Maths (ca 40 lectures and ca 35 students).

33. “Laboratories of Applied Maths”, Univ. of Trento (2013),
BSC students in Mathematics (ca 30 lectures and 90 students).

34. “Advanced Coding Theory and Cryptography”, Univ. of Trento (2013),
MSC students in Mathematics (ca 40 lectures and ca 15 students).

35. “Coding Theory and Applications”, UNiv. of Trento (2013),
MSC students in Mathematics (ca 40 lectures and ca 20 students).

36. “Weaknesses of block ciphers: recent attacks and countermeasures”,
Univ. of Trento (2013), (ca 40 lectures).
MSC graduates in Matematics, Computer Science and Engineering.

37. “Random sources in cryptography and cryptanalysis: requirements and
critical aspects”, Univ. of Trento (2013), (ca 40 lectures).
MSC graduates in Matematics, Computer Science and Engineering.

38. “Laboratories of Applied Maths”, Univ. of Trento (2014),
BSC students in Mathematics (ca 30 lectures and 90 students).

39. “ Complexity in Cryptography”, Univ. of Trento (2014),
PHD students in Mathematics (ca 10 lectures and 10 students).

40. “Advanced Coding Theory and Cryptography”, Univ. of Trento (2014),
MSC students in Mathematics (ca 40 lectures and 15 students).

41. “Coding Theory and Applications”, Univ. of Trento (2014),
MSC students in Mathematics (ca 40 lectures and ca 20 students).

42. “Cryptography”, Univ. of Trento (2014),
MSC students in Mathematics and in Computer Science
(ca 40 lectures and 40 students).

43. ”Applied Cryptography”, EIT Educational, Trento node (2014),
MSC graduates in Matematics, Computer Science and Engineering.

44. “Advanced Coding Theory and Cryptography”, Univ. of Trento (2015),
MSC students in Mathematics (ca 40 lectures and 10 students).

45. “Coding Theory and Applications”, Univ. of Trento (2015),
MSC students in Mathematics (ca 40 lectures and 20 students).

46. “Cryptography”, Univ. of Trento (2015),
MSC students in Mathematics and in Computer Science
(ca 40 lectures and 40 students).

47. “Finite Field and Symmetric Cryptography”, Univ. of Trento (2015),
MSC students in Mathematics (ca 40 lectures and 20 students).

48. ”Mathematical trapdoors in block ciphers: evaluation and attack exploitation”,
Univ. of Trento (2015), (ca 40 lectures).
MSC graduates in Matematics, Computer Science and Engineering.

49. “Advanced Coding Theory and Cryptography”, Univ. of Trento (2016),
MSC students in Mathematics (ca 40 lectures and 10 students).

50. “Coding Theory and Applications”, Univ. of Trento (2016),
MSC students in Mathematics (ca 40 lectures and 20 students).

51. “Cryptography”, Univ. of Trento (2016),
MSC students in Mathematics and in Computer Science
(ca 40 lectures and 30 students).

52. “Finite Field and Symmetric Cryptography”, Univ. of Trento (2016),
MSC students in Mathematics (ca 40 lectures and 20 students).

53. “Cryptography for Telephone Transmissions: video calling”,
Univ. of Trento (2016), (ca 40 lectures).
MSC graduates in Matematics, Computer Science and Engineering.

54. “Advanced Analysis of Block Ciphers”,
Univ. of Trento (2016), (ca 40 lectures).
MSC graduates in Matematics, Computer Science and Engineering.

55. “Advanced Coding Theory and Cryptography”, Univ. of Trento (2017),
MSC students in Mathematics (ca 40 lectures and 10 students).

56. “Coding Theory and Applications”, Univ. of Trento (2017),
MSC students in Mathematics (ca 40 lectures and 20 students).

57. “Cryptography”, Univ. of Trento (2017),
MSC students in Mathematics and in Computer Science
(ca 40 lectures and 30 students).

58. “Finite Field and Symmetric Cryptography”, Univ. of Trento (2017),
MSC students in Mathematics (ca 40 lectures and 20 students).

59. “Finite Field and Symmetric Cryptography”, Univ. of Trento (2018),
MSC students in Mathematics (ca 40 lectures and 20 students).

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.

Since 2012 I have investigated the new fascinating world of cryptocurrencies and blockchain technology. In this context, I'm especially interested in providing security proofs for protocols that can be built with blockchain technology, but I'm also interested in clever choices for the primitives, so that they can guarantee for example anonimity.

One of the problems that I find fascinating is the design of block ciphers that can be proved to be secure w.r.t. some notions. This curiosity led me to research their components, in particular S-Boxes as vectorial Boolean functions, and allowed me to investigate the subtle game of inserting trapdoors/backdoors in the ciphers thorugh a careful choice of the components. This line of research has brought interesting results and also allowed a new form of cryptanalitic attack.

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 (35)

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 Mediterranée, Marseille, FRANCE.

23. 2010, “The small weight words of some Hermitian codes”, Université de Mediterranée, Marseille, FRANCE.

24. 2010, “On Boolean function and non-linearity”, Université de Mediterranée, 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.

32. 2017, "A Security Proof of a Tokenization Algorithm", GSSI, L'Aquila, ITALY.

33. 2017, "Monero: the dark side of cryptocurrencies", University of Genova, Genova, ITALY.

34. 2017, "Cryptographic primitives and their properties", University of Perugia, Perugia, ITALY.

35. 2017, "Blockchain technology and its applications", University of Salerno, Salerno, ITALY.

Talks given at conferences, workshops and other official events (40)

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 nth-root codes", `WCC2007`,
(International Workshop on Coding and Cryptography),
(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.

36. **2017**, "Differential Attacks: Using Alternative Operations, `WCC 2017` *(International Workshop on Coding and Cryptography)*, (with C. Blondeau, R. Civino), Saint-Petersburg, RUSSIA.

37. 2017, "Hidden sums and their application on block ciphers, `WCC 2017` *(International Workshop on Coding and Cryptography)*, (with C. Brunetta, M. Calderini), Saint-Petersburg, RUSSIA.

38. 2017, "Collaborative Multi-Authority Key-Policy Attribute-Based Encryption for Shorter Keys and Parameters", `CAI 2017`, *(7th International Conference on Algebraic Informatics)*, (with R. Longo, C. Marcolla), Kalamata, GREECE.

39. 2017, "Blockchain to protect individual rights", *(Blockchain for Social Good)*, Torino, ITALY.

40. **2018**, "Security proofs for some protocols based on blockchain technology", `DLT 2017`, *(1st Distributed Ledger Technology Workshop)*, (with A. Meneghetti), Perugia, ITALY.

6.3 Other research activities

Organization of Conferences and Workshops (22)

1. "BCRI Workshop on Coding and Cryptography" (2003), Cork, IRELAND.
2. "MIRIAM Coding and Cryptography Workshop" (2003), Milan, ITALY,
3. "BCRI Workshop on Coding and Cryptography" (2004), Cork, IRELAND.
4. "BCRI Workshop on Coding and Cryptography" (2005), Cork, IRELAND.
5. "Workshop D1: Groebner Bases in Cryptography, "Coding Theory, and Algebraic Combinatorics" (2006), Linz, AUSTRIA,
6. "Coding Session at the 4th International Conference on Information, joint MFCSIT06" (2006), Cork, IRELAND.
7. "BCRI Workshop on Coding and Cryptography" (2006), Cork, IRELAND.
8. "Workshop in Cryptography and Computer Algebra" (2008), Pisa, ITALY,
9. "Workshop on Groebner bases and Geometric codes" (2009), Trento, ITALY,
10. "Workshop on block ciphers and their security" (2009), Trento, ITALY,
11. "First Cryptography Workshop BunnyTN" (2011), Trento, ITALY,
12. "Second Cryptography Workshop BunnyTN" (2011), Trento, ITALY,
13. " Workshop on Applied Mathematics" (2011), Trento, ITALY.
14. "Third Cryptography Workshop BunnyTN" (2012), Trento, ITALY,
15. "Fourth Cryptography Workshop BunnyTN" (2013), Trento, ITALY,
16. "Fifth Cryptography Workshop BunnyTN" (2014), Trento, ITALY,
17. "MEGA 2015 (Effective Methods in Algebraic Geometry)" (2015), Trento, ITALY,
18. "Sixth Cryptography Workshop Bunny TN" (2015), Trento, ITALY,
19. "Seventh Cryptography Workshop BunnyTN" (2016), Trento, ITALY,
20. `WTSC2017` "1st Workshop on Trusted Smart Contracts", in collaboration with *Financial Cryptography and Data Security 2017*, Malta, MALTA.
21. `WTSC2018` "2nd Workshop on Trusted Smart Contracts", in collaboration with *Financial Cryptography and Data Security 2018*, Santa Barbara, CURACAO.
22. "Special session on Post-Quantum Cryptography", in collaboration with `ITASEC2018`, Milan, ITALY.

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 milions 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 `STMicrolectronics` 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 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[1] (75):

1. Lucia Berardi, Dept. of Math., Univ. of Milan-Bicocca, 2001,
   Some applications of neural networs

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. * Emmanuela Orsini, Dept. of Math., Univ. of Milan-Bicocca, 2004,
   Metodi algebrici per la costruzione di matrici di parità per LDPCC

9. * Simone Nava, Dept. of Math., Univ. of Milan-Bicocca, 2004,
   Metodi algebrici per la costruzione di matrici di parità per LDPCC

10. Emanuele Betti, Dept. of Math., Univ. of Pisa, 2005,
    Uninterpretazione 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 ottimalità 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

[1] The symbol "*" denotes an internship period in a company.

15. Tony O'Halloran, Dept. of Microelectronics, UCC Cork, 2006,
Forward Error Correction techniques for use in Wireless Sensor Network

16. * Paola Staglianò, 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 crittograci 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 Aldà, 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 Fitzpatricks 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 Brentegani, 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 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. * Ilaria Zappatore, Dept. of Math., Univ. of Trento, 2017.
Primitivity of generalized translation based block ciphers

69. * Giuseppe Giffone, Dept. of Math., Univ. of Trento, 2017.
Analysis of a revocation-storage attribute-based encryption

70. Marco Zaninelli, Dept. of Math., Univ. of Trento, 2017.
On cryptographic properties of Boolean functions

71. * Nicolò Fornari, Dept. of Math., Univ. of Trento, 2017.
Cryptography in the white-box attack model: some constructions and attacks

72. * Alessandro Melloni, Dept. of Math., Univ. of Trento, 2017.
A description of the Peercoin protocol

73. * Cristian Mirto, Dept. of Math., Univ. of Trento, 2017.
The Levenshtein theorem on optimal codes

74. Nicoletta Alfarano Gianira, Dept. of Math., Univ. of Trento, 2017.
The diffusion property of some mixing-layer

75. * Armanda Ottaviano Quintavalle, Dept. of Math., Univ. of Trento, 2018.
Algebraic methods for quantum codes

Ph.D. theses already supervised (17):

1. Marta Giorgetti, Dept. of Math., Univ. of Milan, 2007,
   On some algebraic interpretations of classical codes

2. Emmanuela Orsini, Dept. of Math., Univ. of Milan, 2008,
   On the decoding and distance problems for algebraic codes

3. Christian Spagnol, Dept. of Elec. Eng., UCC Cork, 2008,
   Aspects of LDPC codes for hardware implementation

4. Ilaria Simonetti, Dept. of Math., Univ. of Milan, 2009,
   On some applications of commutative algebra to Boolean functions and their non-linearity

5. Eleonora Guerrini, Dept. of Math., Univ. of Trento, 2009,
   Systematic codes and polynomial ideals

6. Anna Rimoldi, Dept. of Math., Univ. of Trento, 2009,
   On algebraic and statistical properties of AES-like ciphers

7. Chiara Marcolla, Dept. of Math., Univ. of Trento, 2013,
   On structure and decoding of Hermitian codes

8. Matteo Piva, Dept. of Math., Univ. of Trento, 2014.
   Algebraic methods for the distance of cyclic codes

9. Martino Borello, Dept. of Math., Univ. of Milan-Bicocca, 2014,
   Automorphism groups of self-dual binary linear codes

10. Emanuele Bellini, Dept. of Math., Univ. of Trento, 2015,
    Computational techniques for nonlinear codes and Boolean functions

11. Marco Calderini, Dept. of Math., Univ. of Trento, 2015,
    On Boolean functions, symmetric cryptography and algebraic coding theory

12. Federico Pintore, Dept. of Math., Univ. of Trento, 2015,
    Binary quadratic forms, elliptic curves and Schoof's algorithm

13. Claudia Tinnirello, Dept. of Math., Univ. of Trento, 2016,
    Cyclic codes: low-Weight cdewords and locators

14. Marco Pellegrini, Dept. of Math., Univ. of Florence, 2016,
    On the weight distribution of Hermitian codes

15. Alessio Meneghetti, Dept. of Math., Univ. of Trento, 2017,
    Optimal codes and entropy extractors

16. Riccardo Longo, Dept. of Math., Univ. of Trento, 2018,
Formal proofs of security for privacy-preserving blockchains and other cryptographic protocols

17. Roberto Civino, Dept. of Math., Univ. of Trento, 2018,
Differential attacks using alternative operations and block cipher design

Ph.D. theses under supervision, Dept. of Math., Univ. of Trento (**5**):

- Matteo Bonini,
- Giordano Santilli,
- Augustine Musukwa,
- Daniele Taufer,
- Carla Mascia.

6.7 Publications

I will use a "*" to identify an author as one of my students who contributed to the research described in the paper.

Articles published or accepted (Journals) (**40**)

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. "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).

9. "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).

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. “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).

13. “A commutative algebra approach to linear codes”, *Journal of Algebra*, 2009, vol. 321, no. 8, p. 2259–2286 (with *M. Giorgetti).

14. ”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).

15. “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).

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 P3”, *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. "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).

27. "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)

28. "On optimal nonlinear systematic codes",
IEEE Transactions on Information Theory, 2016, vol. 62, p. 3103–3112
(with E. Guerrini, *A. Meneghetti)

29. "Generation of high quality random numbers via an all-silicon-based approach",
Physica Status Solidi (A) Applications and Materials Science, 2016,
vol. 213, p. 3186–3193
(with *A. Meneghetti, A. Tomasi et al.)

30. "The group generated by the round functions of a GOST-like cipher",
Annali di Matematica Pura e Applicata, 2017, vol. 196, p. 1–17
(with R. Aragona, A. Caranti).

31. "Several proofs of security for a tokenization algorithm",
Applicable Algebra in Engineering, Communication and Computing, 2017, vol. 28, p. 425–436 (with R. Aragona, *R. Longo).

32. "On the shape of the general error locator polynomial for cyclic codes",
IEEE Transactions on Information Theory, 2017, vol. 63, p. 3641–3657
(with F. Caruso, E. Orsini, *C. Tinnirello)

33. "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).

34. "Code generator matrices as RNG conditioners",
Finite Fields and their Applications, 2017
vol. 47, p. 46–63 (with A. Tomasi and *A. Meneghetti).

35. "A note on an infeasible linearization of some block ciphers",
Journal of Discrete Mathematical Sciences and Cryptography, 2018,
p. 1–10, *to appear* (with R. Aragona and A. Rimoldi).

36. "On the discrete logarithm problem for prime-field elliptic curves",
Finite Fields and their Applications, 2018
vol. 51, p. 168–182 (with *A. Amadori and F. Pintore).

37. "Hilbert quasi-polynomials for order domains and applications to coding theory",
Advances in Mathematics of Communications, 2018,
p. 1–15, *to appear* (with *C. Mascia and G. Rinaldo).

38. "A proof of security for a key-policy RS-ABE scheme",
JP Journal of Algebra, Number Theory and Applications, 2018,
vol. 40, p. 29–90 (with *F. Giacon, R. Aragona).

39. "A deterministic algorithm for the distance and weight distribution of binary nonlinear codes",
International Journal of Information and Coding Theory, 2018, *to appear* (with *E. Bellini).

40. "On Hidden Sums Compatible with A Given Block Cipher Diffusion Layer",
Discrete Mathematics, 2018, *to appear* (with M. Calderini).

Articles published (*refereed* Conference Proceedings) (25)

1. "Efficient low-density parity-check decoding",
Proc. of The Irish Signal and Systems Conference 2004, 2004, vol. 506,
p. 613–618 (with L. Marnane and *R. Bresnan).

2. "Symmetric Cryptography, provable security, and group theory",
Proc. of International Conference on Information and MFCSIT06, 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,
(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
(with *J. McDonagh, E. Popovici, *A. O'Hallmhurain, 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. 77-81 (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*, 2016, 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*, 2016, vol. 358, p. 197–203 (with R. Aragona and *F. Gozzini).

16. "Encoding in the DTMF channel for two-channel authentication" WCS2014, *Springer LNEE*, 2016, 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).

21. “A post-processing free Si nanocrystals based quantum random number generator”,
EQEC2015, 2015 (with *A. Meneghetti, A. Tomasi et al.).

22. “Differential Attacks: Using Alternative Operations”,
Proc. of Int. Workshop on Coding and Cryptography 2017, *WCC2017*, 2017
p. 12 (with C. Blondeau, *R. Civino)

23. “Hidden sums and their application on block ciphers”,
Proc. of Int. Workshop on Coding and Cryptography 2017, *WCC2017*, 2017
p. 12 (with *C. Brunetta, M. Calderini).

24. “Collaborative Multi-Authority Key-Policy Attribute-Based Encryption for Shorter Keys and Parameters”,
CAI2017, 2017, p. 67–67 (with *R. Longo, C. Marcolla).

25. “On the security of blockchain BIX protocol and certificates”,
CyCon 2017, *IEEE*, 2017, p. 217–232
(with F. Pintore, *R. Longo, G. Rinaldo).

Preprints not yet published (14)

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. 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).

13. arXiv:1708.08814
    "Wave-Shaped Round Functions and Primitive Groups", (with R. Aragona, M. Calderini, R. Civino, *I. Zappatore).

14. arXiv:1702.00581
    "Elementary abelian regular subgroups as hidden sums for cryptographic trapdoors", (with *M. Calderini)

7 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.
- I have acted as an Editor of a Springer LNCS book: "WTSC17", published in 2017, containing the proeccedings for the workshop WTSC17, that I chaired.
- I am acting as an Editor of a Springer LNCS book: "WTSC18", to be published in 2018, containing the proeccedings for the workshop WTSC18, that I chaired.
- 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, reshaping the Major year after year, adapting the course programmes, introducing new courses and setting up more than ten internships per year. 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").
- 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 been heading the Laboratory of Industrial Mathematics and Cryptography in the Dept. of Math. of the Univ. of Trento since 2010. In the Laboratory there work four colleagues, two secretaries, up to six postdocs and 5 PHD students.
- I am preparing a text-book: "Coding Theory and Cryptography: an Algebraic Introduction", from my notes on postgrad courses on this subject.
- I am preparing a text-book: "Groebner bases, affine-variety codes and order domains", from my notes on postgrad courses on this subject.