Curriculum Vitae

Personal Details

Massimiliano Sala, born in Milan (ITALY), 1969.
e-mail: *maxsalacodes@gmail.com*

Full Professor, Head of CryptoLabTN, University of Trento
Acting Director, national initiative De Componendis Cifris

Degrees

1995 - Laurea in Matematica - University of Pisa
The Fibrewise Homotopy Group of Simple Products of Spheres,

2001 - Ph.D. in Mathematics - University of Milan
On some Algebraic Methods for Coding Theory

Summary of academic activities

Editor of **three** international journals, **two** Special Issues, **five** Proceedings

Papers in journals: **54**
Papers in refereed proceedings: **27**
Unpublished preprints: **17**

University courses lectured: **61**

Master's theses supervised: **103**
Ph.D. theses supervised: **22**

Organization of scientific conferences and workshops: **27**

Talks at formal conferences and workshops: **41**
Other invited scientific talks: **36**

Summary of dissemination and outreach activity

Research projects: **35** (of which 31 involving private companies)

International patents: **two** granted **EU patents** and **one** pending **US patent**

Courses for professionals: **28**

Dissemination papers: **13**

Dissemination conferences and workshops: **24**

Interviews with newspapers and other media: **12**

Challenges, Hackathons and nationwide initiatives for students: **5**

Curriculum Vitae

Career

Main academic positions:

- 2001-2002
  Senior Research Fellow, **Consorzio Pisa Ricerche**, Pisa
- 2002-2003
  Visiting Researcher, **BCRI- University College Cork**, Cork
- 2003,
  Assegnista di ricerca (post-doc), **University of Pisa**, Pisa
- 2003–2006
  Senior Research Fellow, **BCRI- University College Cork**, Cork
- 2007-2011
  Research Professor, **University of Trento**, Trento
- 2011-2015
  Associate Professor, **University of Trento**, Trento
- 2015 – ongoing
  Full Professor, **University of Trento**, Trento

Positions related to the UNITN community

- 2010 -- ongoing
  Head of the **Laboratory of Cryptography (CryptoLabTN)**
- 2013 -- 2015
  Member of "**Giunta del Dipartimento di Matematica**"
- 2010 -- 2019
  "**Delegato per gli stage, tirocini e placement", Dept. of Mathematics**
- 2016 -- 2017
  "**Consigliere d'amministrazione della start up di ateneo Intellegit**"
- 2017 -- ongoing
  Advisory of study of "curriculum Cryptography" of MSC in Mathematics

Other positions

- 2017 -- ongoing
  Acting Director, **national initiative De Componendis Cifris,** www.decifris.it
- 2019 -- ongoing
  President of the Crypto Board, **Quadrans Foundation**, Switzerland

---

Curriculum Vitae

Research interests

My main research interest lies in the applications of algebra to coding theory and cryptography.

Efficient decoding of cyclic codes

In my PHD thesis I presented an approach to the study of cyclic codes, by representing its words as points in an affine variety. This method permits to compute the distance, the weight distribution and even the coset weight distribution. A variation to that method can compute the general error locator polynomial, whose existence for any cyclic code was proved for the first time. Improved versions of our approach have solved similar problems for n-th root codes and for affine-variety codes. Similarly, 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.

Design of block ciphers

A fascinating problem 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 and backdoors in the ciphers through a careful choice of the components.

Algebraic cryptanalysis

Cryptanalysis is interesting for me because by attacking a cipher often vulnerabilities can be found and then patched. It is a way of increasing the security of a cryptographic protocol, if done publicly in the community. We claim results both in symmetric and in asymmetric cryptography.

Others

I have been investigating several other research areas, including: computational algebra, group theory, finite fields, LDPC codes, non-linear codes, random number generators, stream ciphers, security proofs for protocols and algorithms, attribute-based encryption, homomorphic encryption, elliptic curves and other number-theoretic cryptosystems. Since 2012 I have also worked in cryptocurrencies and blockchain technology, with the goal of providing security proofs for protocols that can be built with blockchain technology, starting from a suitable choice of the underlying primitives.
Finally, I want to mention that I have often collaborated also with researchers outside academia and that I'm keen on studying problems coming from real-world applications. This has led to **31** research projects developed together with companies. This intense collaboration has also naturally extended to preparing and teaching **28** specific advanced courses (where state-of-art research results are presented) with an audience of company personnel and professionals.

Curriculum Vitae

Editorial Activity

Journals

I'm an editor of the following international academic journals

- **Applicable Algebra in Engineering, Communication and Computing**
- **Advances in Mathematics of Communications**
- **Mediterranean Journal of Mathematics**

Special Issues

I've been an editor of the following Special Issues of journals:

- 2020 - coeditors: A. Meneghetti, S. Mesnager
  The Cryptography of Cryptocurrency,
  Mathematics
- 2019 - coeditors: A. Tansel et al.
  Next General Blockchain Architecture, Infrastructure and Applications,
  Annals of Emerging Technologies in Computing (AETiC)

Proceedings books

I've been an editor of the following Proceedings books:

1. 2009, coeditors: T. Mora, L. Perret, S. Sakata, C. Traverso
   Gröbner bases, coding, and cryptography,
   Springer RISC book series
2. 2017, coeditors: M. Brenner, A. Miller et al.
   Financial Cryptography and Data Security (FC 2017) International Workshops Springer LNCS 10323
3. 2018, coeditors: J. Clark, V. Teague et al.
   Financial Cryptography and Data Security (FC 2018) International Workshops Springer LNCS 10958
4. 2019 - coeditors: A. Bracciali, J. Clark et al .
   Financial Cryptography and Data Security (FC 2019) International Workshops Springer LNCS 11599
5. 2020 - coeditors: M. Bernhard. S. Matsu
   Financial Cryptography and Data Security (FC 2020) International Workshops Springer LNCS 12063

Curriculum Vitae

Academic Publications

Journal Papers:	**54**			
Conference Papers:	**27**			
Unpublished preprints:	**17**			
Scopus h-index:	**10**	--	Scopus citations:	**345**
G. Scholar h-index:	**15**	--	G Scholar citations:	**820**

Selected Publications

Decoding of cyclic codes

- 2005 - coauthor: E. Orsini,
  Correcting errors and erasures via the syndrome variety,
  Journal of Pure and Applied Algebra, vol. 200, p. 191--226.
- 2017 - coauthors: F. Caruso, E. Orsini, C. Tinnirello
  On the shape of the general error locator polynomial for cyclic codes,
  IEEE Transactions on Information Theory, vol. 63, p. 3641--3657.

Design of block ciphers

- 2014 - coauthors: R. Aragona, A. Caranti, F. Dalla Volta
  On the group generated by the round functions of translation based ciphers over arbitrary finite fields,
  Finite Fields and their Applications, vol. 25, p. 293--305.
- 2017 - coauthors: R. Aragona, A. Caranti
  The group generated by the round functions of a GOST-like cipher,
  Annali di Matematica Pura e Applicata, vol. 196, p. 1--17.

Algebraic cryptanalysis

- 2018 - coauthors: A. Amadori, F. Pintore
  On the discrete logarithm problem for prime-field elliptic curves,
  Finite Fields and their Applications, vol. 51, p. 168--182.
- 2019 - coauthors: C. Blondeau, R. Civino
  Differential attacks: using alternative operations,
  Designs, Codes, and Cryptography, vol. 87, p. 225--247.
- 2020 - coauthors: D. Sogiorno, D. Taufer
  A small subgroup attack on Bitcoin address generation,
  Mathematics, vol. 8, art. 1645.

Curriculum Vitae

Journal Papers (54)

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

Curriculum Vitae

---

12. 2009 - coauthors: A. Caranti, F. Dalla Volta
    On some block ciphers and imprimitive groups,
    Applicable Algebra in Engineering, Communication and Computing, vol. 20, p. 339--350.
13. 2009 - coauthor: M. Giorgetti
    A commutative algebra approach to linear codes,
    Journal of Algebra, vol. 321, no. 8, p. 2259--2286.
14. 2009 - coauthors: A. Caranti, F. Dalla Volta
    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, vol. 52, p. 293--301.
15. 2010 - coauthors: E. Guerrini, E. Orsini
    Computing the distance distribution of systematic non-linear codes,
    Journal of Algebra and its Applications, 2010, vol. 9, p. 241--256.
16. 2011 - coauthors: L. Maines, M. Piva, A. Rimoldi
    On the provable security of BEAR and LION schemes,
    Applicable Algebra in Engineering, Communication and Computing, vol. 22, p. 413--423.
17. 2012 - coauthors: C. Fontanari, V. Pulice, A. Rimoldi
    On weakly APN functions and 4-bit S-Boxes,
    Finite Fields and their Applications, vol. 18, p. 522--528.
18. 2012 - coauthors: E. Orsini, C. Marcolla
    Improved decoding of affine-variety codes,
    Journal of Pure and Applied Algebra, vol. 216, p. 1533--1565.
19. 2012 - coauthors: E. Ballico, M. C. Brambilla, F. Caruso
    Postulation of general quintuple fat point schemes in P3,
    Journal of Algebra, vol. 363, p. 113--139.
20. 2013 - coauthors: E. Ballico, M. Elia
    On the evaluation of multivariate polynomials over finite fields,
    Journal of Symbolic Computation, vol. 50, p. 255--262.
21. 2014 - coauthors: R. Aragona, A. Caranti, F. Dalla Volta
    On the group generated by the round functions of translation based ciphers over arbitrary finite fields,
    Finite Fields and their Applications, vol. 25, p. 293--305.
22. 2014 - coauthors:,E. Bellini, E. Guerrini
    Some Bounds on the Size of Codes,
    IEEE Transactions on Information Theory, vol. 60, p. 1475--1480.

Curriculum Vitae

---

23. 2014 - coauthors: C. Marcolla, M. Pellegrini
    On the Hermitian curve and its intersections with some conics,
    Finite Fields and their Applications, vol. 28, p. 166--187.
24. 2014 - coauthors: R. Aragona, C. Marcolla, F. Marinelli
    Some security bounds for the key sizes of DGHV scheme,
    Applicable Algebra in Engineering, Communication and Computing, vol. 25, p.383--392.
25. 2016 - coauthors: C. Marcolla, M. Pellegrini
    On the small weights codewords of some Hermitian codes,
    Journal of Symbolic Computation, vol. 73, p. 27--45.
26. 2016 - coauthors: P. Peterlongo, C. Tinnirello
    A discrete logarithm-based approach to compute low-weight multiples of binary polynomials,
    Finite Fields and their Applications, vol. 38, p. 57--71.
27. 2016 - coauthors: R. Aragona, M. Calderini, D. Maccauro
    On weak differential uniformity of vectorial Boolean functions as a cryptographic criterion,
    Applicable Algebra in Engineering, Communication and Computing, vol. 27, p. 359--372.
28. 2016 - coauthors: E. Guerrini, A. Meneghetti
    On optimal nonlinear systematic codes,
    IEEE Transactions on Information Theory, vol. 62, p. 3103--3112.
29. 2016 - coauthors: A. Meneghetti, A. Tomasi et al
    Generation of high quality random numbers via an all-silicon-based approach,
    Physica Status Solidi (A) Applications and Materials Science, vol. 213, p. 3186--3193.
30. 2017 - coauthors: R. Aragona, A. Caranti
    The group generated by the round functions of a GOST-like cipher,
    Annali di Matematica Pura e Applicata, vol. 196, p. 1--17.
31. 2017 - coauthors: R. Aragona, R. Longo
    Several proofs of security for a tokenization algorithm,
    Applicable Algebra in Engineering, Communication and Computing, vol. 28, p. 425--436.
32. 2017 - coauthors: M. Calderini, I. Villa
    A note on APN permutations in even dimension,
    Finite Fields and Their Applications, vol. 46, p. 1--16.
33. 2017 - coauthors: A. Meneghetti, A. Tomasi
    Code generator matrices as RNG conditioners,
    Finite Fields and their Applications, vol. 47, p. 46--63.
34. 2017 - coauthors: F. Caruso, E. Orsini, C. Tinnirello
    On the shape of the general error locator polynomial for cyclic codes,
    IEEE Transactions on Information Theory, vol. 63, p. 3641--3657.

Curriculum Vitae

35. 2018 - coauthors: R. Aragona, A. Rimoldi
    A note on an infeasible linearization of some block ciphers,
    Journal of Discrete Mathematical Sciences and Cryptography, Vol. 21, p. 209--218.
36. 2018 - coauthors: A. Amadori, F. Pintore
    On the discrete logarithm problem for prime-field elliptic curves,
    Finite Fields and their Applications, vol. 51, p. 168--182.
37. 2018 - coauthors: C. Mascia, G. Rinaldo
    Hilbert quasi-polynomials for order domains and applications to coding theory,
    Advances in Mathematics of Communications, vol. 12, p. 287--301.
38. 2018 - coauthors: R. Aragona, F. Giacon
    A proof of security for a key-policy RS-ABE scheme,
    JP Journal of Algebra, Number Theory and Applications, vol. 40, p. 29--90.
39. 2018 - coauthor: E. Bellini
    A deterministic algorithm for the distance and weight distribution of binary nonlinear codes,
    International Journal of Information and Coding Theory, vol. 5, p. 18--35.
40. 2019 - coauthor: M. Calderini
    On Hidden Sums Compatible with A Given Block Cipher Diffusion Layer,
    Discrete Mathematics, vol. 342, p. 373--386.
41. 2019 - coauthors: R. Aragona, M. Calderini, R. Civino, I. Zappatore
    Wave-shaped round functions and primitive groups,
    Advances in Mathematics of Communications, vol. 13, p. 67--88.
42. 2019 - coauthors: A. Meneghetti, A.O. Quintavalle, A. Tomasi
    Two-tier blockchain timestamped notarization with incremental security,
    Annals of Emerging Technologies in Computing, vol. 3, p. 25--33.
43. 2019 - coauthor: M. Pellegrini
    Weight distribution of Hermitian codes and matrices rank,
    Finite Fields and their Applications, vol. 60, art. 101578.
44. 2019 - coauthors: A. Meneghetti, T. Parise, D. Taufer
    A survey on efficient parallelization of blockchain-based smart contracts,
    Annals of Emerging Technologies in Computing, vol. 3, p. 9--16.
45. 2019 - coauthors: C. Blondeau, R. Civino
    Differential attacks: using alternative operations,
    Designs, Codes, and Cryptography, vol. 87, p. 225--247.
46. 2019 - coauthors: C. Brunetta, M. Calderini
    On hidden sums compatible with a given block cipher diffusion layer,
    Discrete Mathematics, vol. 342, p. 373--386.

Curriculum Vitae

---

47. 2020 - coauthors: M. Ceria, T. Mora
    Zech tableaux as tools for sparse decoding,
    Rendiconti Sem. Mat. Univ. Pol. Torino, vol. 78, p. 43 -- 56.

48. 2020 - coauthor: M. Bonini
    Intersections between the norm-trace curve and some low degree curves,
    Finite Fields and their Applications, vol. 67, art. 101715.

49. 2020 - coauthors: D. Sogiorno, D. Taufer
    A small subgroup attack on Bitcoin address generation,
    Mathematics, vol. 8, art. 1645.

50. 2020 - coauthor: A. Musukwa
    On the linear structures of balanced functions and quadratic APN functions,
    Cryptography and Communications, vol. 12, p. 859--880.

51. 2020 - coauthors: M. Ceria, T. Mora
    HELP: a sparse error locator polynomial for BCH codes,
    Applicable Algebra in Engineering, Communications and Computing, vol. 31, p. 215-233.

52. 2020 - coauthors: A. Meneghetti, D. Taufer
    A new ECDLP-based PoW model,
    Mathematics, vol. 8, art. 1344.

53. 2020 - coauthors: A. Meneghetti, D. Taufer
    A survey on PoW-based consensus,
    Annals of Emerging Technologies in Computing, vol. 4, p. 8--18.

54. 2020 - coauthors: R. Civino, M. Calderini
    On properties of translation groups in the affine general linear group with applications to cryptography,
    Journal of Algebra. accepted for publication,
    DOI: 10.1016/j.jalgebra.2020.10.034

Curriculum Vitae

Conference papers (27)

1. 2004 - Coauthors: R. Bresnan, L. Marnane
   Efficient low-density parity-check decoding,
   Proc. of The Irish Signal and Systems Conference, vol. 506, p. 613--618.
2. 2006,
   Symmetric Cryptography, provable security, and group theory,
   Proc. of Int. Conference on Information and MFCSIT06, p. 279--282.
3. 2007 - Coauthor: I. Simonetti
   An algebraic description of Boolean functions,
   Proc. of Int. Workshop on Coding and Cryptography (WCC2007), p. 343--349.
4. 2007 - coauthor: E. Guerrini
   An algebraic approach to the classification of some non-linear codes,
   Proc. of Int. Workshop on Coding and Cryptography (WCC2007), p. 177--185.
5. 2007 - coauthor: M. Giorgetti
   General error locator polynomials for nth-root codes,
   Proc. of Int. Workshop on Coding and Cryptography (WCC2007), p. 167--176.
6. 2007 - coauthors: R. Agarwal, B. O'Flynn, E. M. Popovici
   Low Cost Error Recovery in Delay-Intolerant Wireless Sensor Networks,
   Proc. of ECCTD2007, p. 699--702.
7. 2007 - coauthors: J. McDonagh, A. O'Hallmhurain, V. Katewa, E. M. Popovici
   Efficient Construction and Implementation of Short LDPC Codes for Wireless Sensor Networks,
   Proc. of ECCTD2007, p. 703--706.
8. 2011 - coauthors: C. Marcolla, M. Pellegrini
   On the weights of affine-variety codes and some Hermitian codes,
   Proc. of Int. Workshop on Coding and Cryptography (WCC2011), p. 273--282.
9. 2013 - coauthors: E. Bellini, E. Guerrini
   Some bounds on the size of codes,
   Proc. of Int. Workshop on Coding and Cryptography (WCC2013), p. 158--166.
10. 2013 - coauthor: M. Piva
    A new bound for cyclic codes beating the Roos bound,
    Proc. of CAI2013, Springer LNCS, vol. 8080, p. 101--112.
11. 2013 - coauthor: M. Calderini
    Generalized AG codes as evaluation codes,
    Proc. of CAI2013 - Springer LNCS, vol. 8080, p. 74--82.

Curriculum Vitae

---

12. 2014 - coauthors: R. Aragona, C. Marcolla, F. Marinelli
    Some security bounds for the DGHV scheme,
    Proc. of YACC2014, p. 77--81.
13. 2014 - coauthors: P. Peterlongo, C. Tinnirello
    Low-Weight Common Multiples of Binary Primitive Polynomials through Discrete Logarithms,
    Proc. of YACC2014, p. 10.
14. 2014 - coauthor: C. Pellegrini, A. Rimoldi
    Geometric features for hand-written signatures,
    Springer Proceedings in Mathematics and Statistics, vol. 84, p. 117--134.
15. 2015 - coauthors: R. Longo, C. Marcolla
    Key-Policy Multi-Authority Attribute-Based Encryption,
    Proc. of CAI2015, Springer LNCS, vol. 9270, p. 152--164.
16. 2015 - coauthors: M. Piva, M. Pizzato
    Attacking BEAR and LION schemes in a realistic scenario,
    Proc. of CAI2015, Springer LNCS, vol. 9270, p. 189--195.
17. 2015 - coauthor: M. Calderini
    On differential uniformity of maps that may hide an algebraic trapdoor,
    Proc. of CAI2015, Springer LNCS, vol. 9270, p. 70--78.
18. 2015 - coauthors: A. Meneghetti, A. Tomasi et al.
    A post-processing free Si nanocrystals based quantum random number generator,
    Proc. of EQEC2015, EA_P_32.
19. 2016 - coauthors: F. Alda, R. Aragona, L. Nicolodi
    Implementation and improvement of the Partial Sum Attack on 6-round~AES,
    Proc. of WCS2014, Springer LNEE, vol. 358, p. 181--195.
20. 2016 - coauthors: A. Meneghetti, P. Peterlongo
    Encoding in the DTMF channel for two-channel authentication,
    Proc. of WCS2014, Springer LNEE, vol. 358, p. 205--212.
21. 2016 - coauthors: R. Aragona, F. Gozzini
    A Real Life Project in Cryptography: Assessment of RSA Keys,
    Proc. of WCS2014, Springer LNEE, vol. 358, p. 197--203.
22. 2017 - coauthors: C. Blondeau, R. Civino
    Differential Attacks: Using Alternative Operations,
    Proc. of Int. Workshop on Coding and Cryptography (WCC2017), p. 12.
23. 2017 - coauthors: C. Brunetta, M. Calderini
    Hidden sums and their application on block ciphers,
    Proc. of int. Workshop on Coding and Cryptography (WCC2017), p. 12.

Curriculum Vitae

---

24. 2017 - coauthors: R. Longo, C. Marcolla
    Collaborative Multi-Authority Key-Policy Attribute-Based Encryption for Shorter Keys and Parameters,
    Proc. of CAI2017, p. 67, full version at https://eprint.iacr.org/2016/262.pdf.
25. 2017 - coauthors: R. Longo, F. Pintore, G. Rinaldo
    On the security of blockchain BIX protocol and certificates,
    Proc. of Int. Conference on Cyber Conflict (CyCon2017), p.1--16.
26. 2019 - coauthors: A. Meneghetti, A.O.Quintavalle, A. Tomasi
    Two-tier blockchain timestamped notarization with incremental security,
    Proc. of DLT@ ITASEC2019, CEUR Proceedings, Vol. 2334, p. 32--42.
27. 2020 - coauthors: A. Meneghetti, D. Taufer
    A note on an ECDLP-based PoW model,
    Proc. of DLT@ ITASEC2020, CEUR Proceedings, vol. 2580.

Preprints (17)

We list only preprints whose content has never been published in any other form.

1. 2003 - coauthor: F. Ponchio
   A lower bound on the distance of cyclic codes,
   unpublished BCRI - UCC preprint, no. 7
2. 2005 - coauthors: A. Rimoldi, P. Fragneto
   An approach to create coprime polynomial pairs,
   unpublished BCRI - UCC preprint, no. 48
3. 2006 - coauthors: A. Caranti, F. Dalla Volta, F. Villani
   Imprimitive permutations groups generated by the round functions of key-alternating block ciphers and truncated differential cryptanalysis,
   unpublished arXiv preprint, https://arxiv.org/abs/math/0606022
4. 2006 - coauthor: E.Betti
   A theory for distance bounding cyclic codes,
   Unpublished BCRI - UCC preprint, no. 62.
5. 2006 - coauthor:E. Guerrini
   A classification of MDS binary systematic codes,
   unpublished BCRI - UCC preprint, no. 57
6. 2007 - coauthors: M. Lucey, C. C. Murphy
   M-Channel Paraunitary Multirate Filter Bank Factorisation over Fields of Characteristic Two,
   Unpublished BCRI - UCC preprint, no. 60

Curriculum Vitae

---

7. 2008 - coauthors: F. Dalla Volta, M. Giorgetti
   Permutation equivalent maximal irreducible Goppa codes,
   unpublished arXiv preprint, https://arxiv.org/abs/0806.1763

8. 2009 - coauthors: M. Rossi, C. Spagnol
   Quasi-cyclic LDPC codes with high girth,
   unpublished arXiv preprint, https://arxiv.org/abs/0906.3410

9. 2010 - coauthors: A. Rimoldi, I. Toli
   A possible intrinsic weakness of AES and other cryptosystems,
   unpublished arXiv preprint, https://arxiv.org/abs/1006.5894

10. 2010 - coauthors: E. Bertolazzi, A. Rimoldi
    Do AES encryptions act randomly?
    unpublished arXiv preprint, https://arxiv.org/abs/1011.2644

11. 2016 - coauthors: C. Marcolla, R. Longo
    Collaborative Multi-Authority Key-Policy Attribute-Based Encryption for Shorter Keys and Parameters, Unpublished IACR preprint, https://eprint.iacr.org/2016/262

12. 2019 - coauthor: R. Longo
    Public Ledger for Sensitive Data,
    Unpublished IACR preprint, https://eprint.iacr.org/2019/713.pdf

13. 2020 - coauthors: A. Meneghetti, M. Pellegrini
    A formula on the weight distribution of linear codes with applications to AMDS codes,
    unpublished arXiv preprint, https://arxiv.org/abs/2003.14063

14. 2020 - coauthors: M. Battagliola, R.Longo, A. Meneghetti
    Threshold ECDSA with an Offline Recovery Party,
    unpublished arXiv preprint, https://arxiv.org/abs/2007.04036

15. 2020 - coauthor D. Taufer
    The group structure of elliptic curves over Z/NZ,
    unpublished arXiv preprint, https://arxiv.org/abs/2010.15543

16. 2020 - coauthors: R. Longo, A. Meneghetti
    Threshold Multi-Signature with an Offline Recovery Party,
    Unpublished IACR preprint, https://eprint.iacr.org/2020/023.pdf

17. 2020 - coauthor: C. Spadafora, R. Longo
    Coercion-Resistant Blockchain-Based E-Voting Protocol,
    Unpublished IACR preprint, https://eprint.iacr.org/2020/674.pdf

Curriculum Vitae

Courses that I have lectured at university level (61):

1. **2002** - *Coding Theory and Cryptography* (20 lectures)
   University of Milano-Bicocca, MSC in Applied and Industrial Mathematics
2. 2002 - *Coding Theory* (30 lectures)
   University of Milan, Ph.D. in Mathematics
3. **2003** - *Coding Theory and Cryptography* (30 lectures)
   University of Milano-Bicocca, MSC in Applied and Industrial Mathematics
4. 2003 - *Coding Theory* (40 lectures)
   University of Milan, Ph.D. in Mathematics
5. **2004** - *Coding Theory and Cryptography* (30 lectures)
   University of Milano-Bicocca, MSC in Applied and Industrial Mathematics
6. 2004 - *Ring and Field Theory* (30 lectures)
   University College Cork UCC, BSC and MSC in Mathematics
7. **2005** - *Coding Theory and Groebner bases* (15 lectures)
   University of Pisa, BSC in Mathematics
8. 2005 - *Coding Theory and Cryptography* (30 lectures)
   University of Milano-Bicocca, MSC in Applied and Industrial Mathematics
9. **2006** - *Coding Theory and Cryptography* (30 lectures)
   University of Milano-Bicocca, MSC in Applied and Industrial Mathematics
10. 2006 - *Symmetric Cryptography* (10 lectures)
    University of Milan, Ph.D. in Mathematics
11. 2006 - *Coding and Cryptography* (20 lectures)
    University of Florence, Ph.D. in Mathematics
12. **2007** - *Coding Theory and Cryptography* (30 lectures)
    University of Milano-Bicocca, MSC in Applied and Industrial Mathematics
13. 2007 - *Algebraic Coding Theory* (40 lectures)
    University of Trento, BSC in Mathematics
14. 2007 - *Discrete Fourier Transform* (40 lectures)
    University of Trento, BSC in Mathematics
15. **2008** - *Algebraic Coding Theory* (40 lectures)
    University of Trento, BSC in Mathematics
16. 2008 - *Advanced Coding Theory* (40 lectures)
    University of Trento, MSC students in Mathematics

Curriculum Vitae

---

17. **2009** - *Algebraic Coding Theory* (40 lectures)
    University of Trento, BSC in Mathematics
18. 2009 - *Advanced Coding Theory* (40 lectures)
    University of Trento, MSC in Mathematics
19. 2009 - *Groebner bases, geometric codes and order domains* (10 lectures)
    University of Trento, Ph.D. in Mathematics
20. 2009 - *Classical and Advanced Coding Theory* (80 lectures)
    University of Trento, BSC and MSC in Mathematics
21. **2010** - *Block ciphers and their security* (40 lectures)
    University of Trento, Ph.D. in Mathematics
22. 2010 - *Classical and Advanced Coding Theory* (80 lectures)
    University of Trento, BSC and MSC in Mathematics
23. **2011** - *Classical and Advanced Coding Theory* (80 lectures)
    University of Trento, BSC and MSC in Mathematics
24. **2012** - *Boolean functions and their applications to cryptography* (40 lectures)
    University of Trento, Ph.D. in Mathematics
25. 2012 - *Groebner Bases, Curves, Codes and Cryptography* (8 lectures)
    University of Trento, Ph.D. in Mathematics
26. 2012 - *Classical and Advanced Coding Theory* (80 lectures)
    University of Trento, BSC and MSC in Mathematics
27. 2012 - *Laboratories of Applied Maths* (30 lectures)
    University of Trento, BSC in Mathematics
28. 2012 - *Cryptography* (40 lectures)
    University of Trento, BSC and MSC in Mathematics
29. **2013** - *Cryptography* (40 lectures)
    University of Trento, BSC and MSC in Mathematics
30. 2013 - *Laboratories of Applied Maths* (30 lectures)
    University of Trento, BSC in Mathematics
31. 2013 - *Advanced Coding Theory and Cryptography* (40 lectures)
    University of Trento, MSC in Mathematics
32. 2013 - *Coding Theory and Applications* (40 lectures)
    University of Trento, MSC in Mathematics
33. **2014** - *Laboratories of Applied Maths* (30 lectures)
    University of Trento, BSC in Mathematics

Curriculum Vitae

---

34. 2014 - *Complexity in Cryptography* (10 lectures)
    University of Trento, PHD in Mathematics
35. 2014 - *Advanced Coding Theory and Cryptography* (40 lectures)
    University of Trento, MSC in Mathematics
36. 2014 - *Coding Theory and Applications* (40 lectures)
    University of Trento, MSC in Mathematics
37. 2014 - *Cryptography* (40 lectures)
    University of Trento, MSC in Mathematics and Computer Science
38. **2015** - *Advanced Coding Theory and Cryptography* (40 lectures)
    University of Trento, MSC in Mathematics
39. 2015 - *Coding Theory and Applications* (40 lectures)
    University of Trento, MSC in Mathematics
40. 2015 - *Cryptography* (40 lectures)
    University of Trento, MSC in Mathematics and Computer Science
41. 2015 - *Finite Field and Symmetric Cryptography* (40 lectures)
    University of Trento, MSC in Mathematics
42. **2016** - *Advanced Coding Theory and Cryptography* (40 lectures)
    University of Trento, MSC in Mathematics
43. 2016 - *Coding Theory and Applications* (40 lectures)
    University of Trento, MSC in Mathematics
44. 2016 - *Cryptography* (50 lectures)
    University of Trento, MSC in Mathematics and Computer Science
45. 2016 - *Finite Field and Symmetric Cryptography* (40 lectures)
    University of Trento, MSC in Mathematics
46. **2017** - *Advanced Coding Theory and Cryptography* (40 lectures)
    University of Trento, MSC in Mathematics
47. 2017 - *Coding Theory and Applications* (40 lectures)
    University of Trento, MSC in Mathematics
48. 2017 - *Cryptography* (50 lectures)
    University of Trento, MSC in Mathematics and Computer Science
49. 2017 - *Finite Field and Symmetric Cryptography* (40 lectures)
    University of Trento, MSC in Mathematics
50. **2018** - *Finite Field and Symmetric Cryptography* (40 lectures)
    University of Trento, MSC in Mathematics

Curriculum Vitae

---

51. 2018 - *Advanced Coding Theory and Cryptography* (40 lectures)
    University of Trento, MSC in Mathematics
52. 2018 - *Coding Theory and Applications* (40 lectures)
    University of Trento, MSC in Mathematics
53. 2018 - *Cryptography* (50 lectures)
    University of Trento, MSC in Mathematics and Computer Science
54. **2019** - *Finite Field and Symmetric Cryptography* (40 lectures)
    University of Trento, MSC in Mathematics
55. 2019 - *Advanced Coding Theory and Cryptography* (40 lectures)
    University of Trento, MSC in Mathematics
56. 2019 - *Coding Theory and Applications* (40 lectures)
    University of Trento, MSC in Mathematics
57. 2019 - *Cryptography* (50 lectures)
    University of Trento, MSC in Mathematics
58. 2019 - *Applied Cryptography* (40 lectures)
    University of Trento, MSC in Computer Science
59. **2020** - *Finite Field and Symmetric Cryptography* (40 lectures)
    University of Trento, MSC in Mathematics
60. 2020 - *Advanced Coding Theory and Cryptography* (40 lectures)
    University of Trento, MSC in Mathematics
61. 2020 - *Cryptography* (50 lectures)
    University of Trento, MSC in Mathematics

Curriculum Vitae

Master's Theses supervised (103)

1. 2001 - **Lucia Berardi**,
   Some applications of neural networks
   Dept. of Math., University of Milan-Bicocca
2. 2003 - **Leonarda Mangieri,**
   Implementations of coding-decoding procedures for a number theory family of Space-Time codes
   Dept. of Math., University of Milan-Bicocca
3. 2003 - **Francesca Villani,**
   Modes of operation for a block cipher
   Dept. of Math., University of Milan-Bicocca
4. 2003 - **Marta Giorgetti,**
   An investigation of LDPC decoding for Goppa codes
   Dept. of Math., University of Milan-Bicocca
5. 2003 - **Jennifer Manginelli,**
   An investigation of LDPC decoding for Goppa codes
   Dept. of Math., University of Milan-Bicocca
6. 2004 - **Richard Bresnan,**
   Novel code construction and decoding techniques for LDPC codes
   Dept. of Elec. Eng., University College Cork
7. 2004 - **Marta Rossi,**
   Construction of quasi-cyclic LDPC codes
   Dept. of Math., University of Milan-Bicocca
8. 2004 - **Emmanuela Orsini,**
   Metodi algebrici per la costruzione di matrici di parità per LDPCC
   Dept. of Math., University of Milan-Bicocca
9. 2004 - **Simone Nava,**
   Metodi algebrici per la costruzione di matrici di parità per LDPCC
   Dept. of Math., University of Milan-Bicocca
10. 2005 - **Emanuele Betti,**
    Un'interpretazione algebrica della distanza dei codici ciclici
    Dept. of Math., University of Pisa
11. 2005 - **Anna Rimoldi,**
    Coppersmith's algorithm with Fitzpatrick's techniques
    Dept. of Math., University of Milan-Bicocca

Curriculum Vitae

---

12. 2005 - **Eleonora Guerrini,**
    Distanza e ottimalità in codici non lineari
    Dept. of Math., University of Pisa
13. 2005 - **Ilaria Simonetti,**
    Crittosistemi polinomiali
    Dept. of Math., University of Milan-Bicocca
14. 2006 - **James McDonagh,**
    LDPC Codes Using Quasi-Cyclic Encoding
    Dept. of Microelectronics, University College Cork
15. 2006 - **Tony O'Halloran,**
    Forward Error Correction techniques for use in Wireless Sensor Network
    Dept. of Microelectronics, University College Cork
16. 2006 - **Paola Staglianò,**
    Sistemi crittografici e il problema della fattorizzazione
    Dept. of Math., University of Milan-Bicocca
17. 2008 - **Valeria Bodrone,**
    Basi di Groebner e codici correttori
    Dept. of Math., University of Torino
18. 2009 - **Chiara Marcolla,**
    Parole di peso piccolo dei codici Hermitiani
    Dept. of Math., University of Trento
19. 2009 - **Lara Maines,**
    Una debole rappresentazione del gruppo simmetrico
    Dept. of Math., University of Trento
20. 2009 - **Marco Pizzato,**
    The Jacobian Conjecture
    Dept. of Math., University of Trento
21. 2010 - **Marco Frego,**
    Probabilità errore in decodifica e bound relativi
    Dept. of Math., University of Trento
22. 2010 - **Matteo Piva,**
    Decoding error probability with a new bound
    Dept. of Math., University of Trento
23. 2011 - **Daniele Giovannini,**
    A mathematical overview of modern stream ciphers
    Dept. of Math., University of Trento

Curriculum Vitae

---

24. 2011 - **Valentina Pulice,**
    A security classification of Boolean functions
    Dept. of Math., University of Trento
25. 2011 - **Stefano Martin,**
    Construction and evaluation of block ciphers
    Dept. of Math., University of Trento
26. 2011 - **Stefania Vanzetti,**
    Attacchi ai sistemi crittografici basati sul logaritmo discreto:il caso delle curve iperellittiche
    Dept. of Math., University of Torino
27. 2012 - **Alberto Ravagnani,**
    On Goppa codes on the Hermitian curve
    Dept. of Math., University of Trento
28. 2012 - **Chiara Pellegrini,**
    Signature verification algorithms and algebraic homomorphic encryption
    Dept. of Math., University of Trento
29. 2012 - **Giada Sciarretta,**
    Biometric signature protection and decoding algorithm analysis
    Dept. of Math., University of Trento
30. 2012 - **Valentina Da Rold,**
    Biometric signature protection with channel analysis
    Dept. of Math., University of Trento
31. 2013 - **Martina Curto**,
    Intersections between Hermitian curve and parabolas.Their application to Hermitian codes
    Dept. of Math., University of Trento
32. 2013 - **Daniel Pinter,**
    Cryptographic application of number theory to online banking
    Dept. of Math., University of Trento
33. 2013 - **Francesco Aldà,**
    The Partial Sum attack on 6-round reduced AES:Implementation and improvement
    Dept. of Math., University of Trento
34. 2013 - **Alessio Meneghetti,**
    Algebraic post-processing and non-binary entropy extractors
    Dept. of Math., University of Trento
35. 2013 - **Nadir Cordioli,**
    Euclidean algorithm and Fitzpatrick's algorithm:A comparison beyond distance
    Dept. of Math., University of Trento

Curriculum Vitae

---

36. 2014 - **Simona Dimase,**
    Cryptanalysis of GSM stream ciphers
    Dept. of Math., University of Trento
37. 2014 - **Beatrice Ridolfi,**
    Cryptanalysis of Bluetooth stream cipher
    Dept. of Math., University of Trento
38. 2014 - **Daniele Maccauro,**
    On some algebraic properties of Boolean functions
    Dept. of Math., University of Perugia
39. 2014 - **Cecilia Boschini,**
    NTWO: a post quantum cipher
    Dept. of Math., University of Trento
40. 2014 - **Aaron Gaio,**
    Some teaching experience in computational algebra
    Dept. of Math., University of Trento
41. 2014 **- Francesco Gozzini,**
    RLWE-based somewhat homomorphic encryption, with an application to the symmetric searchable encryption problem
    Dept. of Math., University of Trento
42. 2014 - **Franca Marinelli,**
    Somewhat Homomorphic Encryption with some security bounds
    Dept. of Math., University of Trento
43. 2014 - **Federico Giacon,**
    Revising RS-ABE, an encryption scheme for user revocation and attribute-based access
    Dept. of Math., University of Padova
44. 2014 **- Riccardo Longo,**
    Attribute Based Encryption with algebraic methods
    Dept. of Math., University of Trento
45. 2014 - **Giulia Traverso,**
    On some modern applications of cryptography
    Dept. of Math., University of Trento
46. 2014 - **Giulia Perina,**
    Cryptographic algorithms for the iPhone
    Dept. of Math., University of Trento

Curriculum Vitae

---

47. 2014 - **Ambra Valenti,**
    Algebraic generation of pseudorandom numbers
    Dept. of Math., University of Trento
48. 2014 - **Giulia Benedetti**,
    Algebraic weakness of the dual Elliptic curve PRNG
    Dept. of Math., University of Trento
49. 2014 - **Piera Galber,**
    Algebraic coding in Blue-Ray technology
    Dept. of Math., University of Trento
50. 2015 - **Gloria Massera,**
    LDPC Codes in Quantum Key Distribution
    Dept. of Math., University of Trento
51. 2015 - **Marco Iavernaro**
    On some cryptographic properties of vectorial Boolean functions
    Dept. of Math., University of Trento
52. 2015 - **Irene Villa,**
    On Boolean functions in even dimension
    Dept. of Math., University of Trento
53. 2015 - **Marco Martinoli,**
    Glitch propagation model and cryptography
    Dept. of Math., University of Trento
54. 2015 - **Lucia Brentegani,**
    Cryptographic properties of PGP
    Dept. of Math., University of Trento
55. 2015 - **Roberta Barbi,**
    Polynomial interpolation over finite fields and applications to list decoding of Reed-Solomon codes
    Dept. of Math., University of Trento
56. 2016 - **Pasqua Valentina Mauri,**
    PKI and IBE: authentication method and algebraic background
    Dept. of Math., University of Trento
57. 2016 - **Francesco De Vito,**
    An application of Edwards elliptic curves to Ripple protocol
    Dept. of Math., University of Trento,

Curriculum Vitae

---

58. 2016 - **Marta Salvaterra,**
    On Bitcoin and the security of ECDSA digital signature
    Dept. of Math., University of Trento
59. 2016 - **Valentina Calzavara,**
    Cryptographic significance of key wrapping
    Dept. of Math., University of Trento
60. 2016 - **Andrea Zanini,**
    On message authentication codes and related mathematical problems
    Dept. of Math., University of Trento
61. 2016 - **Patrick Harasser,**
    Cover attacks on hyperelliptic curve cryptography
    Dept. of Math., University of Trento
62. 2016 - **Silvia Berlanda,**
    Cryptographic protection for shared processed data onan untrusted platform
    Dept. of Math., University of Trento
63. 2016 - **Roberto Roscino,**
    XMSST. A post-quantum signature for the QKDS public channel authentication
    Dept. of Math., University of Trento
64. 2016 - **Alessandro Amadori**,
    On summation polynomial for elliptic curves
    Dept. of Math., University of Trento
65. 2016 - **Carlo Brunetta,**
    On some computational aspects for hidden sums in Boolean functions
    Dept. of Math., University of Trento
66. 2017 - **Alessandro Budroni,**
    Hash maps in pairing-based cryptography
    Dept. of Math., University of Trento
67. 2017 - **Manni Sara,**
    Symmetric authentication methods for entities: a proof of security for NKerberos
    Dept. of Math., University of Trento
68. 2017 - **Francesco Battistoni,**
    Blockchain and Smart Contract
    Dept. of Computer Science, University of Verona
69. 2017 - **Ilaria Zappatore,**
    Primitivity of generalized translation based block ciphers
    Dept. of Math., University of Trento

Curriculum Vitae

---

70. 2017 - **Giuseppe Giffone,**
    Analysis of a revocation-storage attribute-based encryption
    Dept. of Math., University of Trento
71. 2017 - **Marco Zaninelli,**
    On cryptographic properties of Boolean functions
    Dept. of Math., University of Trento
72. 2017 - **Nicolò Fornari,**
    Cryptography in the white-box attack model: some constructions and attacks
    Dept. of Math., University of Trento
73. 2017 - **Alessandro Melloni,**
    A description of the Peercoin protocol
    Dept. of Math., University of Trento
74. 2017 - **Cristian Mirto,**
    The Levenshtein theorem on optimal codes
    Dept. of Math., University of Trento
75. 2017 - **Nicoletta Alfarano Gianira,**
    The diffusion property of some mixing-layer
    Dept. of Math., University of Trento
76. 2018 - **Armanda Ottaviano Quintavalle,**
    Algebraic methods for quantum codes
    Dept. of Math., University of Trento
77. 2018 - **Stefania Innocenti,**
    On index calculus for elliptic curves
    Dept. of Math., University of Trento
78. 2018 - **Mattia Veroni,**
    Computing isogenies from elliptic curves over finite fields
    Dept. of Math., University of Trento
79. 2018 - **Luca Girardi,**
    On the minimum distance of AG codes over the GGS curve
    Dept. of Math., University of Trento
80. 2018 - **Eshun Samuel Nana,**
    Security analysis of LORAWAN networks
    Dept. of Math., University of Trento
81. 2019 - **Alex Pellegrini,**
    On two algebraic decisions problems and their instances
    Dept. of Math., University of Trento

Curriculum Vitae

---

82. 2019 - **Samuele Andreoli,**
    Analysis and implementation of lattice-based key exchanges
    Dept. of Math., University of Trento
83. 2019 - **Mattia Righele,**
    Classical code-based algorithms for post-quantum cryptography
    Dept. of Math., University of Trento
84. 2019 - **Flavio Pizzorno,**
    A Bitcoin risk assessment under the hypothesis of a quantum computer
    Dept. of Math., University of Trento
85. 2019 - **Alessandro Gollini,**
    Algorithms for polynomial multiplication over finite fields
    Dept. of Math., University of Trento
86. 2019 - **Tommaso Parise,**
    Sharding and parallelisation of blockchain-based computations
    Dept. of Math., University of Trento,
87. 2019 - **Gaetano Russo,**
    Post-Quantum McEliece-based cryptosystems: LEDA and BIKE
    Dept. of Math., University of Trento,
88. 2019 - **Rocco Mora,**
    Efficient decoding algorithms for QC-LDPC and QC-MDPC code-based cryptosystems
    Dept. of Math., University of Trento
89. 2019 - **Rosanna Racanelli,**
    On Format Preserving Encryption and its applications to security and privacy
    Dept. of Math., University of Trento
90. 2019 - **Jacopo Pasini,**
    Ring signatures and Monero
    Dept. of Math., University of Trento
91. 2019 - **Alberti Alessandro,**
    Android cryptography and keystore
    Dept. of Math., University of Trento
92. 2020 - **Paolo Bartolucci,**
    Some cryptographic methods for digital identity
    Dept. of Math., University of Trento
93. 2020 - **Edoardo Signorini,**
    Post-quantum cryptography: polynomial LWE and NewHope
    Dept. of Math., University of Trento

Curriculum Vitae

---

94. 2020 - **Chiara Spadafora,**
    A new blockchain-based secure e-voting protocol
    Dept. of Math., University of Trento
95. 2020 - **Thomas Chiozzi,**
    On Weil and Tate pairings and their applications in cryptography
    Dept. of Math., University of Trento
96. 2020 - **Leonardo Pavone,**
    Survey on digital signatures
    Dept. of Math., University of Trento
97. 2020 - **Michele Battagliola,**
    A threshold signature algorithm with an offline participant
    Dept. of Math., University of Trento
98. 2020 - **Giuseppe D'Alconzo,**
    Average-case complexity and problems from Coding theory
    Dept. of Math., University of Trento
99. 2020 - **Giulia Bracco,**
    On the nonlinearity of Boolean functions
    Dept. of Math., University of Trento
100. 2020 - **Lara Vicino,**
    On the cubic norm-trace curve and its AG codes
    Dept. of Math., University of Trento
101. 2020 - **Giulia Biasi,**
    Rainbow: a multilayered Oil and Vinegar signature scheme
    Dept. of Math., University of Trento
102. 2020 - **Salvatore Schiavulli,**
    Two secure multi-party computation protocols achieving passive security
    Dept. of Math., University of Trento
103. 2020 - **Federico Mazzone,**
    A threshold MPC signature scheme with an offline recovery party for custody of crypto-assets
    Dept. of Math., University of Trento

Curriculum Vitae

Ph.D. theses supervised (22)

1. 2007 - **Marta Giorgetti**,
   On some algebraic interpretations of classical codes
   Dept. of Math., University of Milan
2. 2008 - **Emmanuela Orsini**,
   On the decoding and distance problems for algebraic codes
   Dept. of Math., University of Milan
3. 2008 - **Christian Spagnol,**
   Aspects of LDPC codes for hardware implementation
   Dept. of Elec. Eng., University College Cork
4. 2009 - **Ilaria Simonetti,**
   On some applications of commutative algebra to Boolean functions and their non-linearity
   Dept. of Math., University of Milan
5. 2009 - **Eleonora Guerrini,**
   Systematic codes and polynomial ideals
   Dept. of Math., University of Trento
6. 2009 - **Anna Rimoldi,**
   On algebraic and statistical properties of AES-like ciphers
   Dept. of Math., University of Trento
7. 2013 - **Chiara Marcolla,**
   On structure and decoding of Hermitian codes
   Dept. of Math., University of Trento
8. 2014 - **Matteo Piva,**
   Algebraic methods for the distance of cyclic codes
   Dept. of Math., University of Trento
9. 2014 - **Martino Borello,**
   Automorphism groups of self-dual binary linear codes
   Dept. of Math., University of Milan-Bicocca
10. 2015 - **Emanuele Bellini,**
    Computational techniques for nonlinear codes and Boolean functions
    Dept. of Math., University of Trento
11. 2015 - **Marco Calderini,**
    On Boolean functions, symmetric cryptography and algebraic coding theory
    Dept. of Math., University of Trento

Curriculum Vitae

---

12. 2015 - **Federico Pintore,**
    Binary quadratic forms, elliptic curves and Schoof 's algorithm
    Dept. of Math., University of Trento
13. 2014 - **Claudia Tinnirello,**
    Cyclic codes: low-weight codewords and locators
    Dept. of Math., University of Trento
14. 2016 - **Marco Pellegrini,**
    On the weight distribution of Hermitian codes
    Dept. of Math., University of Florence
15. 2017 - **Alessio Meneghetti,**
    Optimal codes and entropy extractors
    Dept. of Math., University of Trento
16. 2018 - **Riccardo Longo,**
    Formal proofs of security for privacy-preserving blockchains and other cryptographic protocols
    Dept. of Math., University of Trento
17. 2018 - **Roberto Civino,**
    Differential attacks using alternative operations and block cipher design
    Dept. of Math., University of Trento
18. 2019 - **Matteo Bonini,**
    Intersections of algebraic curves and their link to the weight enumerators of algebraic-geometric code
    Dept. of Math., University of Trento
19. 2019 - **Giordano Santilli,**
    An investigation on integer factorization applied to public key cryptography
    Dept. of Math., University of Trento
20. 2019 - **Augustine Musukwa,**
    Some cryptographic properties of Boolean functions
    Dept. of Math., University of Trento
21. 2019 - **Carla Mascia,**
    Ideals generated by 2-minors: binomial edge ideals and polyomino ideals
    Dept. of Math., University of Trento
22. 2020 - **Daniele Taufer,**
    Elliptic Loops
    Dept. of Math., University of Trento

Curriculum Vitae

Organization of scientific conferences and workshops (27)

1. 2003 - *BCRI Workshop on Coding and Cryptography,*
   Cork, IRELAND
2. 2003 - *MIRIAM Coding and Cryptography Workshop,*
   Milan, ITALY
3. 2004 - *BCRI Workshop on Coding and Cryptography,*
   Cork, IRELAND
4. 2005 - *BCRI Workshop on Coding and Cryptography*
   Cork, IRELAND
5. 2006 - *Groebner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics*
   Linz, AUSTRIA
6. 2006 - *Coding Session at the 4th International Conference on Information, joint MFCSIT,*
   Cork, IRELAND
7. 2006 - *BCRI Workshop on Coding and Cryptography*
   Cork, IRELAND
8. 2008 - Workshop in Cryptography and Computer Algebra
   Pisa, ITALY
9. 2009 - *Workshop on Groebner bases and Geometric codes*,
   Trento, ITALY
10. 2009 - *Workshop on block ciphers and their security*,
    Trento, ITALY
11. 2011 - *First Cryptography Workshop BunnyTN*,
    Trento, ITALY
12. 2011 - *Second Cryptography Workshop BunnyTN*,
    Trento, ITALY
13. 2011 - *Workshop on Applied Mathematics*,
    Trento, ITALY
14. 2012 - *Third Cryptography Workshop BunnyTN*",
    Trento, ITALY,
15. 2013 - *Fourth Cryptography Workshop BunnyTN*,
    Trento, ITALY

Curriculum Vitae

---

16. 2014 - *Fifth Cryptography Workshop BunnyTN*,
    Trento, ITALY
17. 2015 - MEGA 2015 (Effective Methods in Algebraic Geometry)",
    Trento, ITALY
18. 2015 - *Sixth Cryptography Workshop Bunny TN*,
    Trento, ITALY
19. 2016 - *Seventh Cryptography Workshop BunnyTN*,
    Trento, ITALY
20. 2017 - *1st Workshop on Trusted Smart Contracts WTSC2017*,
    (in *Financial Cryptography and Data Security 2017)*, **Malta, MALTA**.
21. 2018 - *Special session on Post-Quantum Cryptography*
    (in *ITASEC2018*), **Milan, ITALY**
22. 2018 - *2nd Workshop on Trusted Smart Contracts WTSC2018,*
    (in *Financial Cryptography and Data Security 2018)*, **Santa Barbara, CURACAO**.
23. 2019 - *CifrisChain2019,*
    In collaboration with **CONSOB**, **Rome, ITALY.**
24. 2019 - PQ*Cifris2019,*
    In collaboration with **CONSOB**, **Rome, ITALY.**
25. 2019 - *3rd Workshop on Trusted Smart Contracts WTSC2019*,
    (in *Financial Cryptography and Data Security 2019)*, **Saint Kitts, SAINT KITTS**
26. 2020 - *4th Workshop on Trusted Smart Contracts WTSC2020*,
    (in *Financial Cryptography and Data Security 2020)*, **Sabah, MALAYSIA**
27. 2020 - *Workshop in CRYPTANALYSIS: a key tool in securing and breaking ciphers,*
    (in *ITASEC2020*), **Ancona, ITALY**

Curriculum Vitae

Talks given at conferences, workshops and other official events (41)

1. 2002 - *Using the syndrome variety to study cyclic codes*
   Workshop on Applications of Commutative Algebra, Catania
2. 2003 - *Bound on minimum weight codewords for BCH codes with d=5*
   BCRI Workshop on Coding and Cryptography, Cork
3. 2003 - *Recent trends in coding theory*
   MIRIAM Coding and Cryptography Workshop, Univ. of Milan, Milan
4. 2004 - *Efficient low-density parity-check decoding*
   The Irish Signal and Systems Conference (with L. Marnane and R. Bresnan), **Dublin**
5. 2005 - *On a class of quasi-cyclic LDPC codes*
   MEGA05, (Effective Methods in Algebraic Geometry), (with M. Rossi), **Alghero**
6. 2005 - *A bound for the distance of cyclic codes which is sometimes stronger than the Roos bound* - **MEGA05,** (with E. Betti)**, Alghero**
7. 2005 - *On the distance of non-linear codes*
   MEGA05 (Effective Methods in Algebraic Geometry), (with E. Guerrini), **Alghero**
8. 2006 - *A theory for the distance of cyclic codes*
   Groebner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics, Linz
9. 2006 - *Relations between bounds on the distance of cyclic codes and FGLM decoding*
   Groebner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics, Linz
10. 2006 - *Symmetric Cryptography, provable security, and group theory*
    Fourth International Conference on Information, joint MFCSIT06, Cork
11. 2007 - *An algebraic approach to the classification of some non-linear codes*
    WCC2007 (Int. Workshop on Coding and Cryptography), (with E. Guerrini), **Paris**
12. 2007 - *An algebraic description of Boolean functions*
    WCC2007 (Int. Workshop on Coding and Cryptography),(with I. Simonetti), **Paris**
13. 2007 - *General error locator polynomials for nth-root codes*
    WCC2007, (Int. Workshop on Coding and Cryptography), (with M. Giorgetti), **Paris**
14. 2007 - *Improved decoding of affine-variety codes*
    The Claude Shannon Workshop on Coding, Cryptography, **Cork**
15. 2008 - *An approach to a linear approximation of the AES*
    The Claude Shannon Workshop on Coding, Cryptography, **Cork**
16. 2009 - *Optimal binary codes with 4 codewords are linear*
    Workshop on Groebner bases and Geometric codes, Trento

Curriculum Vitae

17. 2009 - *On translation-based cryptosystems and their security*
    Workshop on block ciphers and their security, **Trento**
18. 2011 - *On the weights of affine-variety codes and some Hermitian codes*
    WCC2011 (with C. Marcolla and M. Pellegrini), **Paris**
19. 2011 - *Attacks and security of systems: comparisons and conclusions*
    Public key Cryptography: beyond RSA, Univ. of Torino, Torino
20. 2011 - *On the provable security of BEAR and LION schemes*
    The Claude Shannon Workshop on Coding, Cryptography, Cork
21. 2012 - *Hand-written signature and homomorphic encryption*
    SAGA Workshop, Trento
22. 2013 - *Some bounds on the size of codes*
    WCC2013, (with E. Bellini and E. Guerrini), **Bergen**
23. 2013 - *On the Hermitian curve and its intersections with some conics*
    MEGA2013, (with C. Marcolla and M. Pellegrini), **Frankfurt**
24. 2013 - *Generalized AG codes as evaluation codes*
    CAI2013 (Int. Conf. on Algebraic Informatics), (with M. Calderini), **Porquerolles Island**
25. 2013 - *A new bound for cyclic codes beating the Roos bound*
    CAI2013 (with M. Piva), **Porquerolles Island**
26. 2014 - *Boolean functions and trapdoors in block ciphers*
    International Workshop on Boolean Functions and Their Applications, Sorendal
27. 2014 - *Some security bounds for the DGHV scheme*
    YACC2014 (with F. Marinelli, R. Aragona and C. Marcolla), **Porquerolles Island**
28. 2014 - *Low-Weight Common Multiples of Binary Primitive Polynomials through Discrete Logarithms*, **YACC2014, Porquerolles Island.**,
29. 2014 - Implementation and improvement of the Partial Sum Attack on 6-round AES
    WCS2014 (Work. on Commun. Sec.), (with F. Aldà, R. Aragona, L. Nicolodi), **Ancona**
30. 2015 - *A Discrete Logarithm-based Approach to Compute Low-Weight Multiples of Binary Polynomials*, **MEGA2015** (with P. Peterlongo and C. Tinnirello), **Trento**
31. 2015 - *Algorithmic approach using polynomial systems for the nonlinearity of Boolean functions*, **MEGA2015** (with E. Bellini and T. Mora), **Trento**
32. 2015 - *Key-Policy Multi-Authority Attribute-Based Encryption*
    CAI2015 (with R. Longo and C. Marcolla), **Stuttgart**
33. 2015 - Attacking BEAR and LION schemes in a realistic scenario
    CAI2015 (with M. Pizzato and M. Piva), **Stuttgart**

Curriculum Vitae

---

34. 2015 - *On differential uniformity of maps that may hide an algebraic trapdoor*
    CAI2015 (with M. Pizzato and M. Piva), **Stuttgart**
35. 2015 - *On an algebraic trapdoor*
    XX Congresso dell'UMI (with R. Aragona), **Siena**
36. 2017 - *Differential Attacks: Using Alternative Operations*
    WCC 2017 (with C. Blondeau, R. Civino), **Saint-Petersburg**
37. 2017 - *Hidden sums and their application on block ciphers*
    WCC 2017, (with C. Brunetta, M. Calderini), **Saint-Petersburg**
38. 2017 - *Collaborative Multi-Authority Key-Policy Attribute-Based Encryption for Shorter Keys and Parameters,* **CAI 2017**, (with R. Longo, C. Marcolla), **Kalamata**
39. 2017 - *Blockchain to protect individual rights*
    Blockchain for Social Good, **Torino**
40. 2018- *Security proofs for some protocols based on blockchain technology*
    DLT2018 (1st Distributed Ledger Techn. Workshop) (with A. Meneghetti), **Perugia**
41. 2018 - *Computational aspects for the nonlinearity of Boolean functions*
    BFA2018, Loen

Talks outside conferences (36)

1. 2001 - *Secure and safe communications, coding theory, mathematical foundations of error correction* -- **Appl. Math. seminar series, Dept. of Math., Univ. of Milan, Milan**
2. 2001 - *Safe communications and coding theory*
   Math. seminar series Dept. of Math. and Appl., Univ. of Milan-Bicocca, Milan
3. 2002 - *On the syndrome variety for cyclic codes*
   Commutative Algebra group seminar series, Dept. of Math., Univ. of Pisa, Pisa
4. 2002 - *On the McEliece-Niederreiter Cryptosystem*
   Appl. Math. seminar series, Dept. of Math., Univ. of Milan, Milan
5. 2002 - *Solutions of polynomial systems on any field and Groebner bases*
   Appl. Math. seminar series, University College Cork, Cork
6. 2003 - *On general error locator polynomials for cyclic codes*
   School of Math. Sciences Colloquium, University College Cork, Cork.

Curriculum Vitae

---

7. 2003 - *An introduction to LDPC codes*
   CODES seminar series, University College Cork, Cork
8. 2003 - *On the sum-product algorithm and optimal decoding of linear codes- Part I*
   CODES seminar series, University College Cork, Cork
9. 2003 - *On the sum-product algorithm and optimal decoding of linear codes- Part II*
   CODES seminar series, University College Cork, Cork
10. 2004 - *Protecting data: how to get a train and arrive safe and sound*
    MathSoc Seminars, University College Cork, Cork
11. 2004 - *Digital Watermarking from an Information Theory point of view*
    CODES seminar series, University College Cork, Cork
12. 2004 - *Bounds on the distance of cyclic codes*
    IMA 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, University College Cork, Cork
14. 2005 - *A mixed "graph theory"-algebra approach to LDPC codes*
    University College Dublin, Dublin
15. 2005 - *General error locator polynomials for cyclic codes*
    Algebra and Geometry seminar series, Univ. of Genoa, Genoa
16. 2006 - *The syndrome variety and decoding of cyclic codes*
    University of Trento, Trento
17. 2006 - *Cyclic codes: decoding and distance bounding*
    CCA seminar series, ENSTA, Paris
18. 2007 - *Towards a moduli space for codes*
    Dept. of Mathematics, University of Torino, Torino
19. 2008 - *Intersections of Hermitian curves and minimum weight words*
    Dept. of Mathematics, Univ. of Torino, Torino
20. 2008 - *On Boolean functions and Groebner bases*
    Dept. of Mathematics, Univ. of Torino, Torino
21. 2010 - *Cryptography and weak group representations*
    Dept. of Mathematics, Univ. of Torino, Torino
22. 2010 - *An intrinsic weakness of the AES and other translation-based ciphers*
    Université de la Méditerranée, Marseille
23. 2010 - *The small weight words of some Hermitian codes*
    Université de la Méditerranée, Marseille

Curriculum Vitae

---

24. 2010 - *On Boolean function and non-linearity*
    Université de la Méditerranée, Marseille
25. 2011 - *On the provable security of some cryptographic primitives*
    Dept. of Mathematics, University of Torino, Torino
26. 2013 - *Bitcoin: the digital currency of the future*
    University of Verona, Verona
27. 2013 - *On the provable security of block ciphers from their components*
    University of Verona, Verona
28. 2013 - *Bitcoin: the digital currency of the future*
    University of Bolzano, Bolzano
29. 2014 - *On the Hermitian curve and its intersections with some conics*
    University of Messina, Messina
30. 2014 - *A bound on the size of systematic codes*
    University of Perugia, Perugia
31. 2014 - *CryptoLabTN: some real-life projects in Cryptography*
    Marche Polytechnic University, Ancona
32. 2017 - *A Security Proof of a Tokenization Algorithm*
    GSSI, L'Aquila, L'Aquila
33. 2017 - *Monero: the dark side of cryptocurrencies*
    University of Genoa, Genoa
34. 2017 - *Cryptographic primitives and their properties*
    University of Perugia, Perugia
35. 2017 - *Blockchain technology and its applications*
    University of Salerno, Salerno
36. 2018 - *Optimal non-linear Boolean functions as multivariable polynomials: the even case*
    Colloquium di Matematica, University of Roma Tre, Rome

Curriculum Vitae

Research projects with companies

Since my period as PHD student I've been actively involved in research with private companies, being the first that with Ansaldo Segnalamento Ferroviario on codes for railway signalling system (1999-2000). Immediately after my PHD defence, I have worked with Piaggio on optimization of engine production planning (2001-2002). In my Irish experience I've had many industrial collaborations, of which the most significant was this research contract

2005 - *Complexity issues in algebraic Coding Theory and Cryptography*, **STMicroelectronics**

Since I've started working at the University of Trento, I've had numerous research contracts with companies, as listed below:

1. 2008--2009 - *Data encryption for electronic payments,*
   Easycardservices
2. 2009--2010, *Error correcting codes for hard-disks,*
   IDT
3. 2010--2012, *Security assessment of ciphers for online-banking,*
   SGS - Banco Popolare
4. 2010--2012, *Security assessment of ciphers,*
   iTwin
5. 2012 - *Data encryption for handwritten signature verification,*
   Corvallis
6. 2012 - *Encryption for biometrics signatures,*
   PayBay Network
7. 2012--2013 - *Handwritten signature verification,*
   Corvallis
8. 2012--2013 - *An authentication model based on biometric signatures*,
   PayBay Networks
9. 2012--2013 - *Security issues in TITAN (an experimental e-payment system),*
   Poste Italiane and PayBay Networks
10. 2012--2013 - *Transaction signing in online banking,*
    IKS
11. 2013 - Secure multi-touch biometric user authentication
    Expert System

Curriculum Vitae

---

12. 2013 - *Homomorphic encryption,*
    Telsy
13. 2013 - *Lunghezza ottimale delle chiavi crittografiche di CA per la generazione di certificati Interbancari e EFT POS*, **Consorzio Bancomat**
14. 2013--2014 - *Cryptography for on-line banking,*
    AliasLab
15. 2013--2014 - *Mobile Banking: difese crittografiche,*
    Tecmarket e Banco Popolare
16. 2015 - *Nuovi sistemi di pagamento mobile payment con fidelity card, PagoBancomat e Criptovalute*, **Argentea** (with co-funding by **Fondazione CARITRO**)
17. 2015--2016 - *Scelta di chiavi forti di cifratura basate su curve ellittiche e valutazioni di sicurezza relative,* **ID Quantique**
18. 2016 - *Algoritmo di tokenizzazione e detokenizzazione*
    Poste -TAS
19. 2016 - *Studio di fattibilità per l'automatizzazione di un sistema di riconoscimento remoto per la app Chat&Cash,* **SGS**
20. 2016 - *Algoritmo di tokenizzazione e detokenizzazione,*
    Poste Italiane e TAS Group
21. 2016 - *Studio sulla lunghezza ottimale delle chiavi fornitore e delle chiavi terminale EFT-POS,* **Consorzio Bancomat**
22. 2017 - *Digital Notary Double Blockchain - PoC setup and customization,*
    Athilab e Nike Consulting
23. 2017 - *Scientific and cryptographic evaluation of Foodchain Infrastructure,*
    Foodchain
24. 2019 - *Design crittografico per la piattaforma Quadrans,*
    Foundation Quadrans
25. 2019 - *Valutazione crittografica per una piattaforma di blockchain,*
    Ailia SA
26. 2019 - *Protocollo di Threshold Multi-Signature su Curve Ellittiche,*
    Conio Inc.
27. 2019 - *Analisi preliminare algoritmi Proof-of-Work per tecnologie blockchain,*
    Foodchain
28. 2020 - *Algoritmi di cifratura per la Cloud Encryption,*
    BVTech

Curriculum Vitae

Other research projects

I have obtained some public funding for a few research projects, where I've applied jointly

1. 2008 -- 2011 - *Algebraic cryptography and coding,*
   MIUR (Italian Ministry of Education, Universities and Research)
2. 2008 -- 2009 *CRS*
   PAT (Provincia Autonoma di Trento)
3. 2015 -- 2018 *Group theory and cryptography (PRIN)* **MIUR**
4. 2013--2017 - *On silicon chip quantum optics for quantum computing and secure communications,* **PAT**

Courses for professionals and people working in companies (28)

1. 2010 - Trento (6-17 September, 40 hours)
   Criteri matematici per la sicurezza di un sistema crittografico
2. 2010 - Trento (29 November-3 Decembre, 40 hours)
   Crittoanalisi differenziale avanzata
3. 2011 - Trento (5-9 September, 40 hours)
   Valutazione matematica della sicurezza degli stream cipher
4. 2011 - Trento (6-10 June,40 hours)
   Valutazione matematica della sicurezza di un cifrario a blocchi
5. 2012 - Roma (26-30 November, 40 hours)
   Crittoanalisi avanzata di cifrari a flusso
6. 2013 - Trento (3-7 June, 40 hours)
   Sorgenti di randomicità in crittografia e crittoanalisi: specifiche e criticità
7. 2013 - Trento (9-13 June, 40 hours)
   Debolezza dei cifrari a blocchi: attacchi recenti e contromisure
8. 2014 - Online (30 videos)
   Applied Cryptography
9. 2015 - Trento (21-25 September, 40 hours)
   Mathematical trapdoors in block ciphers: evaluation and attack exploitation
10. 2016 - Trento (12-13 May, 10 hours)
    Bitcoin, Blockchain and their new frontiers

Curriculum Vitae

---

11. 2016 - Trento (26-27 September, 10 hours)
    Bitcoin, Blockchain and their new frontiers II
12. 2016 - Trento (17-21 October, 40 hours)
    Advanced Analysis of Block Ciphers
13. 2016 - Roma (10-11 November, 10 hours)
    Bitcoin, Blockchain and their new frontiers
14. 2016 - Milano (21-22 November, 10 hours)
    Bitcoin, Blockchain and their new frontiers
15. 2016 - Trento (7-11 November, 30 hours)
    Cryptography for Telephone Transmissions: video calling
16. 2016 - Online (17 October-12 December, 25 videos)
    BoAB: Bitcoin and other Applications of Blockchain
17. 2017 - Trento (8-22-29 May, 12 hours)
    Bitcoin, Blockchain and their new Frontiers
18. 2017 - Milano (19 Sept.-2-17 October, 12 hours)
    Bitcoin, Blockchain and their new Frontiers
19. 2017 - Roma (3-14-28 Novembre, 12 hours)
    Bitcoin, Blockchain and their new Frontiers
20. 2017 - Online (1 April- 1 July, 25 videos)
    BoAB: Bitcoin and other Applications of Blockchain
21. 2018 - Roma (9-13 April, 40 hours)
    Crittoanalisi avanzata di RSA
22. 2018 - Roma (7-11 May, 40 hours)
    Post-quantum Cryptography
23. 2018 - Roma (8-12 October, 40 hours)
    Quantum Information
24. 2019 - Roma (13-17 May, 40 hours)
    Crittografia PostQuantum
25. 2019 - Roma (9-13 Septembre, 40 hours)
    Quantum Information
26. 2020 - Roma (14-18 September, 40 hours)
    Cloud Encryption: Omomorfa
27. 2020 - Roma (12-16 October, 40 hours)
    Cloud Encryption: Functional

Curriculum Vitae

---

28. 2020 - Online (30 Novembre - 4 December, 20 videos)
    Cifrari a blocchi

Dissemination activity

Dissemination papers (13)

1. 2013 - Agenda Digitale
   Acquisti online, verso un nuovo framework anti frode
2. 2013 - Agenda Digitale
   Strumenti personali colonna della nuova sicurezza online
3. 2014 - Agenda Digitale
   Bitcoin, due imboscate attendono sul cammino della valuta
4. 2015 - coauthors: M. Baldi, M. Elia
   La sicurezza nell'impero delle comunicazioni,
   Gnosis, vol. 2, p. 118--121
5. 2015 - coauthors: M. Baldi, M. Elia
   I pratici effetti dell'astrazione matematica nella crittografia
   Gnosis, vol. 4, p. 112-119
6. 2016,
   Autenticazione e cifratura dei dati biometrici,
   Gnosis, vol. 1, p. 194--199
7. 2016,
   La crittografia al centro dello scontro tra Apple e FBI
   Gnosis, vol. 2, p. 138--143
8. 2016 - coauthors: M. Baldi, M. Elia
   Il futuro della crittografia teorica e pragmatica e il post quantum,
   Gnosis, vol. 4, p. 168--173
9. 2016,
   Cifratura del cloud e crittografia quantistica. Due balzi di conoscenza
   Gnosis, vol. 3, p. 142--147
10. 2016 - Agenda Digitale
    Dal voto elettronico a un nuovo Cloud, gli usi più innovativi della Blockchain
11. 2018 - coauthor: M. Elia
    Il caso Enigma. La storia (I parte)
    Gnosis, vol. 1, p. 46--59
12. 2018 - coauthor: M. Elia
    Il caso Enigma. La crittoanalisi (II parte)
    Gnosis, vol. 2, p. 46--59
13. 2018 - Agenda Digitale
    Bitcoin, solo i fork lo renderanno maturo per i pagamenti, ecco perché

Curriculum Vitae

Workshops for a wide audience (24)

The aim of these workshops is to present technological advances driven by research to a wide non-academic audience. From 2011 to 2018 they have been organized mostly within the Laboratory of Cryptography (CryptoLabTN), which I founded in 2010 and led until 2020, while from 2018 to 2020 they have been organized mostly within the De Componendis Cifris (De Cifris), which is the Italian initiative in Cryptography, founded in 2018.

- **2011**
  - *Crittografia e sicurezza della Posta Elettronica Certificata PEC* - **Trento**
  - Crittografia e sicurezza nei dati biomedici - **Trento**
  - *Protezione dei dati e crittografia nel cloud computing* - **Trento**
  - *Crittografia a chiave pubblica: oltre RSA* - **Torino**
  - *Pagamenti elettronici e on-line banking: effettiva sicurezza crittografica* - **Trento**
  - *La crittografia nei telefonini anti-intercettazione* - **Trento**
  - *Crittografia a chiave pubblica: oltre RSA* - **Trento**
- **2012**
  - *Firma Digitale e PEC: facile e sicura* - **Trento**
  - *E-commerce e on-line banking: effettiva sicurezza crittografica* - **Trento**
  - *La sicurezza nei dispositivi e token per scambio dati cifrati* - **Trento**
  - *La sicurezza del Cloud Computing* - **Trento**
- **2013**
  - *E-payment Security* - **Trento**
  - *Trust and Cloud Computing* - **Trento**
  - *Bitcoin: The currency of the Future* - **Trento**
- **2015**
  - *Smartphone: cifrature e sicurezza* - **Trento**
  - *Bitcoin e altcoin: applicazioni e limitazioni* - **Milano**
- **2016** - *Cryptographic Aspects of Cloud and Distributed Computing* - **Trento**
- **2017** - *Blockchain and Innovative Applications* - **Trento**
- **2018**
  - *Blockchain e smart contract* - **Vicenza**
  - **(De Cifris)** *CifrisChain2019* - **Roma**
  - *De Cifris a Salerno* - **Salerno**
  - *De Cifris a Milano* - **Milano**
  - De Cifris a Roma - **Roma**
- **2019**
  - *Meeting De Cifris Nord Italia* - **Torino**
  - *Meeting De Cifris Centro-Sud Italia* - **Perugia**

Curriculum Vitae

Cryptographic challenges organized nationwide for Italian students

- **2019 -** *HACKATHON De Cifris di Smart Contract*
- **2016** - *Digital Signature awareness contest*
- **2015** - *ECC awareness contest*
- **2014** - *RSA awareness contest*
- **2011** - *CryptoWars2011*

Interviews (12)

1. 2014 - Il Sole 24 ore
   Tutti gli usi alternativi (e utili) del «cuore» di Bitcoin
2. 2011 - Il Sole 24 ORE
   Crittografia a prova di «cloud»
3. 2012 - Il Sole 24 ORE
   Crittografia, da sola non basta
4. 2015 - Il Sole 24 ORE
   Datemi una blockchain e vi cambierò il mondo
5. 2015 - Il Sole 24 ORE
   Le tre “S” del peer-to-peer: soldi, sicurezza e sapere
6. 2014 - Il Sole 24 ORE
   WhatsApp indiscreto
7. 2014 - Il Sole 24 ORE
   Il futuro della crittografia
8. 2014 - Il Sole 24 ORE
   La protezione alla fonte
9. 2013 - Il Sole 24 ORE
   Ecco SafePlug, lo scatolotto per la privacy prêt-à-porter
10. 2011 - Il Sole 24 ORE
    Non farsi intercettare? Un gioco da ragazzi
11. 2013 - la Repubblica
    Un software incrocia i dati e fa scattare l'allarme
12. 2012 - Radio3
    Chiavi deboli in un sistema crittografico