Emmanuela Orsini

Assistant Professor (Tenure-Track),
Dept Computing Sciences, Bocconi University
via Rontgen 1 (room 2c2-03), Milano, Italy

+39 02 5836.5621
emmanuela.orsini@unibocconi.it
https://cseao.github.io/

Education

Ph.D. in Mathematics and Statistics for Computational Sciences *January 2008*
Department of Mathematics, University of Milano, Italy.
Field: Algebraic Error Correcting Codes
Thesis: *On the decoding and distance problem of algebraic codes*
Advisors: Prof. Teo Mora and Prof. Massimilano Sala

Post-graduate Master in Applied Mathematics *September 2005*
Department of Mathematics,
Università degli Studi di Milano Bicocca and STMicroelectronics.
Thesis: *Parity-check matrices and decoding algorithms for LDPC codes*

Laurea Degree (M.Sc. equivalent) in Mathematics *April 2003*
Department of Mathematics, Università degli Studi di Pisa
Field: Commutative Algebra
Thesis : *Gröbner bases and specializations*
Advisor: Prof. Patrizia Gianni

Academic and Non-academic Positions

Assistant Professor (Tenure-track) *Feb 2023 – Present*
Bocconi University, Dept. Computing Sciences

External Consultant
Zama (https://www.zama.ai/) *2024*

Free Researcher
COSIC, Katholieke Universiteit Leuven (KU Leuven) *Jan 2023- Jan 2025*

Research Expert (*Permanent* Research Position) *Jan 2018 – Jan 2023*
COSIC, Katholieke Universiteit Leuven (KU Leuven), Belgium

Senior Research Associate *Jan 2012 – Dec 2017*
Cryptography Group, Department of Computer Science
University of Bristol, UK

Postdoctoral Researcher *Jan 2008 – December 2011*
Department of Mathematics
Università degli Studi di Trento and Università di Pisa

Awards and Other Qualifications

- Italian National Scientific Qualification (ASN) for Associate Professor. *2025*

- Qualification aux fonctions de maître de conférences en Informatique (France) *2011*
- Qualification aux fonctions de maître de conférences en Mathématique (France) *2011*
- Fellowship from the Istituto Nazionale di Alta Matematica (INdAM) *2001–2002*

Research Grants

TEF Project: SwitchFHE. One postdoctoral position funded for 2 years, with the possibility of a 2-year renewal (2+2).
Role: PI *Budget:* ≈ 160.000,00€ (renewable) *2026–2028*

Fromager: Verify and Evaluate Software with Zero-Knowledge of its Source Code
DARPA program: Securing Information for Encrypted Verification and Evaluation (SIEVE)
Role: PI, ≈ 913.336, 00$
(Total amount received by our team ≈ 12M$) *April 2020 – April 2024*

COED – Computing on Encrypted Data
Program: Collective Research & Development and Collective Knowledge Dissemination/Transfer (COOCK), Research Foundation Flanders
Role: co-PI, ≈ 325.000,00€ *December 2020 – December 2022*

MOZAIK – Scalable and Secure Data Sharing
FWO Strategic Basic Research (SBO) from Research Foundation Flanders
Role: grant writer, collaborator, ≈ 1.261.734,00€ *March 2021 – March 2025*

NIST Post-Quantum Standardization Submissions

I contributed three candidate algorithms to NIST's Post-Quantum Cryptography standardization project. This is an open, multi-round competition launched in 2016 to select quantum-resistant security standards.

- First Round Submission: Nigel P. Smart, Martin R. Albrecht, Yehuda Lindell, Emmanuela Orsini, Valery Osheter, Kenny Paterson, Guy Peer, **LIMA: A PQC Encryption Scheme.** Website: https://lima-pq.github.io/.

- Second Round Submitter: Thomas Poppelmann, Erdem Alkim, Roberto Avanzi, Joppe Bos, Léo Ducas, Antonio de la Piedra, Peter Schwabe, Douglas Stebila, Martin R Albrecht, Emmanuela Orsini, Valery Osheter, Kenneth G Paterson, Guy Peer, Nigel P Smart, **New Hope. Post-quantum Key Encapsulation.** Website: https://newhopecrypto.org/.

- *Additional Call for Post-quantum Signatures:* Carsten Baum, Lennart Braun, Cyprien Delpech de Saint Guilhem, Michael Klooß, Christian Majenz, Shibam Mukherjee, Emmanuela Orsini, Sebastian Ramacher, Christian Rechberger, Lawrence Roy, Peter Scholl, **Faest Signature Algorithm** . Website: https://faest.info/
(**November 2024: Proposal advanced to the second round (ongoing)**)

Academic Service (Community)

General Chair : IACR Theory of Cryptography Conference (TCC 2024, 2-6 December, Milano)

Workshop Organization:
"COED Industry Day", 2022, Leuven, Belgium
https://www.esat.kuleuven.be/cosic/projects/coed/event/internal-event-coed-industry-day-2/
" Computation on Encrypted Data Industry Day", 2019 , Leuven, Belgium
https://www.cosic.esat.kuleuven.be/events/industryday2018/

Editorial Board
IACR Communication in Cryptology (2024),
Mathematical Cryptology

Program Committee Member

2026 EUROCRYPT, SCN

2024 CRYPTO, 6thZKProof Workshop

2023 EUROCRYPT, ASIACRYPT, CFAIL, TPMPC

2022 TCC, CANS, TPMPC

2021 ACM CCS, WAHC, 4thZKProof Workshop, ASIACRYPT

2020 PKC, SCN, TCC, WAHC

2019 WAHC, IMACC

- SCN 2018, CANS 2016, MobiWis 2015

Grant Reviews
European Research Council (2024, 2023),
Israeli Science Foundation (2022, 2023, 2025),
NWO Talent Programme, Netherland Organization for Scientific Research (2025)

Conference Reviews : FOCS (2025), CRYPTO (2018–2022), EUROCRYPT (2016–2023), PETS2017, ASIACRYPT (2020,2019,2017), Financial Crypto 2016, TCC 2015

Journal Reviews : IEEE Transactions on Information Theory; Journal of Cryptology, IEEE Communication Letters; IEEE Transactions on Information, Forensics and Security; Journal of Algebra, Journal of Algebra and its Applications; IEEE Transactions on Communications; Design, Codes and Cryptography; INS Information Sciences; Applicable Algebra in Engineering, Communication and Computing (AAECC)

University/Department Service

Hiring Committee: Member (2024-2025)
Discrimination, Inclusion, Diversity: Delegate for the Computing Sciences Department (2024–Present)

Supervision

PhD students
Robi Pedersen, "Post-quantum cryptographic protocols", (2020 – 2024)
(*now post-doc at DTU Copenhagen*)

Internship: Daniel Morales Escalera (Universidad de Málaga) (July 2024 – September 2024)

PhD Committee Member

- Claudia Tinnirello (Dept. Mathematics, University of Trento, 2016)
- Gabriele Spini (Mathematical Institute, Leiden University, 2017)
- Jaron Skovsted Gundersen, (Dept. Mathematics, Aalborg University, 2021)
- Manuel Joao Duarte Serejo Goulao, (Departamento de Matemática Instituto Superior Técnico, Universidade de Lisboa, 2022)
- Tibauld Feneuil (Sorbonne Université, Paris, France 2023)
- Clément Ducros (Institut de Recherche en Informatique Fondamentale (IRIF), Université Paris Cité, France 2024)
- Jules Maire, (Sorbonne Université, Paris, France 2023)
- Eliana Carrozza (Institut de Recherche en Informatique Fondamentale (IRIF), Université Paris Cité, France 2025)

BSc and MSc Students

- Giorgio Dell'Immagine, "Post-quantum signatures from non-linear secret sharing", Master Thesis, Dept. Computer Science, University of Pisa, 2025.
- Antonio Maria Favuzza, Master Thesis, Bocconi University, 2025.
- Alessandro Marchioro, "Threshold signatures from VOLE", Master thesis, Dept. Mathematics, University of Padova, 2023.
- L. Sau, "Post-quantum Signatures from Zero-knowledge Arguments", Bachelor thesis, University of Pisa, Dept. Mathematics, 2022.
- F. Orrù "Key-exchange Protocols from Non-commutative Groups',' Master thesis, University of Pisa, Dept. Mathematics, 2022.
- F. Sisinni, "Isogeny-based Key-exchange in Binary Fields", Master thesis, University of Pisa, Dept. Mathematics, 2021 (*now PhD student at Department of Applied Mathematics and Computer Science, DTU Compute Copenhagen*).
- R. Zanotto, "Isogeny-based Oblivious Transfer Protocols',' Master thesis, University of Pisa, Dept. Mathematics, 2021 (*now PhD student at CISPA*).
- B. Smith "On Verifiable Document Redacting Using zk-SNARKs", Master thesis, KU Leuven, 2021.
- A. Moutarlier "Medium scale elections with post-quantum e-voting schemes" Master thesis, KU Leuven, 2020.
- T. Marchant, "GELD: Blockchain with Balances," Master thesis, KU Leuven, 2019.
- Michele Orrù, "Universal Composability, MPC and Oblivious Transfer", University of Trento, 2016 (*now Chargé de Recerche at CNRS*).

- Heng Liu, "Implementation of Dishonest Majority Multiparty Computation for Binary Circuits", Master Thesis, University of Bristol, 2015.
- Cecilia Boschini, Co-advisor, "NTWO: a post-quantum cipher", Master Thesis, University of Trento, 2014 (*now senior researcher at ETH Zurich*).

Teaching

- *Cryptography and Security* (Instructor) *2024-2025*
  Bocconi University
- *Information Theory* (Main instructor) *2023-2024*, *2024-2025*
  Bocconi University
- *Computer Science* (Main instructor) *2023-2024*, *2022-2023*
  Bocconi University
- *Post-quantum Cryptography* (Main instructor) *2021-2022*
  Dept. Mathematics, University of Pisa
- *Public-key Cryptography* (Main instructor) *November 2018*
  ESTEC - ESA (European Space Agency)
- *Advanced Methods in Cryptography* (TA) *2019-2018*, *2018-2017*
  KU Leuven, Computer Science, Mathematics, Math-Eng
- *Coding and Information Theory* (Main instructor) *2014-2015*, *2015-2016*, *2016-2017*
  Department of Computer Science, University of Bristol, UK
- *Geometry and Linear Algebra* (TA) *2008-2009*, *2009-2010*, *2010-2011*
  First-year course, Department of Mechanical Engineering, University of Pisa
- *Statistics* (Main instructor) *2008-2009*, *2009-2010*, *2010-2011*
  First-year course, Department of Mechanical Engineering, University of Pisa
- *Algebra* (TA) *2009-2010*
  First-year course, Department of Mathematics, University of Pisa
- *Coding Theory* (TA) *2006-2007*, *2007-2008*
  Department of Mathematics, University of Pisa

Referred Publications

52. Kelong Cong, Emmanuela Orsini, Erik Pohle, Oliver Zajonc, *Row Reduction Techniques for n-Party Garbling*, **CRYPTO 2025**.
51. Carsten Baum, Ward Beullens, Lennart Braun, Cyprien Guilhem, Michael Kloob, Shibam Mukherjee, Emmanuela Orsini, Sebastian Ramacher, Christian Rechberger, Lawrence Roy, Peter Scholl, *Shorter, Tighter, FAESTer: Optimizations and Improved (QROM) Analysis for VOLE-in-the-Head Signatures*, **CRYPTO 2025**.
50. Carsten Baum, Ward Beullens, Shibam Mukherjee, Emmanuela Orsini, Sebastian Ramacher, Christian Rechberger, Lawrence Roy, Peter Scholl *One Tree to Rule Them All: Optimizing GGM Trees and OWFs for Post-Quantum Signatures*, **ASIACRYPT 2024**.

49. Vincenzo Botta, Michele Ciampi, Emmanuela Orsini, Luisa Siniscalchi, Ivan Visconti, *Black-box (Efficient) Non-malleable Zero-Knowledge*, **CRYPTO 2024**.

48. Emmanuela Orsini, Riccardo Zanotto, *Simple Two-Message OT in the Explicit Isogeny Model*, **IACR Communications in Cryptology 2024** and **ArticCrypt 2025**

47. Ilaria Chillotti, Emmanuela Orsini, Peter Scholl, Barry Van Leeuwen, *Scooby: Improved multi-party homomorphic secret sharing based on FHE*, **Information and Computation 2024**.

46. Mariana Gama, Emad Heydari Beni, Emmanuela Orsini, Nigel P. Smart, Oliver Zajonc, *MPC with Delayed Parties over Star-Like Networks*, **ASIACRYPT 2023**.

45. Carsten Baum, Lennart Braun, Cyprien Delpech de Saint Guilhem, Michael Klooß, Emmanuela Orsini, Lawrence Roy, Peter Scholl, *Publicly Verifiable Zero-Knowledge and Post-Quantum Signatures from VOLE-in-the-Head*, **CRYPTO 2023**.

44. Lennart Braun, Cyprien Delpech de Saint Guilhem, Robin Jadoul, Emmanuela Orsini, Nigel P. Smart, Titouan Tanguy, *ZK-for-Z2K: MPC-in-the-Head Zero-Knowledge Proofs for* Z_{2^k}, **IMACC 2023**.

43. Michele Ciampi, Emmanuela Orsini, Luisa Siniscalchi, *Four-Round Black-Box Non-Malleable Schemes from One-Way Permutations*, **TCC 2022**.

42. Cyprien Delpech de Saint Guilhem, Emmanuela Orsini, Titouan Tanguy, Michiel Verbauwhede, *Efficient Proof of RAM Programs from Any Public-Coin Zero-Knowledge System*, **SCN 2022**.

41. Ilaria Chillotti, Emmanuela Orsini, Peter Scholl, Nigel Smart and Barry Van Leeuwen, *Scooby: Improved Multi-Party Homomorphic Secret Sharing Based on FHE*, **SCN 2022**.

40. Carsten Baum, Robin Jadoul, Emmanuela Orsini, Peter Scholl, Nigel P. Smart, *Feta:Efficient Threshold Designated-Verifier Zero-Knowledge Proofs*, **ACM CCS 2022**.

39. Carmit Hazay, Emmanuela Orsini, Peter Scholl, Eduardo Soria-Vazquez, *Efficient MPC from Syndrome Decoding*, **Journal of Cryptology**, 2022 .

38. Sai Sheshank Burra, Enrique Larraia, Jesper Buus Nielsen, Peter Sebastian Nordholt, Claudio Orlandi, Emmanuela Orsini, Peter Scholl, Nigel P. Smart, *High Performance Multi-Party Computation for Binary Circuits Based on Oblivious Transfer*, **Journal of Cryptology**, 34(3), 2021.

37. Cyprien Delpech de Saint Saint Guilhem, Emmanuela Orsini, Titouan Tanguy, *Limbo: Efficient Zero-knowledge MPCitH–based Arguments*, **ACM CCS 2021**.

36. Jan-Pieter D'Anvers, Emmanuela Orsini, Frederik Vercauteren, *Error Term Checking: Towards Chosen Ciphertext Security without Re-encryption*, **APKC 2021**.

35. Carsten Baum, Cyprien Delpech de Saint Guilhem, Daniel Kales, Emmanuela Orsini, Peter Scholl, Greg Zaverucha, *Banquet: Short and Fast Signatures from AES*, **PKC 2021**.

34. Aner Ben-Efraim, Kelong Cong, Eran Omri, Emmanuela Orsini, Nigel P. Smart, Eduardo Soria-Vazquez, *Large Scale, Actively Secure Computation from LPN and Free-XOR Garbled Circuits*. **EUROCRYPT 2021**. Full version available as eprint Report 2021/120.

33. Karim Baghery, Cyprien Delpech de Saint Guilhem, Emmanuela Orsini, Nigel P. Smart, Titouan Tanguy, *Compilation of Function Representations for Secure Computing Paradigms*, **CT-RSA 2021**. Full version available as eprint Report 2021/195.

32. Emmanuela Orsini, *Efficient, Actively Secure MPC with a Dishonest Majority: a Survey*, International Workshop on the Arithmetic of Finite Fields, **WAIFI 2020**.

31. Cyprien Delpech de Saint Guilhem, Emmanuela Orsini, Christophe Petit, Nigel P. Smart, *Semi-Commutative Masking: A Framework for Isogeny-based Protocols, with an Application to Fully Secure Two-Round Isogeny-based OT*, **CANS 2020**. Full version available as eprint Report 2018/648.

30. Carsten Baum, Emmanuela Orsini, Peter Scholl, Eduardo Soria-Vazquez, *Efficient Constant-Round MPC with Identifiable Abort and Public Verifiability*, **CRYPTO 2020**. Full version available as eprint Report 2020/767.

29. Emmanuela Orsini, Nigel P. Smart, Frederik Vercauteren, *Overdrive2k: Efficient Secure MPC over Z_{2k} from Somewhat Homomorphic Encryption*, **CT-RSA 2020**. Full version available as eprint Report 2019/153.

28. Abdelrahaman Aly, Emmanuela Orsini, Dragos Rotaru, Nigel Smart, Tim Wood *Zaphod: Efficiently Combing LSSS and Garbled Circuits in SCALE*, In **CCS@WAHC 2019**.

27. Cyprien Delpech de Saint Guilhem, Lauren De Meyer, Emmanuela Orsini, Nigel P. Smart, *BBQ: Using AES in Picnic Signatures*, In **SAC 2019**. Full version available as eprint Report 2019/781.

26. Carmit Hazay, Emmanuela Orsini, Peter Scholl, Eduardo Soria-Vazquez *Concretely Efficient Large-Scale MPC with Active Security (or, TinyKeys for TinyOT)*, **ASIACRYPT 2018**. Full version available as eprint Report 2018/843.

25. Carmit Hazay, Emmanuela Orsini, Peter Scholl, Eduardo Soria-Vazquez, *Efficient MPC from Syndrome Decoding (or: Honey, I Shrunk the Keys)*, **CRYPTO 2018**. Full version available as eprint Report 2018/208.

24. Martin R. Albrecht, Emmanuela Orsini, Kenneth G. Paterson, Guy Peer, Nigel P. Smart, *Tightly Secure Ring-LWE Based Key Encapsulation with Short Ciphertexts*, **ESORICS 2017**. Full version available as eprint Report 2017/354.

23. Fabrizio Caruso, Emmanuela Orsini, Massimiliano Sala, Claudia Tinnirello, *On the shape of the general error locator polynomial for cyclic codes*, In **IEEE Transactions on Information Theory**, 63(6): 3641-3657, 2017. Preprint available as CoRR abs/1502.02927.

22. Marcel Keller, Emmanuela Orsini, Dragos Rotaru, Peter Scholl, Eduardo Soria- Vazquez and Srinivas Vivek, *Faster Secure Multi-Party Computation of AES and DES Using Lookup Tables*, **ACNS 2017**: 229-249. Full version availaible as eprint Report 2017/378.

21. Michele Orrù, Emmanuela Orsini, Peter Scholl, *Actively Secure 1-out-of-N OT Extension with Application to Private Set Intersection*, In **Topics in Cryptology - CT-RSA 2017**: 381-396. Full version availaible as eprint Report 2016/933.

20. Marcel Keller, Emmanuela Orsini, Peter Scholl *MASCOT: Faster Malicious Arithmetic Secure Computation with Oblivious Transfer*, **ACM Conference on Computer and Communications Security - CCS 2016**: 830-842. Full version availaible as eprint Report 2016/505.

19. Carsten Baum, Emmanuela Orsini, Peter Scholl *Efficient Secure Multiparty Computation with Identifiable Abort* In **Theory of Cryptography, TCC-B 2016**: 461-490. Full version available as ePrint Report 2016/187.

18. Ashish Choudhury, Emmanuela Orsini, Arpita Patra, Nigel P. Smart, *Linear Overhead Optimally-Resilient Robust MPC Using Preprocessing*, **Security and Cryptography for Networks, SCN 2016**: 147-168. Full version available as ePrint Report 2015/705 .

17. Joop van de Pol, Emmanuela Orsini, Nigel P. Smart, *Bootstrapping BGV Ciphertexts With A Wider Choice of p and q*, in **IET Information Security** (invited) 10(6): 348-357, 2016.

16. Tore Kasper Frederiksen, Marcel Keller, Emmanuela Orsini, Peter Scholl, *A Unified Approach to MPC with Preprocessing using OT*, In **Advances in Cryptology - ASIACRYPT 2015**: Volume 1, pag. 711-735. Full version available as ePrint Report 2015/901.

15. Marcel Keller, Emmanuela Orsini, Peter Scholl, *Actively Secure OT Extension with Optimal Overhead* In **Advances in Cryptology - CRYPTO 2015**: Volume 1, pag. 724-741. Full version available as ePrint Report 2015/646 .

14. Cecilia Boschini, Emmanuela Orsini, Carlo Traverso, *Betweeen Codes and Lattices: Hybrid lattices and the NTWO cryptosystem* In **Effective Methods in Algebraic Geometry - MEGA 2015**.

13. Joop van de Pol, Emmanuela Orsini, Nigel P. Smart, *Bootstrapping BGV Ciphertexts With A Wider Choice of p and q*, In **Public Key Cryptography - PKC 2015**: pag. 673-698. Full version available as ePrint Report 2014/408.

12. Enrique Larraia, Emmanuela Orsini, Nigel P. Smart, *Dishonest Majority Multi-Party Computation for Binary Circuits*, In **Advances in Cryptology - CRYPTO 2014**: Volume 2, pag. 495-512. Full version available as ePrint Report 2014/101.

11. A. Choudhary, E. Orsini, A. Patra and J. Loftus and N.P. Smart, *Between a Rock and a Hard Place: Interpolating Between MPC and FHE*, **Advances in Cryptology - ASIACRYPT 2013**: Volume 2, pag. 221-240. Full version available as ePrint2013/085.

10. Chiara Marcolla, Emmanuela orsini, Massimiliano Sala, *Improved decoding of affine-variety code*
In **Journal of Pure and Applied Algebra**, Vol. 216, Issue 7, July 2012, pp. 1533-1565.

9. Eleonora Guerrini, Emmanuela Orsini, Massimilaino Sala, *Computing the distance of some nonlinear code* **Journal of Algebra and Its Applications**, Volume 9, No. 1 (2010), 1-16.

8. Emmanuela Orsini, Carlo Traverso, *The LPC signature* In **Second International Conference on Symbolic Computation and Cryptography - SCC2 2010**, Royal Holloway, London, UK, pages 129-135, 2010.

7. Teo Mora, Emmanuela Orsini, *Decoding Cyclic Codes* In **Mathematical Methods in Computer Science - MMICS 2008**, Karlsruhe, Germany, December 17-19.

6. Daniel Augot, Emanuele Betti, Emmanuela Orsini, *An introduction to linear and cyclic code*, In **Gröbner Coding and Cryptography**, RISC Book Series, Springer, 2009, pp. 47-68.

5. Teo Mora, Emmanuela Orsini, *Decoding cyclic codes: the Cooper philosophy*
In **Gröbner Bases, Coding, and Cryptography, Coding and Cryptography**, RISC Book Series, Springer, 2009, pp. 69-91.

4. Eleonora Guerrini, Emmanuela Orsini, Ilaria Simonetti, *An algorithm for the distance distribution of systematic nonlinear code*, In **Gröbner Bases, Coding, and Cryptography**, RISC Book, Springer, Heidelberg pp. 367- 372.

3. Emmanuela Orsini, Massimiliano Sala, *General error locator polynomials for binary cyclic code with* $n < 63$ *and* $t \leq 2$, In **IEEE Transactions on Information Theory**, 2007, pp.1095-1107, Vol. 53, No 3.

2. Emmanuela Orsini, Massimilano Sala, *An algebraic decoding algorithm for binary cyclic codes* **Effective Methods in Algebraic Geometry - MEGA 2005**, Alghero, Sardinia, Italy .

1. Emmanuela Orsini, Massimilano Sala, *Correcting errors and erasures via the syndrome variety*, In **Journal of Pure and Applied Algebra**, Vol. 200, 1-2, August 2005, pp. 191-226.

Selected Invited Talks

- *VOLE-based Zero-knowledge Schemes*
Plenary Talk, French National Days of Security, Caen, June 23-25, 2025.
- *VOLE-based Zero-knowledge and Signature Schemes*
On the Mathematics of post-quantum crypotgraphy and spering meetings, Irchel Campus, University of Zurich, June 2-6, 2025
- *Secret-sharing for MPC*
Workshop on Secret-sharing, Girona, Spain, May 12-14, 2025
- *Introduction to MPC and SPDZ protocols*
ISCwsISC (The Third ISC WInter School on Information Security and Cryptology), February 2023.

- *Lattice-based cryptography*
  PQCifris 2022, Trento, Italy.

- *Data Protection Frontiers: MPC, FHE and more*
  Summer School on Security and Privacy in the (golden) Age of AI, Leuven, 2022.

- *Recent progress in MPCitH protocols*
  4th Annual ZKProof Workshop, April 2021.

- *Post-quantum secure oblivious transfer*
  Seminari per il gruppo UMI, Unione Matematica Italiana, Crittografia e Codici, April 2021.

- *Efficient Actively Secure OT Extension: 5 Years Later*
  NIST Workshop on Multi-Party Threshold Schemes 2020, November 2020.

- *Secure Multi-party Computation - An algebraic perspective*
  International Workshop on the Arithmetic of Finite Fields WAIFI 2020, July 2020, Rennes, France.

- *Efficient Evaluation of Symmetric Primitives in MPC*
  Fewer Multiplications in Cryptography - FewMult 2017, Jussieu campus of Université Pierre et Marie Curie, Paris. Affiliated event with Eurocrypt 2017.

- *Efficient Multi-party Computation with Oblivious Transfer*
  Department of Computer Science, Royal Holloway, University of London, January 2107.

- *Actively secure OT-extension and applications*
  Department of Computer Science, University of Salerno, July 2015.

- *Bootstrapping BGV Ciphertexts With A Wider Choice of p and q*,
  Department of Computer Science, University of Surrey, UK, March 2015.

- *Post-quantum cryptography*
  La crittografia del quotidiano e le frontiere della crittografia
  Presidenza del Consiglio dei Ministri (Prime Minister's Office), Rome, Italy, May 2014.

- *Altre alternative ad RSA*,
  Department of Mathematics, University of Torino, Italy.
  Workshop: "Crittografia a chiave pubblica: oltre RSA", May 2011.

- *Hybrid lattices and the NTWO cryptosystem*
  I Workshop of Cryptography BunnyTN 2011
  Department of Mathematics, University of Trento, Italy, March 2011.

- *Lattice Gröbner bases and lattice problems*,
  eRISC Séminaire
  Université de la Méditerrané, Campus de Luminy, Marseille, France, March 2011.

- *Lattice Gröbner bases, SVP and Lattice Polly Cracker Signature*, **Seminaire Algo**, Université de Caen, France, December 2010.

- *On the structure of the syndrome variety*
  S3CM, **Soria Summer School on Computational Mathematics**, Soria, Spain, July 2008.

Languages

Italian native speaker and fluent in English.