Curriculum Vitae

Emmanuela Orsini

✉ emmanuela.orsini@unibocconi.it
https://cseao.github.io/

Current position

Tenure-Track Assistant Professor — February 2023-present
Department of Computing Sciences, Bocconi University, Milano, Italy.

Education

Ph.D. in Mathematics and Statistics for Computational Sciences — January 2008
Department of Mathematics, University of Milano, Italy.
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 for LDPC codes*
Advisor: Ing. Devis Gatti (STMicroelectronic, Milano)

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

Other qualifications

- Qualification aux fonctions de maître de conférences en Informatique (France) — 2011
- Qualification aux fonctions de maître de conférences en Mathématique (France) — 2011

Past academic positions

Research Expert (permanent position) — Jan 2018 – January 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 — December 2010 – December 2011
Department of Mathematics
Università degli Studi di Trento

Postdoctoral Researcher — Jan 2008 – Sept 2010
Department of Mathematics
Università degli Studi di Pisa

Research grants

Title: Fromager – Verify and Evaluate Software with Zero-Knowledge of its Source Code
Program: DARPA Securing Information for Encrypted Verification and Evaluation (SIEVE)
Role: KU Leuven Subcontract to GALOIS Inc. (KU Leuven PI)
Amount: $913.336,00
Project duration: 30/04/2020 – 29/04/2024
Project description: SIEVE aims to develop computer science theory and software that can generate mathematically verifiable statements that can be shared publicly without giving sensitive information away. Under the program, researchers will explore the creation of verifiable public statements about software, general computations, as well as social-technical interactions.

Title: MOZAIK – Scalable and Secure Data Sharing
Program: FWO Strategic Basic Research (SBO) from Research Foundation Flanders
Role: Project team member
Amount: 1.261.734,00 (euro)
Project duration: 31/03/2021 – 30/03/2025
Project description: Through the use of various PETs and distributed computation, MOZAIK mainly aims to research and develop: 1) a secure and privacy-friendly distributed IoT-data collection and analytics system; 2) an on-demand platform to support businesses and sectors to access expertise, knowledge, algorithms and tools on privacy and security enhancing technologies; 3) a hybrid personal and non-personal data sharing marketplace which complies with prevailing legislation and allows data owners to remain in control of their data and its subsequent use.

Title: COED – Computing on Encrypted Data
Program: Collective Research & Development and Collective Knowledge Dissemination/Transfer (COOCK), Research Foundation Flanders
Role: co-PI
Amount: 325.000,00 (euro)
Project duration: 12/01/2020 – 11/31/2022
Project description: Enabling data processing on encrypted data, so that personal, sensitive and reliable data can be used securely in AI applications.

Services to the Scientific Community

Program committees :

- EUROCRYPT 2023
- TCC 2022, CANS 2022, TPMPC 2022
- ACM CCS 2021, WAHC 2021, 4thZKProof Workshop, ASIACRYPT 2021.
- PKC 2020, SCN 2020, TCC 2020, WAHC 2020
- WAHC 2019, IMACC 2019
- SCN 2018, CANS 2016, MobiWis 2015

External reviewer : CRYPTO (2021,2020,2019,2018), EUROCRYPT (2022,2021,2020,2019,2018,2017,2016), PETS2017, ASIACRYPT (2020,2019,2017), Financial Crypto 2016, TCC 2015; IEEE Transactions on Information Theory; Journal of Cryptology, IEEE Communication Letters; IEEE Transactions on Information, Forensics and Security; IEEE Transactions on Communications; Design, Codes and Cryptography;

INS Information Sciences; Applicable Algebra in Engineering, Communication and Computing (AAECC)

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)

Organizer: Workshop " Computation on Encrypted Data Industry Day", 2019 , Leuven, Belgium https://www.cosic.esat.kuleuven.be/events/industryday2018/

Students

Supervision PhD students: (2020 –) Robi Pedersen, "Post-quantum cryptographic protocols" (co-advisor with Fre Vercauteren)

Supervision BSc and MSc students:

- 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.
- 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.

Teaching

- *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.

- *Coding Theory and Cryptography* (TA) 2005-2006
  Department of Mathematics, University of Milano-Bicocca

NIST Post-quantum standardization submissions

- 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/`.

Publications

Referred journals, conferences (with proceedings) and book chapters

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

40. 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**.

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

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

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

36. 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.

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

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

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

32. 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.

31. 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.

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

29. 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.

28. 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.

27. 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.

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

25. 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.

24. 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.

23. 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.

22. 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.

21. 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.

20. 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.

19. 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.

18. 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.

17. 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.

16. 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 .

15. 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.

14. 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.

13. 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 .

12. 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.

11. 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.

10. 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.

9. 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.

8. 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.

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

1. Emmanuela Orsini, *New decoding algorithm for cyclic code*,
In **Proceeding of Miriam Workshop**, Industrial Days 2003-2004, Milano, Volume 2, pp. 62-65, June 2005.

Referred conferences (without proceedings)

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

2. 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.

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

Selected Invited Talks

- *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, September 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.