CURRICULUM VITAE
Formato Europeo/European Format
(2005-present)

Personal information

Name / Surname	**Marco Pedicini**
Address	Department of Mathematics and Physics, Roma Tre University, Largo San Leonardo Murialdo 1 – 00146 Rome, Italy
Personal Email	mailto:marco.pedicini@uniroma3.it
Website	http://www.mat.uniroma3.it/users/pedicini

Current Position

(2012-present)	Associate Professor (full time).
SSD	MATH-01/A Logica Matematica

Research Topics/Experiences

My research interests focus on themes at the crossroad of logic and theoretical computer science. In particular, my work spans the fields of Proof Theory in Computer Science, Computational Methods for Systems Biology, Computational Number Theory, Cryptography and Cryptanalysis. Albeit this whole activity falls in the area of Theoretical Computer Science, it achieves in interdisciplinary research its own specificity. Interactions with other disciplines are the key to evaluating my activity. I developed a special kind of expertise while linking theoretical results with practical issues in the development of advanced applications for computer science.

Scientific/Technical Qualification

(Scopus 2026)	h-index: 9, No. publications: 41, No. citations: 328
(Google Scholar 2026)	h-index: 13, No. publications: 54, No. citations: 604

Thematic Area Keywords

Logic	Computational Logic, Computability, Proof Theory, Linear Logic, Geometry of Interaction
Cryptography	Cloud Cryptography, Cryptanalysis of Symmetric Systems
Specific to Digital Transition Programme	Cryptography, Privacy Preserving Machine Learning, Cloud Computing, High Performance Computing, Quantum Computing.

Education and Training

(1999)	PhD (date of defence 15 January 1999), at Equipe de Logique Mathématique of the University Paris 7 (France), title of thesis *Exécution et Programmes*, thesis supervisor J.-Y. Girard;
(1992)	DEA Logique et Fondements de l'Informatique, at University Paris 7, title of the master degree memory: *Schémas Principaux et Réseaux de Preuves*, supervisor J. van de Wiele;
(1991)	Laurea of Mathematical Sciences at University of Rome "La Sapienza", title of the "tesi di laurea": *Lambda Calcolo Puro, Reti di Dimostrazione e Riduzione di Testa*, thesis supervisor C. Böhm co-supervisor G.F. Mascari.

Work Experience

(2022 – present) ASSOCIATE PROFESSOR of Mathematical Logic (MATH-01/A previously SSD MAT/01) Roma Tre University ("Nota CUN" on 13/9/2022 and "Decreto Rettorale" n. 96682 on 19/09/2022),

(2012 – 2022) ASSOCIATE PROFESSOR of Computer Science (SSD INF/01) Roma Tre University (selection published on Gazzetta Ufficiale n. 32 of 22/04/2008, qualification registered on Dean Act 29/10/2010);

(1992-2012) CNR-RESEARCHER, CNR registration number n. 00015, level III, Istituto per le Applicazioni del Calcolo "Mauro Picone", Roma;

Main Roles and Responsibilities

(2024 – present) MEMBER of the Editorial Board of *Journal of Mathematical Cryptology*;

(2023 – present) MEMBER of the doctoral school, Dept. Mathematics and Physics, Roma Tre University;

(2023 – present) MEMBER and DEPUTY DIRECTOR of the Scientific Committee of De Componendis Cifris Association;

(2019 – present) MEMBER of the Advisory Board "De Componendis Cifris" – Roma Tre University Member;

(2019 – present) MEMBER of the Scientific Committee in the Book Series "Cryptography" Aracne Publisher;

(2022-present) MEMBER of the Scientific board for the postgraduate course Data Analytics, Roma Tre University

(2024-2025) SCIENTIFIC COORDINATOR of the research activity on "Quantum Randomness and Post-Quantum Cryptography " among E4 - Computer Engineering s.p.a. and Dept. of Mathematics and Physics, Roma Tre University.

(2019 – 2022) MEMBER of the doctoral school, Dept. Mathematics and Physics, Roma Tre University;

(2022) SCIENTIFIC COORDINATOR of the activity on "Formal representation and reasoning on algorithms" contract with Epigenesys srl and Dept. of Mathematics and Physics of Roma Tre University.

(2021-2022) COORDINATOR of four editions of the Course "Fondamenti e Applicazioni della Tecnologia Blockchain" organised as Dept. of Mathematics and Physics, Roma Tre University and offered to Banca d'Italia.

(2021-2022) SCIENTIFIC COORDINATOR of the joint research activity on "Complex Networks" among CNR-IAC and Dept. of Mathematics and Physics, Roma Tre University.

(2010-2013) SCIENTIFIC CONSULTANT of E-Security srl for Supercomputer Project XASMOS - distributed infrastructure for computer security;

(2008-2009) MEMBER of the doctoral school, Dept. Mathematics, Roma Tre University;

(2003-2005) CHIEF OF SCIENTIFIC ORGANIZATION of Araknos srl (Via Boezio 6, Rome), company specialised in computer security; I was involved in activities on Open Source Software, and in supporting the definition of research projects concerning computer security.

(2004-2011) CONSULTANT of Stato Maggiore della Difesa, Centro Intelligence Interforze.

Main Research Experience

(2024-2025) PRINCIPAL INVESTIGATOR of the Roma Tre unit of the Project "Advanced and Quantum-safe Solutions for Digital Identity and digital Tracing" (AQuSDIT) in the Program PE SERICS - SEcurity and RIghts in the CyberSpace (SERICS) (codice PE000000014 - CUP SERICS - SPOKE 5) CRYPTOGRAPHY AND DISTRIBUTED SYSTEMS SECURITY PNRR Missione 4 - Componente 2 - Investimento 1.3 Finanziato dall'Unione europea - NextGenerationEU2 CODICE CUP: H73C22000880001 (2024-2025).

(2024-2025) PRINCIPAL INVESTIGATOR for the *incarico per la realizzazione di Multi-party Computation specializzati nella teoria dei Numeri* n. CIG: 9958090BD2, by Fondazione Bruno Kessler, Trento (2024-2025).

(2020-2023) PRINCIPAL INVESTIGATOR of Subcontract "Modellazione computazionale nei sistemi biologici" of Workpackage 5 "Modelling and Simulation" of H2020-JTI-IMI2- "ERA4TB - European Tuberculosis Regimen Accelerator" (GA n. 85398);

(June 2019) VISITING PROFESSOR, Scuola Normale Superiore di Pisa;

(March-April 2019) VISITING PROFESSOR, Simons Institute for the Theory of Computing, Berkeley University;

(2012-2016) PRINCIPAL INVESTIGATOR of Research Unit at Roma Tre University of the Project MIUR-PRIN2010-2011, Metodi logici per il trattamento dell'informazione;

(2013-2016) PARTICIPANT to the Project UE Strep FP7-ICT-2011-9 (MISSION-T2D) – Multiscale Immune System SImulator for the Onset of Type 2 Diabetes integrating genetic, metabolic and nutritional data;

(2010-2012) PRINCIPAL INVESTIGATOR of the section "INT.P01.007.006 *Applied cryptography: analysis and performance of cryptographic primitives*", Istituto per le Applicazioni del Calcolo in the sub-project "INT.P01.007 Trustworthy and Secure Future Internet" of the CNR National Project "INT.P01 Security";

(2008-2010) PRINCIPAL INVESTIGATOR of Research Unit at IAC-CNR of the Project (MIUR-PRIN2007) "CONCERTO: Controllo e certificazione dell'uso delle risorse";

(2007-2009) PARTICIPANT, Project EUFP6/2005/NEST-PATH Contract No IST-2006-043241 (Complexdis) "Unravelling complex diseases with complexity theory: from networks to the bedside";

(2006-2007) PRINCIPAL INVESTIGATOR (for the italian part) of the CNR/CNRS Project "Interaction and Complexity" (O. Laurent was the french principal investigator).

(2005-2006) PARTICIPANT, Project "FOLLIA: Fondazioni Logiche di Linguaggi Astratti di Programmazione" (MIUR-COFIN2005);

Conference and Workshop Communications

Since 1992, I taught more than 50 conference lectures, in particular as a speaker in:

(2025) Varese (IT), Conference Optimal Control and Inverse Problems in PDE Theory June, 9 - 13 - Villa Toeplitz, Varese, Riemann International School of Mathematics: *An Object-Oriented Approach to Idempotent Analysis: Integral Equations as Optimal Control Problems*;

(2025) Rome (IT), Meeting Proof, Argumentation, Computation, Modalities And Negation (PACMAN2025) May, 14 - 16 - Rome (Italy), Roma Tre University: *Proof Theory, and Cryptography: Reasoning About the Uncomputable*;

(2024) Udine, (IT), AILA2024 Meeting, I gave a talk on a joint work with Mario Piazza: *Geometry of interaction and non-determinism*;

(2024) Recife, (BR), Departamento de Matemática, Universidade Federal de Pernambuco. Recife Meeting on Mathematics, I gave a talk on a joint work with Paola Loreti and Vilmos Komornik: *Expansions in non-integer bases: Fibonacci expansions, a quasi-ergodic approach and Kakeya's method*;

(2020) Sharjah, (UAE), American University of Sharjah, Third International Conference of Mathematics and Statistics (AUS-ICMS'20) I gave a talk at the special session: Discrete Dynamic Modeling of Biological Systems on *Compositionality in the Boolean Model of Regulatory Networks*;

(2019) Rome, (IT), Casa dell'Aviatore in Rome, Conference "Crittografia e Crittotecnologie" organised by AFCEA - Rome and De Componendis Cifris. I gave a talk *Cryptography and cryptotechnologies*;

(2018) Roma, (IT), Roma Tre University, I gave a talk at the meeting "De Componendis Cifris incontra Roma": *Cosa la crittografia può fare per la privacy nell'ambito dei big data*;

(2018) Roma, (IT), Sapienza University of Rome, XIV Biennial Conference of the Italian Society of Applied and Industrial Mathematics, I gave a talk at the MS-27: Discrete Mathematics, Number Theory and Applications to Control : *Quantum entanglement and the Bell matrix*, joint work with Anna Chiara Lai, Silvia Rognone;

(2018) Roma, (IT), Sapienza University of Rome, XIV Biennial Conference of the Italian Society of Applied and Industrial Mathematics, I gave a talk at the MS-30: Modeling, Simulation and Data Analysis for Sport : *Hypothesis testing in tennis game point scoring*, joint work with Stefano Baraldo, Mirco Ieraci and Massimiliano Mollica;

(2018) Bologna, (IT), Università degli Studi di Bologna, PIHOC2018, Workshop on Probabilistic Interactive and Higher-Order Computation, I presented a joint work with Mario Piazza: *Stream abstract machines. parallel and non-deterministic execution* `http://pihoc2018.cs.unibo.it`

(2018) Roma, (IT), Roma Tre University, Meeting of the "DE COMPONENDIS CIFRIS" Association, I presented Roma Tre University cryptography activities: *Crittografia al Dipartimento di Matematica e Fisica di Roma Tre* `http://www.decifris.it/index_gennaio2018.html`

(2017) Padova, (IT), Università degli Studi di Padova, XXVI incontro dell'Associazione Italiana di Logica e sue Applicazioni, I presented a joint work with Mario Piazza: *Stream abstract machines. parallel and non-deterministic execution* `https://events.math.unipd.it/aila2017/`

(2017) Venice, (IT), European Centre for Living Technology, Universit!à Ca' Foscari, I presented a joint work with Maria Concetta Palumbo and Filippo Castiglione: *Attractors in synchronous and asynchronous genetic regulatory networks* `http://wivace.org/2017/index2017.html`

(2016) Prague, (CZ), Czech Technical University in Prague, Conference Numeration 2017 – I presented a joint work with Vilmos Komornik: *Critical Bases for Ternary Alphabets;*.

(2016) Bologna, (IT), Department of Computer Science, University of Bologna, First General Meeting of the Linear Logic GDRI – I presented a joint work with Anna Chiara Lai and Mario Piazza: *Abstract Machines, Optimal Reduction, and Streams*.

(2015) Sharjah, (UAE), American University of of Sharjah, Second International Conference on Mathematics and Statistics (AUS-ICMS '15), I presented a joint work with Maria Concetta Palumbo, Filippo Castiglione and Daniele Santoni: *A multi-threaded algorithm for finding attractors in synchronous and asynchronous genetic regulatory networks*.

(2015) Rome, (IT), Roma Tre University, Workshop: Proof and Types 25 years later, I presented a joint work with Mario Piazza: *Sequential and Parallel Abstract Machines for Optimal Reduction*.

(2014) Debrecen, (HU), University of Debrecen, Faculty of Informatics, Workshop Numeration and Substitutions, I presented the joint work with Vilmos Komornik and Anna Chiara Lai: *Generalized golden ratios in ternary alphabets*

(2014) Rome, (IT), University of Rome "La Sapienza", Controllability and networks, Conference in honour of the 60th birthday of Vilmos Komornik, title of the work *An algorithmic view of non-integer basis developments*

(2014) Soesterberg, (NL), Utrecht University, TFP 2014: 15th Symposium on Trends in Functional Programming joint work with Giulio Pellitta and Mario Piazza, title: *Sequential and Parallel Abstract Machines for Optimal Reduction*

(2013) Bertinoro, CEUB - University of Bologna, FOPARA 2013, joint work with Daniele Canavese, Emanuele Cesena, Rachid Ouchary and Luca Roversi, title: *Can a light typing discipline be compatible with efficient implementation of finite field inversion ?*

(2011) Perth, Curtin University, Australasian Information Security Conference, joint work with Andrea Agnesse, title : *Cube attack in finite fields of higher order*.

(2008) Marseille, CIRM – Luminy, Workshop Discrete models of biological networks : from structure to dynamics, joint work with Filippo Castiglione and Daniele Santoni, title : *Implementation of a regulatory gene network to simulate the TH1/2 differentiation in an agent-based model of hypersensitivity reactions*.

(2008) Prague, 2008, Doppler Institute, Czech Technical University, Workshop Journèes Numèration, joint work with Vilmos Komornik and Anna Chiara Lai, title: *Critical constants for unique expansions in general alphabets*.

(2007) Siena, Univ. di Siena, Conference Computation and Logic in the Real World, CiE 2007, joint work with Mario Piazza, title: *Elementary Complexity into the Hyperfinite* II_1 *Factor*.

(2007) Paris, 2007, Univ. Paris 7, Workshop Aspects dynamiques de la numération, joint work with Anna Chiara Lai, title : *Ergodic properties of greedy expansions*.

(2005) Lisbon, Univ. di Lisbona, Workshop Developments in Computational Models (DCM 2005), satellite event of ICALP 2005, title : *Supporting function calls within PELCR*.

Service to National and International Community

(2024 - present) Member of the Editorial Board of the *Journal of Mathematical Cryptology*;

(2026) Co-organiser with Lorenzo Grassi (Eindhoven University of Technology) of the Workshop SPRING2026 (Workshop on Symmetric Primitives over prime fields and integer RINGs), May 10, 2026, affiliated event of the IACR Eurocrypt 2026 Conference.

(2025) General Co-chair with Lorenzo Grassi (Eindhoven University of Technology) of IACR FSE 2025 (Fast Software Encryption), 17–21 March 2025, at Roma Tre University.

(2025) Member of the organising team of the Workshop on Symmetric-Key Cryptanalysis Automation and Modelling (SKCAM) 15 March 2025, at Roma Tre University.

(2025) Member of the organising team of the Workshop on Cryptanalysis of Algebraic Hash Functions (CAHF) 16 March 2025, at Roma Tre University.

(2025) Organising Committee of the Spring School on Symmetric-Key Cryptanalysis 10–14 March 2025, at Roma Tre University.

(2023) Co-organiser with Massimiliano Sala (University of Trento) and Giulia Cavicchioni (University of Trento) of CIFRIS24, Frascati (Rome) 25-27 September 2024 at the Center Donato Menichella of Banca d'Italia.

(2024) Co-chair with Dr. Michela Iezzi and Dr. Matteo Nardella (ART, Banca d'Italia) of the Workshop Cloud Cifris 24 at CIFRIS24, Rome 27 September 2024, at the Center Donato Menichella of Banca d'Italia.

(2023) Organiser and Member of the Scientific Committee of the *Workshop Privacy-Preserving Machine Learning*, affiliated event of CIFRIS23;

(2022) Organiser and Member of the Scientific Committee of the *Workshop on Privacy Preserving systems, software and tools*, at the Laboratory of Cryptography and Cybersecurity of the Department of Mathematics and Physics, Roma Tre University;

(2020) Organiser and Member of the Program Committee with Prof. A. Visconti and Prof. R. La Scala of the Tutorial Workshop at ITASEC20: "Cryptanalysis: A Key Tool in Securing and Breaking Ciphers";

(2017) Organiser and Program Chair of the International Workshop "Numeration 2017", in Rome (Department of Mathematics and Physics, Roma Tre University) 5-9 June 2017;

(2008) Organiser and Member of the Program Committee with Prof. V. Komornik (University of Strasbourg) and Prof. P. Loreti (University of Rome La Sapienza) of the International Workshop "Dynamical Aspects in Number Systems", in Rome (CNR Headquarters) 6-7 February 2008;

(2006) Organiser and speaker of Introductory Course to Cryptography and digital signature (10 lectures delivered to the computer systems service of Segretariato Generale della Presidenza della Repubblica, in Rome (Palazzo del Quirinale) 27 - 28 February 2006.

Teaching Experience

Most of my teaching activity was at Roma Tre University, Department of Mathematics:

(2022-2026) Quantum Computing (undergraduate course) (main instructor);

(2021-2022) Towards Information Theory, Neural Networks and beyond (graduate course) (main instructor);

(2017-2026) Computability and Complexity (undergraduate course) (main instructor);

(2010-2026) Algorithms for Cryptography (undergraduate course) (main instructor);

(2017-2018) Programming Languages (undergraduate course) (main instructor);

(2001-2017) Models of Computation (undergraduate course) (main instructor);

(2008-2016) Computational Journalism (undergraduate course) (main instructor);

(2007-2017) Information Theory (undergraduate course) (main instructor);

(2012-2013) Advanced Java Programming (undergraduate course) (main instructor);

(2008-2009) Fundamentals of Computer Science (undergraduate course) (main instructor);

(2004) Computational Models in Systems Biology (graduate course) (main instructor);

(2002-2004) Applied Cryptography (undergraduate course) (main instructor);

(2000-2005) Computer Literacy (undergraduate course) (main instructor);

(2000) Programming Laboratory (undergraduate course) (main instructor).

Honours, Awards, Memberships, Other Qualifications

(2013 – 2026) ASN National Scientific Qualification as Full Professor in 01/A1;

(2012 – present) Research Associate in Computer Science of Italian CNR at Istituto per le Applicazioni del Calcolo "Mauro Picone", Roma;

(2000) Best Paper Award at the 2nd ACM-SIGPLAN International Conference on Principles and Practice of Declarative Programming (PPDP'00) for: M. Pedicini and F. Quaglia, "A Parallel Implementation for Optimal Lambda-Calculus Reduction";

(1993 – present) MEMBERSHIP of AILA (Associazione Italiana di Logica e sue Applicazioni), UMI (Unione Matematica Italiana), IACR (International Association of Cryptologic Research), EMS (European Mathematical Society).

(2023) FOUNDER MEMBER of DE COMPONENDIS CIFRIS ASSOCIATION APS, Milan, Italy.

Additional Information

(1997 – present) Research and development of the software **PELCR**: this implementation permits the parallel execution of functional languages on distributed machines (PRINCIPAL INVESTIGATOR AND DEVELOPER).

Publications

(2026) KOMORNIK V, PEDICINI M (2026) Estimates of Fibonacci series. Accepted to be published on *The American Mathematical Monthly*, MAA.

(2026) DE SCLAVIS F, NARDELLI M, PEDICINI M (2026) Thresholding Post-Quantum Signatures. Accepted to be presented at CTB2026, affiliated event at Eurocrypt2026.

(2026) GASPARINI L, ONOFRI E, PALMUCCI M, PEDICINI M. (2026) Cross-primitive comparison in CP-ABE Bilinear Pairing vs. Lattices, in Journal of Mathematical Cryptology, vol. 20, no. 1, 2026, pp. 20250051 https://doi.org/10.1515/jmc-2025-0051.

(2026) BELLINI E, BRUNELLI R, GERAULT D, HAMBITZER A, PEDICINI M. (2026) Generic Partial Decryption as Feature Engineering for Neural Distinguishers. In: Escudero, D., Damgård, I. (eds) Progress in Cryptology – LATINCRYPT 2025. LNCS, vol 16129. Springer, Cham. https://doi.org/10.1007/978-3-032-06754-8_14, Cryptology ePrint Archive, Paper n. 2024/896, https://eprint.iacr.org/2025/1443.pdf.

(2025) CIMATTI A, DE SCLAVIS F, GALANO G, GIAMMUSSO S, IEZZI M, MUCI A, NARDELLI M, PEDICINI M. (2024) Dynamic-FROST: Schnorr Threshold Signatures with a Flexible Committee, *Journal of Mathematical Cryptology*, vol. **19**, no. 1, 2025, pp. 20240045. (IACR e-print archive Paper n. 2024/896).

(2025) KOMORNIK V, LORETI P, PEDICINI M. (2024) Multiple Kakeya Expansions, to appear in *Annali della Scuola Normale Superiore di Pisa, Classe di Scienze* https://doi.org/10.2422/2036-2145.202404_009 https://journals.sns.it/index.php/annaliscienze/article/view/6996/2544.

(2025) Gasparini L, Onofri E, Palmucci M, Pedicini M. (2026) Comparing Lattices and Bilinear Parings in CP-ABE, FCiR-ACTA, proceedings of Financial Cryptography in Rome 2025 (FCiR25), FCiR25 Acta in De Cifris Koine, vol. 8, pp. 81-84, (2025) De Cifris Press, November 2025 ISBN: 979-12-81863-07-1 ISSN: 3034-9796 https://doi.org/10.69091/koine/vol-8-P10

(2024) CIANFRIGLIA M, ONOFRI E, PEDICINI M. (2024) $\mathsf{mR}_{\mathsf{LWE}}$-CP-ABE: a revocable CP-ABE for Post-Quantum Cryptography, Journal of Mathematical Cryptology **18**, no. 1, 2024, pp. 20230026. https://doi.org/10.1515/jmc-2023-0026.

(2024) KOMORNIK V, LORETI P, PEDICINI M. (2024) A Quasi-Ergodic Approach To Non-Integer Base Expansions, Journal of Number Theory – **254** pp. 146 – 168 https://doi.org/10.1016/j.jnt.2023.07.009.

(2023) CIANFRIGLIA M, ONOFRI E, ONOFRI S, PEDICINI M. (2023) Fourteen Years of Cube Attacks, https://link.springer.com/article/10.1007/s00200-023-00602-w, AAECC (2023) Springer.

(2023) GIORDANI G, GRASSI L, ONOFRI S, PEDICINI M. (2023) Invertible Quadratic Non-Linear Functions over $\mathbb{F}_p^n$ via Multiple Local Maps, LNCS 14064, Progress in Cryptology - AFRICACRYPT2023, pp. 151 – 176. https://link.springer.com/chapter/10.1007/978-3-031-37679-5_7 Cryptology ePrint Archive, Paper 2023/690, https://eprint.iacr.org/2023/690

(2023) CIANFRIGLIA M, ONOFRI E, PEDICINI M. (2022) $\mathsf{mR}_{\mathsf{LWE}}$-CP-ABE: a revocable CP-ABE for Post-Quantum Cryptography, Cryptology ePrint Archive, Paper 2023/922, https://eprint.iacr.org/2023/922

(2022) GRASSI L, ONOFRI S, PEDICINI M, SOZZI L. (2022) Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_{p^n}$, Application to Poseidon. In Transactions on Symmetric Cryptography vol 3 (2022) p. 20–72, https://tosc.iacr.org/index.php/ToSC/article/view/9849

(2022) CASTIGLIONE F, NARDINI C, ONOFRI E, PEDICINI M, TIERI P (2022) Explainable Drug Repurposing Approach From Biased Random Walks. In IEEE/ACM Transactions on Computational Biology and Bioinformatics, 2022, n. 20(2), pp. 1009–1019. https://doi.org/10.1109/tcbb.2022.3191392

(2022) ONOFRI E, PEDICINI M. (2022) Novel notation on Cube Attacks. In Selected papers from the ITASEC2020 Workshop Cryptanalysis a Key Tool in Securing and Breaking Ciphers. Collectio Ciphrarum 2, pp. 25-30.

(2022) CIANFRIGLIA M, PEDICINI M. (2022) Unboxing Kite-attack. In Selected papers from the ITASEC2020 Workshop Cryptanalysis a Key Tool in Securing and Breaking Ciphers. Collectio Ciphrarum 2, pp. 31-36.

(2022) CIANFRIGLIA M, ONOFRI E, ONOFRI S, PEDICINI M. (2022) Ten years of cube attacks In IACR e-print archive n.137/2022.

(2021) GRASSI L, ONOFRI S, PEDICINI M, SOZZI L. (2021) Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_{p^n}$. In IACR e-print archive n.1695/2021.

(2019) CIANFRIGLIA M, GUARINO S, BERNASCHI M, LOMBARDI F, PEDICINI M. (2019) Kite attack: reshaping the cube attack for a flexible GPU-based maxterm search, pp. 1 – 18, Journal of Cryptographic Engineering, Springer Berlin Heidelberg; doi:10.1007/s13389-019-00217-3;

(2019) LAI A C, PEDICINI M, PIAZZA M. (2019) Abstract Machines, Optimal Reduction, and Streams, pp. 1 – 32, Mathematical Structures in Computer Science, Cambridge University Press (CUP); doi:10.1017/s096012951900001x;

(2019) PEDICINI M, PIAZZA M. (2017) What Arrow's Information Paradox Says (To Philosophers), On the Cognitive, Ethical, and Scientific Dimensions of Artificial Intelligence, pp. 83 – 94, Springer Berlin Heidelberg, ISBN: 9783030018009, doi:10.1007/978-3-030-01800-9_5;

(2018) PEDICINI M, PIAZZA M. (2017) Kálmar elementary complexity and von Neumann algebras Panamerican Mathematical Journal, Volume 28, Issue 4, pp. 1 – 28;

(2018) CASTIGLIONE F, MANCINI E, PEDICINI M, JARRAH A S. (2018) Quantitative Modeling Approaches, in Reference Module in Life Sciences, Elsevier, 2018, ISBN 9780128096338;

(2018) PEDICINI M, PALUMBO M C, CASTIGLIONE F. (2018) Computing Hierarchical Transition Graphs of Asynchronous Genetic Regulatory Networks. In: Pelillo M., Poli I., Roli A., Serra R., Slanzi D., Villani M. (eds) Artificial Life and Evolutionary Computation. WIVACE 2017. Communications in Computer and Information Science, vol 830, pp 88-103. Springer;

(2017) CIANFRIGLIA M, GUARINO S, BERNASCHI M, LOMBARDI F, PEDICINI M. (2017) A Novel GPU-Based Implementation of the Cube Attack, In: Gollmann D., Miyaji A., Kikuchi H. (eds) Applied Cryptography and Network Security. ACNS 2017. Lecture Notes in Computer Science, vol 10355. Springer, Cham doi:10.1007/978-3-319-61204-1_10;

(2017) KOMORNIK V, PEDICINI M, PETHŐ A. (2017) Multiple common expansions in non-integer bases, Acta Sci. Math. (Szeged) 83 (2017), p. 51–60;

(2017) KOMORNIK V, PEDICINI M. (2017) Critical Bases For Ternary Alphabets, Acta Mathematica Hungarica, Volume 152, Issue 1, pp. 25-57, Springer-Verlag;

(2016) LAI A. C, PEDICINI M, ROGNONE S. (2016) Quantum Entanglement and the Bell matrix, July 2016, Volume 15, Issue 7, pp 2923-2936, Quantum Information Processing

(2015) CANAVESE D, CESENA E, OUCHARY R, PEDICINI M, ROVERSI L. (2015) Light combinators for finite fields arithmetics, 111, 365–394, Science of Computer Programming;

(2014) CANAVESE D, CESENA E, OUCHARY R, PEDICINI M, ROVERSI L. (2014) Can a light typing discipline be compatible with efficient implementation of finite field inversion ? In Foundational and Practical Aspects of Resource Analysis Third International Workshop, FOPARA 2013, Bertinoro, Italy, August 29-31, 2013, Revised Selected Papers, Lecture Notes in Computer Science n. 8552, pp. 38–57 Springer-Verlag Berlin Heidelberg;

(2012) CESENA E, PEDICINI M, ROVERSI L. (2012) Typing a Core Binary-Field Arithmetic in a Light Logic. In R. Peña, M. van Eekelen, and O. Shkaravska (Eds.): FOPARA 2011, Lecture Notes in Computer Science n. 7177, pp. 19–35, Springer-Verlag Berlin Heidelberg;

(2011) AGNESSE A, PEDICINI M. (2011) Cube attack in finite fields of higher order. In: Australasian Information Security Conference 2011, Conferences in Research and Practice in Information Technology. Perth, Australia, 17 - 20/1/2011, SIDNEY: Australian Computer Society., vol. 116

(2011) CLANCY T, PEDICINI M., CASTIGLIONE F, SANTONI D, NYGAARD V, LAVELLE T. J, BENSON M, HOVIG E (2011). Immunological network signatures of cancer progression and survival. BMC MEDICAL GENOMICS, vol. 4:28, ISSN: 1755-8794, doi:10.1186/1755-8794-4-28

(2011) KOMORNIK V, LAI A. C, PEDICINI M. (2011). Generalized golden ratios of ternary alphabets. JOURNAL OF THE EUROPEAN MATHEMATICAL SOCIETY, vol. 13(4); p. 1113-1146, ISSN: 1435-9855, doi:10.4171/JEMS/277

(2010) PEDICINI M., PIAZZA M (2010). An application of von Neumann Algebras to compurtational complexity. In: New Essays In Logic and Philosophy of Science. Milan, 8-10 Ottobre 2007, LONDON: College Publications, vol. 1, p. 183-194, ISBN/ISSN: 9781848900035

(2010) PEDICINI M., BARRENÄS F, CLANCY T, CASTIGLIONE F, HOVIG E, KANDURI K, SANTONI D, BENSON M (2010). Combining network modeling and gene expression microarray analysis to explore the dynamics of Th1 and Th2 cell regulation. PLOS COMPUTATIONAL BIOLOGY, vol. 6 (12); p. e1001032, ISSN: 1553-734X, doi:10.1371/journal.pcbi.1001032

(2010) CASTIGLIONE F, SANTONI D, PEDICINI M. (2010). Implementing agent's rules with gene regulatory networks in mesoscopic-level models of cellular interactions. In: GABRIEL P. C. FUNG. A PRACTICAL GUIDE TO BIOINFORMATICS ANALYSIS. ANNERLEY: iConcept Press Pty Ltd., ISBN/ISSN: 978-0-9807330-2-0

(2009) PEDICINI M., PIAZZA M (2009). Elementary computation and von Neumann Algebras. vol. arXiv:0912.5342v1, p. 1-22, 29/12/2009

(2008) PEDICINI M., SANTONI D, CASTIGLIONE F (2008). Implementation of a regulatory gene network to simulate the TH1/2 differentiation in an agent-based model of hypersensitivity reactions. BIOINFORMATICS, vol. 24(11); p. 1374-1380, ISSN: 1367-4803

(2007) PEDICINI M., QUAGLIA F (2007). PELCR: Parallel Environment for Optimal Lambda-Calculus Reduction. ACM TRANSACTIONS ON COMPUTATIONAL LOGIC, vol. 8; p. 1-36, ISSN: 1529-3785, doi:10.1145/1243996.1243997

(2007) PEDICINI M., PIAZZA M (2007). Elementary Complexity into the Hyperfinite II_1 Factor. In: CiE 2007. Siena, Italy

(2006) COSENTINO A, PEDICINI M., QUAGLIA F (2006). Supporting Function Calls within PELCR. ELECTRONIC NOTES IN THEORETICAL COMPUTER SCIENCE, vol. 135; p. 107-117, ISSN: 1571-0661, doi:10.1016/j.entcs.2005.09.025

(2006) BAILLOT P, PEDICINI M. (2006). An embedding of the BSS model of computation in light affine lambda-calculus. In: LCC'06. Seattle, USA

(2005) PEDICINI M. (2005) Greedy Expansions and Sets with Deleted Digits. Theoretical Computer Science, 332/1-3 pp. 313-336. Amsterdam, The Netherlands. Elsevier, doi:10.1016/j.tcs.2004.11.002;

(2001) LORETI P, PEDICINI M. (2001) An idempotent analogue of resolvent kernels for a deterministic optimal control problem (Russian). Matematicheskie Zametki 69 (2001) no. 2, 235–244. https://link.springer.com/article/10.1023/A:1002824402949;

(2000) KOMORNIK V, LORETI P, PEDICINI M. (2000) An approximation property of Pisot numbers. Journal of Number Theory, vol. 80 n. 2, 218–237 doi:10.1006/jnth.1999.2456;

(2000) BAILLOT P, PEDICINI M. (2000) Elementary complexity and geometry of interaction. Annales Societatis Mathematicae Polonae. Series IV. Fundamenta Informaticae 45(1-2):1-31, http://iospress.metapress.com/content/9d1cd4ucuha04uvt;

(2002) PEDICINI M, QUAGLIA F. (2002) Scheduling vs. Communication in PELCR. EuroPar2002 Parallel Processing. LNCS 2400, pages 648–654. Springer-Verlag;

(2000) PEDICINI M, QUAGLIA F. (1999) A parallel implementation for optimal lambda-calculus reduction. ACM Proceedings of the 2nd International Conference on Principles and Practice of Declarative Programming (PPDP 2000), pages 3–14. ACM Press;

(1999) P. BAILLOT AND M. PEDICINI. Elementary complexity and geometry of interaction (extended abstract). In J.-Y. Girard, editor, 4th International Conference, TLCA'99, L'Aquila, number 1581 in Lecture Notes in Computer Science, pages 25–39. Springer Verlag, Berlin;

(1998) MASCARI GF, PEDICINI M. (1998) Types and dynamics in partially additive categories. In J. Gunawardena, editor, Idempotency, volume 11 of Publications of the Isaac Newton Institute, pages 112–132, Cambridge, UK. Cambridge University Press. doi:10.2277/052155344X

(1997) DANOS V, PEDICINI M, REGNIER L (1997) Directed virtual reductions. In M. Bezem and D. van Dalen, editors, Computer Science Logic, 10th International Workshop, CSL'96, volume 1258 of Lecture Notes in Computer Science, pages 76–88. EACSL, Springer Verlag, Berlin, DE.

(1994) MASCARI GF, PEDICINI M. (1994) Head linear reduction and pure proof net extraction. Theoret. Comput. Sci., 135(1):111–137, 1994. Selected papers of the Meeting on the Mathematical Foundations of Programming Semantics (MFPS'92), Part I (Oxford, 1992), Amsterdam, The Netherlands, 1994. Elsevier. doi:10.1016/0304-3975(94)90263-1.

Trattamento dei dati personali, informativa e consenso

Acconsento alla pubblicazione del mio CV in ottemperanza alle disposizioni di legge dettate in materia di trasparenza (D.Lgs. 33/2013).