Marco Baldi

curriculum vitae (brief)

Last update: January 31, 2025

Work Address:
Università Politecnica delle Marche
Facoltà di Ingegneria
Dipartimento di Ingegneria dell'Informazione (DII)
Via Brecce Bianche
60131 Ancona, Italy

Work phone: +39 071 220 4894
Work e-mail: m.baldi@univpm.it
Website: link
List of publications: link
Google scholar profile: link
ORCID iD: 0000-0002-8754-5526

Short Bio

Marco Baldi received his Laurea degree in Electronic Engineering (summa cum laude) in 2003 and his PhD degree in Electronic, Computer and Telecommunications Engineering in 2006, with a thesis entitled "Quasi-Cyclic Low-Density Parity-Check Codes and their Application to Cryptography", from Marche Polytechnic University (Univpm). Since 2019 he is an Associate Professor in Telecommunications at the Department of Information Engineering of Univpm, where he also takes part in the Research and Service Center for Privacy and Cybersecurity (CRiSPY). He is a member of the management committee of the CINI Cybersecurity National Laboratory, and coordinates its local node at Univpm. He is founding member and scientific committee member of the National Cryptologic Association De Componendis Cifris. On November 19, 2020, he achieved the National Scientific Habilitation (ASN) as Full Professor in Telecommunications, and on February 6, 2023, he achieved the National Scientific Habilitation (ASN) as Full Professor in Computer Science. His research activity concerns communications reliability and security, with focus on coding and post-quantum cryptography. He is co-author of over 200 scientific papers appeared in international journals, book chapters and conference proceedings, one book and four patents. He is a member of AEIT, CINI, CNIT, GTTI, IEEE Communications Society, IEEE Information Theory Society and an IEEE senior member. He has been vice-chair for the period 2021-2023 and he is chair for the period 2024-2025 of the IEEE Information Theory Society Italian chapter.

Editorial Activity

- Associate Editor on Coding and Information Theory for IEEE Transactions on Communications since January 2025.
- Area Editor on Coding for IEEE Communications Letters since August 2021.
- Senior Editor for IEEE Communications Letters since September 2019.
- Associated Editor for:
  - EURASIP Journal on Wireless Communications and Networking since August 2013.
  - IEEE Communications Letters since August 2014.
  - MDPI Information since March 2019.
- Guest Editor for the special issue entitled "Physical Layer Security Solutions for 5G-and-Beyond" of the EURASIP Journal on Wireless Communications and Networking, 2019.
- Editor of the books:
  - Code-Based Cryptography - 8th International Workshop (Vol. 12087 of Springer Lecture Notes in Computer Science, 2020).
  - Code-Based Cryptography - 7th International Workshop (Vol. 11666 of Springer Lecture Notes in Computer Science, 2019).
  - Proceedings of the Second Italian Conference on Cyber Security (Vol. 2058 of CEUR Workshop Proceedings, 2018).
  - Cryptography and Physical Layer Security - Proceedings of the 2nd Workshop on Communication Security (Vol. 447 of Springer Lecture Notes in Electrical Engineering, 2017).
  - Physical and Data-Link Security Techniques for Future Communication Systems (Vol. 358 of Springer Lecture Notes in Electrical Engineering, 2015).
- Reviewer for more than 40 international journals.
- TPC member for more than 100 international conferences (including flagship conferences such as IEEE Globecom, IEEE ICC, IEEE VTC).

Conference Chairing

- General co-chair of the Workshop on the mathematics of post-quantum cryptography and spring meeting SMS 2025
- General co-chair of the 2025 IEEE European School of Information Theory (IEEE ESIT 2025)
- General co-chair of the 2022 School & Workshop on Post-Quantum Cryptography (PQCifris 2022)
- Financial co-chair of the 2020 IEEE Information Theory Workshop (IEEE ITW 2020)
- General co-chair of the 4th Italian Conference on Cyber Security (ITASEC20)
- Co-organizer of the 2020 International Workshop on Code-Based Cryptography (CBCrypto 2020)
- Co-organizer of the 13th and 14th International Workshop on Security and High Performance Computing Systems (SHPCS 2018 and SHPCS 2019)
- Co-organizer of the 7th Code-Based Cryptography Workshop (CBC 2019)
- Startup track co-chair of the 3rd Italian Conference on Cyber Security (ITASEC19)
- Program co-chair of the 2nd Italian Conference on Cyber Security (ITASEC18)
- Co-organizer of the 1st and 2nd Workshop on Communication Security (WCS 2014 and WCS 2017)

Awards and Recognitions

- IEEE Communications Letters Exemplary Editor for the years 2019, 2022 and 2024
- IEEE Communications Letters Exemplary Reviewer for the years 2013, 2015 and 2021
- Best paper awards:
  - IEEE International Conference on Omni Layer Intelligent Systems (IEEE COINS) 2022
  - 17th International Joint Conference on e-Business and Telecommunications (ICETE 2020)
  - IEEE International Black Sea Conference on Communications and Networking 2015
  - IEEE International Conference on Information and Communication Systems 2015
  - International Conference on Communication Theory, Reliability, and Quality of Service 2010
  - GTTI national meeting 2010
  - International Conference on Advances in Satellite and Space Communications 2009
  - Advanced International Conference on Telecommunications 2009
  - AEIT national meeting 2009
  - International Conference on Software, Telecommunications and Computer Networks 2005, 2007 and 2008

Invited/Keynote Speeches

- "Coding theory and cryptography", Coding Theory & Cryptography Summer School and Collaboration Workshop, Virginia Tech Steger Center, Riva San Vitale, Switzerland, July 2024.
- "The restricted decoding problem and its application to post-quantum cryptography", International Workshop on the Arithmetic of Finite Fields (WAIFI 2024), Ottawa, Canada, June 2024.
- "CROSS: Codes & Restricted Objects Signature Scheme", Workshop on Post-Quantum Cryptography, Indian Institute of Technology, online, Apr. 2024.
- "Standardizing Cryptography: the NIST PQC Competition", Workshop on Post-Quantum Cryptography, Indian Institute of Technology, online, Apr. 2024.
- "Royal Rumbles in Cryptography: the NIST PQC Competition", Workshop on Topics in Applied Cryptography, Cifris23 conference, Rome, Italy, Dec. 2023.
- "Code-based cryptography", De Cifris Trends in Modern Cryptography, online, May 2022.
- "Code-based cryptography: recent advances and open challenges", Indian Institute of Technology, online, May 2022.
- "Cryptography based on non-algebraic codes: recent advances and open challenges", University of Waterloo, online, Dec. 2020.
- "LDPC and MDPC codes in cryptography: are (decoding) failures acceptable?", Algebraic Coding and Cryptography on the East coast Seminar Series, online, Oct. 2020.
- "QC-LDPC codes, QC-MDPC codes and their use in post-quantum cryptography", Carleton Finite Fields eSeminar, Carleton University, online, Jul. 2020, online video.
- "The challenge of using sparse and structured codes in code-based cryptography", Korea Cryptography Forum Annual Symposium, Seoul, Korea, Nov. 2019.
- "From error correction coding to cryptography for resisting quantum computers", Korea Cryptography Forum Annual Symposium, Seoul, Korea, Nov. 2019.
- "Cryptography-aided physical layer techniques for practical security over fading wiretap channels", 5th IEEE GLOBECOM Workshop on Trusted Communications with Physical Layer Security (TCPLS2017), Marina Bay Sands, Singapore, Dec. 2017.

- "Post-quantum cryptographic schemes based on codes", 12th International Workshop on Security and High Performance Computing Systems (SHPCS 2017), Genova, Italy, Jul. 2017.
- "Cryptographic trapdoors from classical and modern codes", Workshop on information theory and coding theory with applications to data security and privacy, Institut Mittag-Leffler, Djursholm, Sweden, May 2017.
- "Code-based cryptosystems with short keys", Neuchatel-Zurich joint seminar on Coding Theory and Cryptography, Zurich, Switzerland, Oct. 2015.
- "Efficient most reliable basis decoding of short block codes", Munich Coding and Modulation Workshop (MCM 2015), Munich, Germany, Jul. 2015.
- "Constructive aspects of code-based cryptography", DIMACS Workshop on The Mathematics of Post-Quantum Cryptography, Piscataway, New Jersey, Jan. 2015.
- "Code-based digital signatures exploiting sparse vectors", Code-based Cryptography Workshop (CBC 2013), Paris-Rocquencourt, France, Jun. 2013.
- "Using sparse codes in cryptographic primitives", Bunny TN 4 Workshop, Trento, Italy, May 2013.
- "LDPC code-based (and other) variants of the McEliece cryptosystem", Trento University, Dec. 2012.
- "Using LDPC codes in the McEliece cryptosystem", University of Zurich, Nov. 2010.
- "LDPC Codes in the McEliece Cryptosystem: attacks and countermeasures", NATO Advanced Research Workshop 2008, Veliko Tarnovo, Bulgaria, Oct. 2008.
- "McEliece cryptosystem based on LDPC codes", University of Bergen, Oct. 2007.

TEDx Talks

- "In cryptography we trust: candies and Rubik's cubes", talk at TEDx Fermo, 18 March 2022, online video.

General Audience Talks/Seminars (in Italian)

- "Cryptography: an ancient discipline facing modern challenges", Cybearly - forecasting 2025, 3 October 2024, online video.
- "Post-Quantum Cryptography and 5G: state of the art and open challenges", 5G and Cloud Security Awareness Days, Rome, Italy, 19 June 2024.
- "Cybersecurity: what do we need to protect ourselves from?", Skilla Webinar, 15 June 2023, online video.
- "5G: cyber risks, countermeasures and security", Higher School of Specialization in Telecommunications of the Italian Ministry of Enterprise and Made in Italy, 29 March 2023, online video.
- "Cybersecurity: how to defend against cyber threats", Confindustria Ancona webinar, 11 March 2022, online video.
- "PQCifris team's activities on post-quantum cryptography", UMI - DeCifris conference 2021, 22 September 2021, online video.
- "Cybersecurity for Industry 4.0", i-Labs webinar, 14 April 2021, online video.
- "Introduction to Cybersecurity", Univpm webinar, 8 March 2021, online video.
- "New information tools and cyber threats", Rete Educazione Digitale (RED) webinar, 8 February 2021, online video.
- "Cybersecurity in school and family: the mistakes not to make", Aiart Marche webinar, 29 January 2021, online video.
- "DeCifris Talk : Quantum & Ring Signatures", BlockChain Caffè webinar, 21 December 2020, online video.
- "National Cybersecurity Laboratory - Who's Who - Interview with Marco Baldi", 22 July 2017, online video.
- "Cybersecurity and SMEs: they steal your data and what do you do?", Expandere 2016, 23 June 2016, online video.

Principal Investigator of Research Projects

- (2024-2028) "Quantum-safe cryptographic tools for the protection of national data and information technology assets" (QSAFEIT), national competitive project, ranked first in the FISA 2022 - Information and Communication Technology (ICT) call selection, funded by the Italian Ministry of University and Research.
- (2024-2025) "Advanced and Quantum-safe Solutions for Digital Identity and digital Tracing" (AQuSDIT), funded by the European Union - Next Generation EU under the Italian Ministry of University and Research National Recovery and Resilience Plan.
- (2023) "Graph Based Intrusion Detection System" (GiBIDS), international competitive project, funded by GÉANT Vereniging under the GÉANT Innovation Programme.
- (2020-2022) "Cyber Risk Assessment Models and Algorithms" (CybeRAMA), national competitive project, funded by the Cariverona Foundation under the "Ricerca e Sviluppo 2018" call. Website: `https://cyberama.dii.univpm.it/`

- (2012-2016) "Enhancing communication security by cross-layer physical and data-link techniques" (ESCAPADE) national competitive project, funded by the Ministry of Education, University and Research (grant RBFR105NLC) under the "FIRB - Futuro in Ricerca 2010" call. Website: `https://www.escapade.dii.univpm.it/`

Task/Unit Leader in Research Projects

- (2024-2026) "SATEllite Lightweight Internet Key Exchange" (SATELIKE), international competitive project funded by ESA/ESOC.
- (2023-2027) "Bringing Knowledge and consensus to prevent and reduce food loss at the primary production stage. Understanding, measuring, training and adopting" (FOLOU), international competitive project funded by the Horizon Europe Framework Programme.
- (2023-2025) "Mathematical Primitives for Post-Quantum Digital Signatures", national competitive project funded by Italian Ministry of University and Research under the PRIN PNRR 2022 call.
- (2023-2025) "POst-quantum Identification and eNcryption primiTives: dEsign and Realization" (POINTER), national competitive project funded by Italian Ministry of University and Research under the PRIN 2022 call.
- (2023-2024) "Post-quantum cryptography algorithms for satellite communication applications" (QUALITA), international competitive project funded by ESA/ESOC.
- (2022-2023) "Over the Air Cryptographic Keys Exchange for Secure Governmental Satellite Communications" (CRYPTOSAT), international competitive project funded by ESA/ESOC.

Participation to Research Projects

- (2023-2025) "Efficient and reliable Communication Networks" (ECONET), funded by the European Union - Next Generation EU under the Italian Ministry of University and Research National Recovery and Resilience Plan.
- (2023-2025) "Pesaro House of Emerging Technologies" (CTE Square), national competitive project funded by Ministry of Business and Made in Italy.
- (2021-2024) "digital TuRn in EUrope: Strengthening relational reliance through Technology" (TRUST), international competitive project funded the Horizon MSCA (Marie Skłodowska-Curie Actions) - RISE (Research and Innovation Staff Exchange) program.
- (2019-2021) "sMart sEcuRe deCentralized indUstRY" (MERCURY) regional competitive project funded by the Marche Regional Administration.
- (2018-2020) "Next Generation ESTRACK Uplink Services" (NEXTRACK) international competitive project funded by ESA/ESOC.
- (2018-2019) "Telemetry Randomizer for High Data Rates" international competitive project funded by ESA/ESOC.
- (2016-2017) "PROTotype of Off-line COrreLator for Arraying of large Aperture Antennas" (PROTOCOL-A.3) international competitive project funded by ESA/ESOC.
- (2015-2016) "Reliable TT&C during superior solar conjunctions" (RESCUe) international competitive project funded by ESA/ESOC.
- (2014-2016) "Next Generation Uplink Coding Techniques" (NEXCODE) international competitive project funded by ESA/ESTEC.
- (2012-2013) "Advanced Coding Schemes for Direct Sequence Spread Spectrum Telecommand Links" international competitive project funded by ESA/ESTEC.
- (2012) "Support to Channel Coding Services" international competitive project funded by ESA/ESOC.
- (2011) "Non Invasive Monitoring by Ultra wide band Radar of Respiratory Activity of people inside a spatial environment" (NIMURRA) national competitive project funded by the Italian Space Agency (ASI).
- (2010) "Support to Channel Coding Services" international competitive project funded by ESA/ESOC.
- (2009) "Randomizer for High Data Rates" international competitive project funded by ESA/ESOC.

COST Actions

- (2023-2027) COST Action CA22168, "Physical layer security for trustworthy and resilient 6G systems" (6G-PHYSEC)", Management Committee Member for Italy and candidate coordinator of Working Group 3 on "Quantum-Resistant Security".
- (2015-2018) COST Action IC1306, "Cryptography for Secure Digital Interaction", Management Committee Substitute for Italy.
- (2013-2016) COST Action IC1104, "Random Network Coding and Designs over GF(q)", member of Working Group 3 on "Cryptographic Aspects of Network Codes".

Evaluation Panels

Reviewer/panel member for:

- Italian Ministry of University and Research
- Dutch Research Council (NWO)
- Polish National Science Centre
- Helmholtz Association
- Romanian Executive Agency for Higher Education, Research, Development and Innovation Funding (UEFISCDI)
- European Science Foundation
- Università di Catania
- Ministry of Education, Youth and Sports of the Czech Republic (MEYS)
- Estonian Research Council
- Natural Sciences and Engineering Research Council of Canada (NSERC)
- KU Leuven Research Council

Standardization initiatives

- Member of the proposing team of the CROSS post-quantum digital signature scheme, currently competing in the second round of the NIST post-quantum cryptography standardization process, additional call for digital signatures.
- Member of the proposing team of the LESS post-quantum digital signature scheme, currently competing in the second round of the NIST post-quantum cryptography standardization process, additional call for digital signatures.
- Member of the proposing team of the LEDAcrypt post-quantum cryptographic algorithms, admitted to the second round of the NIST post-quantum cryptography standardization process.
- Several contributions to the Consultative Committee for Space Data Systems (CCSDS), especially concerning the CCSDS Green Book on TM Synchronization and Channel Coding (CCSDS 130.1-G-1) and the CCSDS Green Book on TC Synchronization and Channel Coding (CCSDS 230.1-G-2).

Industrial collaborations

- Co-founding member and member of the board of directors (2021-present) of Ancharia Srl, spin-off company of Marche Polytechnic University working on cybersecurity.
- Co-founding member and member of the board of directors (2004-2016) of Arielab Srl, spin-off company of Marche Polytechnic University working on telecommunication systems.
- Institutional collaborations on specific projects with several companies, such as Thales Alenia Space, Defence Tech Holding S.p.A., Namirial S.p.A., Videoworks S.p.A., A TLC S.r.l., Videx Electronics S.p.A., Telecom Italia S.p.A., Siemens S.p.A.

Teaching and supervision

- Teaching professor for several courses for Bachelor's, Master's and PhD students at the Polytechnic University of Marche since 2007.
- Director of the postgraduate course on "Cybersecurity, Cyber Risk and Data Protection", jointly organized by the Polytechnic University of Marche and the University of Macerata, for the academic years 2021/2022, 2022/2023, 2023/2024 and 2024/2025. Website: `https://csdp.dii.univpm.it/`.
- Deputy director of the postgraduate course on "Ethics, law and digital technologies", jointly organized by the University of Macerata and the Polytechnic University of Marche, for the academic year 2021/2022, 2023/2024 and 2024/2025. Website: `https://edted.unimc.it/`.
- Teaching professor for several master and specialization courses (on Industry 4.0, Data Science, Blockchain Economy, Big Data Engineering, Privacy and others).
- Extern examiner for the PhD defense of Giovanni Tognolini, PhD course in Mathematics of the University of Trento on March 2025.
- Extern examiner for the PhD defense of the candidates Bilal Ahmad, Carla Amatetti, Pasquale Manuele Grilli and Elia Leoni, PhD course in Electronics, Telecommunications and Information Technology Engineering of the University of Bologna on June 2023.
- Extern examiner for the PhD defense of the candidates Andrea Nicolini, Giampaolo Cuozzo and Riccardo Marini, PhD course in Electronics, Telecommunications and Information Technology Engineering of the University of Bologna on March 2023.
- Extern examiner for the PhD defense of Charbel Saliba at École Nationale Supérieure de l'Électronique et de ses Applications (ENSEA), Cergy Paris Université on May 2022.

- Extern examiner for the PhD defense of Luca Baldanzi at the University of Pisa on May 2021.
- Extern examiner for the PhD defense of Ian Mulholland at University College Dublin on March 2016.
- Supervisor of several postdoc researchers at Marche Polytechnic University since 2013.
- Supervisor of PhD students:
  - Davide De Zuane, IMT School for Advanced Studies Lucca, 2024-present.
  - Alessio Baldelli, Marche Polytechnic University, 2024-present.
  - Riccardo Schiavoni, Marche Polytechnic University, 2024-present.
  - Giacomo Zonneveld, Marche Polytechnic University, 2024-present.
  - Pietro Locatelli, IMT School for Advanced Studies Lucca, 2023-present.
  - Rebecca Giuliani, Marche Polytechnic University, 2023-present.
  - Nibras Abo Alzahab, Marche Polytechnic University, 2022-2024.
  - Lorenzo Principi, Marche Polytechnic University, 2021-2024.
  - Paolo Santini, Marche Polytechnic University, 2016-2019.
- Co-supervisor of PhD students:
  - Ludovica Ilari, University of Macerata, 2021-2024.
  - Linda Senigagliesi, Marche Polytechnic University, 2015-2018.
  - Massimo Battaglioni, Marche Polytechnic University, 2015-2018.
  - Giacomo Ricciutelli, Marche Polytechnic University, 2014-2017.



Firmato digitalmente da Marco Baldi
Data: 02.05.2025 10:52:39 CEST
Organizzazione: UNIVERSITA' POLITECNICA DELLE MARCHE/00382520427