

Ultimo aggiornamento: 23 settembre 2021

Biografia

Marco Baldi ha conseguito presso l'Università Politecnica delle Marche la Laurea in Ingegneria Elettronica (summa cum laude) nel 2003 e il Dottorato di Ricerca in Ingegneria Elettronica, Informatica e delle Telecomunicazioni nel 2006, con una tesi dal titolo "Quasi-Cyclic Low-Density Parity-Check Codes and their Application to Cryptography". Dal 2012 al 2019 è stato Ricercatore a Tempo Determinato in Telecomunicazioni presso il Dipartimento di Ingegneria dell'Informazione dell'Università Politecnica delle Marche. Dal 2019 è Professore Associato in Telecomunicazioni presso lo stesso dipartimento, dove coordina il nodo locale del Laboratorio Nazionale Cybersecurity del CINI e partecipa al Centro di Ricerca e Servizio per la Privacy e la Cybersecurity (CRiSPY). Il 19 novembre 2020 ha conseguito l'Abilitazione Scientifica Nazionale (ASN) come Professore di Prima Fascia nel Settore Scientifico Disciplinare ING-INF/03 - Telecomunicazioni. La sua attività di ricerca riguarda l'affidabilità e la sicurezza delle informazioni, con particolare attenzione alla codifica per l'affidabilità delle comunicazioni e alla crittografia post-quantum. È coautore di oltre 150 pubblicazioni scientifiche apparse su riviste internazionali, capitoli di libri e atti di convegni, un libro e quattro brevetti. La sua attività di ricerca è stata in parte svolta in collaborazione con aziende e istituzioni nazionali ed internazionali. È membro di AEIT, CINI, CNIT, GTTI, IEEE ComSoc, IEEE ITSoc e senior member IEEE.

Indicatori bibliometrici

- 158 documenti, 1345 citazioni, h-index 19 (fonte Scopus).

Interventi su invito

- "McEliece cryptosystem based on LDPC codes", University of Bergen, Oct. 2007.
- "LDPC Codes in the McEliece Cryptosystem: attacks and countermeasures", NATO Advanced Research Workshop 2008, Veliko Tarnovo, Bulgaria, Oct. 2008.
- "Using LDPC codes in the McEliece cryptosystem", University of Zurich, Nov. 2010.
- "LDPC code-based (and other) variants of the McEliece cryptosystem", Trento University, Dec. 2012.
- "Using sparse codes in cryptographic primitives", Bunny TN 4 Workshop, Trento, Italy, May 2013.
- "Code-based digital signatures exploiting sparse vectors", Code-based Cryptography Workshop (CBC 2013), Paris-Rocquencourt, France, Jun. 2013.
- "Constructive aspects of code-based cryptography", DIMACS Workshop on The Mathematics of Post-Quantum Cryptography, Piscataway, New Jersey, Jan. 2015.
- "Efficient most reliable basis decoding of short block codes", Munich Coding and Modulation Workshop (MCM 2015), Munich, Germany, Jul. 2015.
- "Code-based cryptosystems with short keys", Neuchatel-Zurich joint seminar on Coding Theory and Cryptography, Zurich, Switzerland, Oct. 2015.
- "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.
- "Post-quantum cryptographic schemes based on codes", 12th International Workshop on Security and High Performance Computing Systems (SHPCS 2017), Genova, Italy, Jul. 2017.
- "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.
- "From error correction coding to cryptography for resisting quantum computers", Korea Cryptography Forum Annual Symposium, Seoul, Korea, Nov. 2019.
- "The challenge of using sparse and structured codes in code-based cryptography", Korea Cryptography Forum Annual Symposium, Seoul, Korea, Nov. 2019.

- “QC-LDPC codes, QC-MDPC codes and their use in post-quantum cryptography”, Carleton Finite Fields eSeminar, Carleton University, Ottawa (online), Jul. 2020.
- “LDPC and MDPC codes in cryptography: are (decoding) failures acceptable?”, Algebraic Coding and Cryptography on the East coast Seminar Series (online), Oct. 2020.
- “Cryptography based on non-algebraic codes: recent advances and open challenges”, University of Waterloo (online), Dec. 2020.

Attività editoriale

- Senior Editor per IEEE Communications Letters da settembre 2019.
- Associate Editor per:
 - EURASIP Journal on Wireless Communications and Networking da agosto 2013.
 - IEEE Communications Letters da agosto 2014.
 - MDPI Information da marzo 2019.
- Guest Editor per il numero speciale intitolato “Physical Layer Security Solutions for 5G-and-Beyond” del EURASIP Journal on Wireless Communications and Networking, 2019.
- Co-editor dei libri:
 - 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 per oltre 40 riviste internazionali e membro del comitato tecnico di programma per oltre 90 conferenze internazionali.

Organizzazione di conferenze

- Financial co-chair del 2020 IEEE Information Theory Workshop (IEEE ITW 2020)
- General co-chair della 4th Italian Conference on Cyber Security (ITASEC20)
- Co-organizzatore del 2020 International Workshop on Code-Based Cryptography (CBCrypto 2020)
- Co-organizzatore del 13° e 14° International Workshop on Security and High Performance Computing Systems (SHPCS 2018 e SHPCS 2019)
- Co-organizzatore del 7th Code-Based Cryptography Workshop (CBC 2019)
- Startup track co-chair della 3rd Italian Conference on Cyber Security (ITASEC19)
- Program co-chair della 2nd Italian Conference on Cyber Security (ITASEC18)
- Co-organizzatore del primo e secondo Workshop on Communication Security (WCS 2014 and WCS 2017)

Commissioni di valutazione

Membro di commissione di valutazione per: 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.

Premi e riconoscimenti

- IEEE Communications Letters Exemplary Editor Award per l'anno 2019
- IEEE Communications Letters Exemplary Reviewer per gli anni 2013 e 2015
- Premi per miglior articolo:
 - 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

Coordinamento di progetti di ricerca

- (2020-2022) “Cyber Risk Assessment Models and Algorithms” (CybeRAMA), progetto nazionale finanziato dalla Fondazione Cariverona nell’ambito del bando “Ricerca e Sviluppo 2018”. Sito: <https://cyberama.dii.univpm.it/>
- (2012-2016) “Enhancing communication security by cross-layer physical and data-link techniques” (ES-CAPADE), progetto nazionale (codice RBFR105NLC) finanziato dal Ministero dell’Istruzione, Università e Ricerca nell’ambito del bando “FIRB - Futuro in Ricerca 2010”. Sito: <https://www.escapade.dii.univpm.it/>

Partecipazione a progetti di ricerca

- (2019-2021) “sMart sEcuRe deCentralized indUstRY” (MERCURY), progetto regionale finanziato da Regione Marche.
- (2018-2020) “Next Generation ESTRACK Uplink Services” (NEXTRACK), progetto internazionale finanziato da ESA/ESOC.
- (2018-2019) “Telemetry Randomizer for High Data Rates”, progetto internazionale finanziato da ESA/ESOC.
- (2016-2017) “PROTOTYPE of Off-line CORreLator for Arraying of large Aperture Antennas” (PROTOCOL-A.3), progetto internazionale finanziato da ESA/ESOC.
- (2015-2016) “Reliable TT&C during superior solar conjunctions” (RESCUe), progetto internazionale finanziato da ESA/ESOC.
- (2014-2016) “Next Generation Uplink Coding Techniques” (NEXCODE), progetto internazionale finanziato da ESA/ESTEC.
- (2012-2013) “Advanced Coding Schemes for Direct Sequence Spread Spectrum Telecommand Links”, progetto internazionale finanziato da ESA/ESTEC.
- (2012) “Support to Channel Coding Services”, progetto internazionale finanziato da ESA/ESOC.
- (2011) “Non Invasive Monitoring by Ultra wide band Radar of Respiratory Activity of people inside a spatial environment” (NIMURRA), progetto nazionale finanziato dall’Agenzia Spaziale Italiana (ASI).
- (2010) “Support to Channel Coding Services”, progetto internazionale finanziato da ESA/ESOC.
- (2009) “Randomizer for High Data Rates”, progetto internazionale finanziato da ESA/ESOC.

Collaborazioni con industrie

- Co-fondatore e membro del consiglio di amministrazione per il periodo 2004-2016 della società Arielab Srl, spin-off dell’Università Politecnica delle Marche.
- Collaborazioni istituzionali con numerose aziende, tra cui Namirial S.p.A., A TLC S.r.l., Videoworks S.p.A., Videx Electronics S.p.A., Telecom Italia S.p.A., Siemens S.p.A.

Contributi ad iniziative di standardizzazione

- Membro del team proponente della suite di algoritmi crittografici post-quantum LEDAcrypt (<https://www.ledacrypt.org/>), ammessa al secondo round del processo di standardizzazione del NIST di primitive crittografiche post-quantum.
- Numerosi contributi al Consultative Committee for Space Data Systems (CCSDS), specialmente relativi al CCSDS Green Book on TM Synchronization and Channel Coding (CCSDS 130.1-G-1) ed al CCSDS Green Book on TC Synchronization and Channel Coding (CCSDS 230.1-G-2).

Attività didattica

- Docente del corso di “Biomedical Data Protection” del Corso di Laurea Magistrale in Biomedical Engineering dell’Università Politecnica delle Marche dal 2020 ad oggi.
- Docente del corso di “Cybersecurity for Networks” dei Corsi di Laurea Magistrale in Ingegneria Elettronica ed Ingegneria Informatica e dell’Automazione dell’Università Politecnica delle Marche dal 2020 ad oggi.
- Docente del corso di Dottorato su “Open source scientific software for PhD students: Octave” presso l’Università Politecnica delle Marche dal 2016 ad oggi.
- Docente del corso di “Privacy and Security of Biomedical Data” del Corso di Laurea Magistrale in Biomedical Engineering dell’Università Politecnica delle Marche dal 2016 al 2019.
- Docente del corso di “Sicurezza nelle Reti di Telecomunicazione” del Corso di Laurea Magistrale in Ingegneria Elettronica dell’Università Politecnica delle Marche dal 2012 al 2019.

- Docente del corso di “Reti Wireless” del Corso di Laurea Magistrale in Ingegneria Elettronica dell'Università Politecnica delle Marche dal 2007 al 2010.
- Componente del Collegio del Corso di Dottorato in Ingegneria dell'Informazione presso l'Università Politecnica delle Marche dal 2013 ad oggi.
- Vice-direttore del corso di perfezionamento in “Etica, diritto e tecnologie del digitale” organizzato dall'Università di Macerata in collaborazione con l'Università Politecnica delle Marche dal 2020. Sito: <https://edted.unimc.it/>.
- Coordinatore del corso di perfezionamento in “Cybersecurity, Cyber Risk and Data Protection”, organizzato dall'Università Politecnica delle Marche in collaborazione con l'Università di Macerata dal 2020.
- Docente per numerosi master e corsi di specializzazione (su Blockchain Economy, Industry 4.0, Big Data Engineering, Privacy, Data Science e altri).

Supervisione di assegnisti e dottorandi

- Co-tutor di Giacomo Ricciutelli, studente di dottorato presso l'Università Politecnica delle Marche da novembre 2014 ad ottobre 2017.
- Co-tutor di Linda Senigagliesi, studente di dottorato presso l'Università Politecnica delle Marche da novembre 2015 ad ottobre 2018.
- Co-tutor di Massimo Battaglioni, studente di dottorato presso l'Università Politecnica delle Marche da novembre 2015 ad ottobre 2018.
- Co-tutor di Paolo Santini, studente di dottorato presso l'Università Politecnica delle Marche da novembre 2016 ad ottobre 2019.
- Tutor di otto assegnisti di ricerca presso l'Università Politecnica delle Marche dal 2013 ad oggi.
- Esaminatore esterno per la difesa della tesi di dottorato di Ian Mulholland presso University College di Dublino a marzo 2016.
- Esaminatore esterno per la difesa della tesi di dottorato di Luca Baldanzi presso l'Università di Pisa a maggio 2021.