Marco Baldi

curriculum vitae

January 4, 2017

Work address:
Università Politecnica delle Marche
Dipartimento di Ingegneria dell'Informazione (DII)
Via Brecce Bianche, 12
60131 - Ancona
Italy

Phone: (+39) 071 220 4894
Email: m.baldi@univpm.it
websites:
http://www.univpm.it/marco.baldi
https://marcobaldi.github.io/

Short Biography

Marco Baldi received a Laurea degree in Electronic Engineering (summa cum laude) in 2003 and a PhD in Electrical Engineering, Computer Science and Telecommunications in 2006, with a thesis entitled "Quasi-Cyclic Low-Density Parity-Check Codes and Their Application to Cryptography ", by Marche Polytechnic University. Since 2012 is an assistant professor (with tenure track since 2016) in Telecommunications at the Department of Information Engineering of Marche Polytechnic University.

His research activity is focused on coding techniques for communications reliability, security and cryptography, with particular attention to the study of linear block codes for symmetric and asymmetric channels, LDPC codes and their applications in cryptography and secure communications. He is co-author of over 100 scientific papers published in international journals, book chapters and conference proceedings, a book and two patents. His research has been partly carried out in cooperation with companies and national and international organizations, including: Siemens Mobile Communications, Telecom Italia, the Italian Space Agency and the European Space Agency. Following these activities, he is co-author of several public and private technical reports. He has collaborated with the European Space Agency in the activities of the Consultative Committee for Space Data Systems for standardizing techniques for space telecommunications.

He has received several research awards. He gave invited talks and seminars at the University of Bergen, the Bulgarian Academy of Sciences, the University of Zurich, the University of Trento, the Institut National de Recherche en Informatique et en Automatique (INRIA) and the Technische Universität München (TUM).

He serves as Associate Editor for IEEE Communications Letters and EURASIP Journal on Wireless Communications and Networking. He received the IEEE Communications Letters Exemplary Reviewer award for the years 2013 and 2015. He has served and serves as a reviewer for several international journals and conferences. He has participated in various committees for the evaluation of international research projects. He also took part in the technical program committee of several international conferences and has been co-chair of the 2014 and 2017 editions of the Workshop on Communication Security (WCS 2014 and WCS 2017).

He was a co-founder partner and member of the board of directors of Arielab S.r.l., a spin-off company of Marche Polytechnic University, operating since 2004 in the area of Telecommunications Engineering. He is member of AEIT, EURACON, CNIT, GTTI, IEEE Communications Society, IEEE Information Theory Society and senior member of IEEE. He was the secretary of the Adriatic Section of AEIT for the period 2011-2013.

He was the national coordinator of the ESCAPADE research project on communications security topics, funded by the Ministry of Education, University and Research (grant RBFR105NLC) under the "FIRB - Futuro in Ricerca 2010" call. He is coordinator of the cyber security group of Marche Polytechnic University and director of Marche Polytechnic University local node of the CINI National Laboratory of Cyber Security.

Training

March 12, 2003: Laurea Degree in Electronic Engineering

Five-year Laurea Degree (equivalent to Master of Science) in Electronic Engineering obtained with grade 110/110 and honors from Marche Polytechnic University with a thesis entitled "Management of multimedia services on embedded Linux platform for mobile media applications", advisor Prof. Ennio Gambi.

December 21, 2006: PhD

PhD in Electrical Engineering, Computer Science and Telecommunications from Marche Polytechnic University with a thesis entitled "Quasi-Cyclic Low-Density Parity-Check Codes and Their Application to Cryptography", tutor Prof. Franco Chiaraluce.

Qualifications

Professional Engineer Habilitation (first session 2003)

Examination for a license to practice as an engineer passed with score $191/200$.

Current Position

Marche Polytechnic University (1/11/2016 - present)

Tenure-track assistant professor, in full-time commitment regime, pursuant to art. 24, paragraph 3, letter b) of Law no. 240/2010, sector 09/F2 - Telecommunications, within the Department of Information Engineering.

Previous positions

Marche Polytechnic University (8/03/2012 - 31/10/2016)

Fixed term assistant professor, in full-time commitment regime, pursuant to art. 24, paragraph 3, letter a) of Law no. 240/2010, sector 09/F2 - Telecommunications, within the Department of Information Engineering.

Marche Polytechnic University (06/01/2009 - 31/01/2012)

Research Fellow (art. 51, paragraph 6, Law 27 December 1997 n. 449) in the Scientific Sector ING-INF / 03 - Telecommunications, in the Department of Information Engineering, on a project entitled "Study of the impact on the DVB-T system and research of technological solutions to the extension and consequent increase in the number of services offered on digital terrestrial television and integration of new technologies such as the National Service Card (Raffaello Card)".

Marche Polytechnic University (01/04/2008 - 31/05/2009)

Research Fellow (art. 51, paragraph 6, Law 27 December 1997 n. 449) in the Scientific Sector ING-INF / 03 - Telecommunications, in the Department of Biomedical Engineering, Electronics and Telecommunications, on a project entitled "Communication systems for data transfer over heterogeneous LANs".

Marche Polytechnic University (1/10/2007 - 31/03/2008)

Research Fellow (art. 51, paragraph 6, Law 27 December 1997 n. 449) in the Scientific Sector ING-INF / 03 - Telecommunications, in the Department of Electronics, Artificial Intelligence and Telecommunications, on a project entitled "Innovative techniques for the management and the technical support of a services center for DVB-T".

Centro Radioelettrico Sperimentale G. Marconi (January-February 2007)

Contract Researcher.

ArieLAB S.r.l.
(December 2004 - October 2015)

Co-founder and member of the Board of Directors of ArieLAB srl, a spin-off company of Marche Polytechnic University operating in the area of Telecommunications Engineering.

Marche Polytechnic University
(01/11/2003 - 31/10/2006)

PhD student in Electrical Engineering, Computer Science and Telecommunications with University scholarship at the Department of Electronics, Telecommunications and Artificial Intelligence.

E.S.T. S.r.l.
(June 2003 - December 2003)

Hardware / software designer.

Language knowledge

English

Good command of spoken and written language (post-intermediate level C1). Cambridge Certificate in Advanced English obtained on August 10, 2005. Frequent contacts and speeches delivered in English.

Italian

Mother language.

Editorial activity

Editorial activity for Journals and Books

Associate Editor for the IEEE Communications Letters since August 2014.

Associate Editor for the EURASIP Journal of Wireless Communications and Networking since August 2013.

Editor of the book entitled "Physical and Data-Link Security Techniques for Future Communication Systems", published in Vol. 358 of Lecture Notes in Electrical Engineering, Springer, 2015.

Reviewer of books for the publishing house Springer since 2016.

Reviewer for several international journals, including:

- Taylor & Francis Cryptologia since 2016
- Elsevier Computer Networks since 2016
- IEEE Transactions on Wireless Communications since 2016
- Elsevier Computer Communications since 2015
- IEEE Signal Processing Letters since 2015
- IEEE Communications Magazine since 2014
- Journal of Computer Security since 2014
- ETRI Journal since 2014
- Elsevier International Journal on Engineering Science and Technology since 2014
- IEEE Transactions on Computers since 2014
- International Journal of Communication Systems since 2014
- EURASIP Journal on Information Security since 2013
- Designs, Codes and Cryptography since 2013
- Cryptographic Journal of Engineering since 2013
- Digital Signal Processing since 2013
- IET Communications since 2013
- IEEE Transactions on Vehicular Technology since 2013
- IEEE Transactions on Information Theory since 2013
- IEEE Wireless Communications Letters since 2012
- Neurocomputing since 2012
- IEEE Transactions on Very Large Scale Integration Systems since 2012
- International Journal On Advances in Telecommunications since 2012
- IEEE Transactions on Information Forensics & Security since 2011
- EURASIP Journal on Wireless Communications and Networking since 2011
- Journal of Zhejiang University Science C since 2011
- Journal of Systems and Software since 2010
- Applicable Algebra in Engineering, Communication and Computing since 2010
- IET Information Security since 2009
- IEEE Communication Letters since 2009
- IEEE Transactions on Communications since 2009
- IEEE Transactions on Circuits and Systems II since 2009
- Journal of Communications and Networks since 2009
- International Journal of Digital Multimedia Broadcasting since 2009
- Journal of Communication Software and Systems (JCOMSS) since 2008
- Journal of Computing and Information Technology since 2008
- IEEE Transactions on Circuits and Systems I since 2008
- IEEE / IET Electronics Letters since 2007

Organization of conferences

Co-chair of the Workshop on Communication Security (WCS 2014), held in Ancona, Italy, in September 2014.

Co-chair of the Workshop on Communication Security (WCS 2017), affiliated with Eurocrypt 2017, to be held in Paris, France, in April 2017.

Participation in the Technical Program Committee (TPC) of international conferences

- IEEE International Conference on Communication, Networks and Satellite (COMNETSAT 2017)
- SpliTech2017 - Symposium on RFID & Embedded Systems for Internet of Things
- First Italian Conference on Cyber Security (ITA-SEC 2017)
- IEEE ICC 2017 Selected Areas in Communications Symposium - Satellite and Space Communications
- IEEE GlobalSIP 2016 - Symposium on Information Theoretic Approaches to Security and Privacy
- 12th ACM Int. Symp. on QoS and Security for Wireless and Mobile Networks (Q2SWinet 2016)
- IEEE Globecom 2016 - Workshop on Trusted Communications with Physical Layer Security
- IEEE International Conference on Communication, Networks and Satellite (COMNETSAT 2016)
- International conference on Computers, Data Management and Technology Applications (ICCDMTA 2016)
- IEEE International Conference on Telecommunications and Signal Processing (TSP 2016)
- IEEE Industrial Electronics and Applications Conference (IEACon 2016)
- IEEE Globecom 2016 Selected Areas in Communications Symposium - Satellite and Space Communications
- International Conference on Collaboration Technologies and Systems (CTS 2016)
- IEEE ICC 2016 - Workshop on Wireless Physical Layer Security (WPLS)
- IEEE WCNC 2016 - Workshop on Physical Layer Security
- IEEE ICC 2016 - Communications Theory Symposium
- 8th Advanced Satellite Multimedia Systems Conference and 14th Signal Processing for Space Communications Workshop (ASMS/SPSC 2016)
- IEEE World Symposium on Web Applications and Networking (WSWAN 2015)
- International Conference on Signal Processing & Data Mining (ICSPDM 2015)
- International Conference in Computer Technology and Information Systems (ICCTIS 2015)
- IEEE International Conference on Telecommunications and Signal Processing (TSP 2015)
- 3rd International Conference on Digital Signal Processing
- IEEE Globecom 2015 - Workshop on Trusted Communications with Physical Layer Security
- 11th ACM Int. Symp. on QoS and Security for Wireless and Mobile Networks (Q2SWinet 2015)
- 15th IMA International Conference on Cryptography and Coding
- SoftCOM 2015 - Symposium on RFID Technologies & the Internet of Things
- MOBIQUITOUS 2015 - Workshop on Wireless Communication Security at the Physical Layer (WiComSec-Phy 2015)
- International Conference on Collaboration Technologies and Systems (CTS 2015)
- IEEE Globecom 2015 Selected Areas in Communications Symposium - Satellite and Space Communications
- IEEE ICC 2015 - Workshop on Wireless Physical Layer Security (WPLS)

- IEEE ICC 2015 Selected Areas in Communications Symposium - Satellite and Space Communications
- 2nd International Conference on Electrical Engineering and Applications, 2015
- IEEE Symposium on Industrial Electronics Applications (ISIEA 2014)
- IEEE Symposium on Wireless Technology & Applications (ISWTA 2014)
- 10th ACM Int. Symp. on QoS and Security for Wireless and Mobile Networks (Q2SWinet 2014)
- International Conference on Advanced Studies in Computer Science and Engineering (ICASCSE'2014)
- SoftCOM 2014 - Symposium on RFID Technologies & the Internet of Things
- 2nd International Conference on Telecommunication Systems and Networks, 2014
- IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE 2014)
- International Conference on Intelligent Systems and Applications (ICISA'2014)
- International Conference on Biological Models and Industrial Management (ICBMIM'2014)
- International Conference on Electronic Publishing and Information Technology (ICEPIT 2014)
- 2nd International Conference on Digital Signal Processing, 2014
- 2nd International Conference on Computer Science and Engineering, 2014
- International Conference on Advances in Satellite and Space Communications (SPACOMM 2014)
- 1st International Conference on Computer Science and Engineering, 2013
- SoftCOM 2013 - Symposium on RFID Technologies & the Internet of Things
- International Conference on Mobile Applications and Security Management (ICMASM'2013)
- 3rd International Conference on Communications and Signal Processing 2013
- IEEE Symposium on Wireless Technology & Applications (ISWTA 2013)
- International Conference on Advances in Satellite and Space Communications (SPACOMM 2013)
- IEEE Symposium on Computers & Informatics (ISCI 2013)
- 5th International Conference on Communications, Signals and Coding, 2012
- SoftCOM 2012 - Symposium on RFID Technologies & the Internet of Things
- IEEE Symposium on Wireless Technology & Applications (ISWTA 2012)
- International Conference on Advances in Satellite and Space Communications (SPACOMM 2012)
- SoftCOM 2011 - Symposium on RFID Technologies & the Internet of Things
- International Conference on Advances in Satellite and Space Communications (SPACOMM 2011)
- SoftCOM 2010 - Symposium on RFID Technologies & the Internet of Things

- International Conference on Advances in Satellite and Space Communications (SPACOMM 2010)
- SoftCOM 2009 - Symposium on RFID Technologies & the Internet of Things

Reviewer of many contributions submitted for presentation at international conferences.

Reviewer of research projects for:

- Romanian Executive Agency for Higher Education, Research, Development and Innovation Funding (UEFISCDI) - 3rd National Plan for Research, Development and Innovation for the period 2015-2020 (PNCDI III).
- European Science Foundation - 2015 Junior Research AXA Research Fund (postdoctoral) Fellowship Scheme (2015).
- University of Catania - Call for the funding of research projects FIR 2014.
- Ministry of Education, Youth and Sports of the Czech Republic (MEYS) - Czech-Norwegian Research Programme CZ09 (2014).
- Romanian Executive Agency for Higher Education, Research, Development and Innovation Funding - Research within Priority Sectors Programme - RO14 (2014).
- Estonian Research Council - Estonian-Norwegian Research Cooperation Programme (2013).

Awards

Best paper awards

- IEEE International Black Sea Conference on Communications and Networking 2015 (G. Ricciutelli, M. Baldi, N. Maturo, F. Chiaraluce, "LDPC Coded Modulation Schemes with Largely Unequal Error Protection", May 2015)
- IEEE International Conference on Information and Communication Systems 2015 (M. Baldi, F. Chiaraluce, N. Maturo, E. Paolini, "On the applicability of the most reliable basis algorithm for LDPC decoding in telecommand links", Apr. 2015)
- International Conference on Communication Theory, Reliability, and Quality of Service 2010 (M. Baldi, F. Chiaraluce, R. Garello, M. Polano, M. Valentini, "On the effect of estimation and quantization errors in downstream VDSL systems", June 2010)
- Francesco Carassa award for the best paper in the Transmissions Session of 2010 GTTI meeting (M. Baldi, M. Bianchi, F. Chiaraluce, "Physical Layer Security through Non-Systematic Coding", June 2010)
- International Conference on Advances in Satellite and Space Communications 2009 (M. Baldi, G. Cancellieri, F. Chiaraluce, "A Class of Low-Density Parity-Check Product Codes", July 2009)
- Advanced International Conference on Telecommunications 2009 (M. Baldi, G. Cancellieri, F. Chiaraluce, "New LDPC Codes based on Serial Concatenation", May 2009)
- International Conference on Software, Telecommunications and Computer Networks 2008 (E. Zanaj, M. Baldi, F. Chiaraluce, "Share factors optimization in the push-sum algorithm for sensor networks", Sep. 2008)
- International Conference on Software, Telecommunications and Computer Networks 2007 (M. Baldi, G. Cancellieri, F. Chiaraluce, "Iterative Soft-Decision Decoding of Binary Cyclic Codes based on Spread Parity-Check Matrices", Sep. 2007)
- International Conference on Software, Telecommunications and Computer Networks 2005 (M. Baldi, G. Cancellieri, F. Chiaraluce, S. Bianchi, A. Carassai, "Rate Adaptive Low Density Parity Check Codes in Radio Links", Sep. 2005)

Distinctions for reviewer activities

- IEEE Communications Letters 2015 Exemplary Reviewer Award.
- IEEE Communications Letters 2013 Exemplary Reviewer Award.

Other awards

- Appreciation Award for professional support to the TSP 2013 TPC (July 2013)
- Best presentation award at the Day of Study on Technical and Scientific Innovation in Italy in the Electric Energy and ICT fields (M. Baldi, "Post-quantum cryptographic systems for telecommunication security" (in Italian), May 2009)
- Accepted presentation award at the Day of Study on Technical and Scientific Innovation in Italy in the Electric Energy and ICT fields (M. Baldi, "Post-quantum cryptographic systems for telecommunication security" (in Italian), May 2009)

Invited Talks

Neuchatel-Zürich joint seminar on Coding Theory and Cryptography

Title: Code-based cryptosystems with short keys
Place: University of Zürich, Switzerland
Date: October 2015

Munich Coding and Modulation Workshop (MCM 2015)

Title: Efficient most reliable basis decoding of short block codes
Place: Institute for Communications Engineering, Technische Universität München, Germany
Date: July 2015

DIMACS Workshop on "The Mathematics of Post-Quantum Cryptography"

Title: Constructive aspects of code-based cryptography
Place: Rutgers University, Piscataway, New Jersey
Date: January 2015

Code-based Cryptography Workshop (CBC 2013)

Title: Code-based digital signatures exploiting sparse vectors
Place: INRIA, Paris-Rocquencourt, France
Date: June 2013

Bunny TN 4 Workshop

Title: Using sparse codes in cryptographic primitives
Place: University of Trento, Italy
Date: May 2013

Seminar at the University of Trento

Title: LDPC code-based (and other) variants of the McEliece cryptosystem
Place: University of Trento, Italy
Date: December 2012

Seminar at the University of Zürich

Title: Using LDPC codes in the McEliece cryptosystem
Place: University of Zürich, Switzerland
Date: October 2010

NATO Advanced Research Workshop 2008

Title: LDPC Codes in the McEliece Cryptosystem: attacks and countermeasures
Place: Veliko Tarnovo, Bulgaria
Date: October 2008

Seminar at the University of Bergen

Title: McEliece cryptosystem based on LDPC codes
Place: University of Bergen, Norway
Date: October 2007

Invited Papers

IEEE GlobalSIP 2016 – Symposium on Information Theoretic Approaches to Security and Privacy

Title: Achieving semantic security without keys through coding and all-or-nothing transforms over wireless channels
Authors: Marco Baldi, Linda Senigagliesi, Franco Chiaraluce
Place: Washington, D.C.
Date: December 2016

Coordination of research groups

Cyber Security Group of Marche Polytechnic University
(cybsec.univpm.it)

Coordinator of the computer science/telecommunications interdisciplinary research group on cyber security of Marche Polytechnic University and director of the local node of the Cyber Security National Laboratory of the National Inter-University Consortium for Information Technology (CINI), coordinated by University of Rome La Sapienza.

Coordination of research projects

Enhancing communication security by cross-layer physical and data-link techniques (ESCAPADE)
(escapade.dii.univpm.it)
Funded by the Ministry of Education, University and Research (MIUR)

Marco Baldi was the national coordinator of the three-year (extended to four-year) research project ESCAPADE (Protocol RBFR105NLC), funded by the Italian Ministry of Education, University and Research within the "FIRB - Futuro in Ricerca 2010" call, recognized as a high qualification research program under the Ministerial Decree July 1, 2011 n. 276. The project was one of 99 projects funded out of 2416 applications on a national basis.
The research activity of the project was focused on communications security issues at the physical level and cryptography for secure transmission. These activities have produced 20 publications in international journals, 2 books, 3 book chapters, 27 publications in conference proceedings and 2 patents, as well as dissemination and informative results.
The project involved a second national research unit at the University of Padua (coordinated by Prof. Stefano Tomasin) and three research units with foreign institutions (Zurich University, Georgia Institute of Technology and University of Porto).
Duration: 8/03/2012 - 3/7/2016.
overall budget: Euro 426'500.
MIUR grant: Euro 336'050.

Participation in research projects

PROTotype of Off-line COrreLator for Arraying of large Aperture Antennas (PROTOCOL-A.3)
Funded by the European Space Agency (ESA / ESOC)

The PROTOCOL-A.3 project has the aim of studying and implementing numerical techniques for off-line combination of satellite signals received by antennas of multiple Earth stations, in order to improve the downlink transmission performance while avoiding the need to resort to Earth antennas of large size.
Partners: Arpsoft S.r.l., Zelinda Ireland L.t.d., Marche Polytechnic University, Université Catholique de Louvain, National Institute of Astrophysics - Arcetri Observatory.
Period: 2016-2017.

Federated Cloud Security (FCLOSE)
Funded by Marche Polytechnic University

The FCLOSE project is an interdisciplinary project funded by Marche Polytechnic University after a competitive call on a university basis (call "University Scientific Research of type B - 2015"). The project aims to study new techniques for the security of data stored in distributed and federated cloud infrastructures, following approaches drawn from the disciplines of information technology, telecommunications, and operational research.
Partners: Marche Polytechnic University.
Period: 2015-2017.

Reliable TT&C during superior solar conjunctions (RESCUe)
Funded by the European Space Agency (ESA/ESOC)

Role: Collaborator
The RESCUe Project is aimed at designing new coding and modulation techniques for telemetry, tracking, and command communications with spacecrafts during superior solar conjunctions and in the presence of solar scintillation. Partners: Arpsoft S.r.l., CNIT (Marche Polytechnic University), Thales Alenia Space Italy. Period: 2015-2016.

Next Generation Uplink Coding Techniques (NEXCODE)
Funded by the European Space Agency (ESA/ESTEC)

Role: Collaborator
The NEXCODE Project is aimed at designing and implementing error correcting coding techniques for the new telecommand standard for near Earth and deep space missions. The new codes will be included in the next CCSDS recommendations for telecommands and their impact on the overall TT&C transponder architecture will be investigated. Partners: DEIMOS Engenharia, CNIT (University of Bologna, Polytechnic of Turin, Marche Polytechnic University), CTTC Barcelona, Thales Alenia Space Italy. Period: 2014-2015.

Advanced Coding Schemes for Direct Sequence Spread Spectrum Telecommand Links
Funded by the European Space Agency (ESA/ESTEC)

Role: Collaborator
The Project was aimed at studying and assessing several coding schemes for telecommand uplink transmissions under jamming attacks. In particular, coding schemes with soft-decision decoders were considered, like binary and non-binary LDPC codes, Turbo codes and soft-decision decoded BCH codes. Their performance was assessed by simulating direct sequence spread spectrum transmissions over several channels with jamming. Partners: Polytechnic of Turin, Marche Polytechnic University. Period: 2012-2013.

Support to Channel Coding Services - 2012
Funded by the European Space Agency (ESA/ESOC)

Role: Collaborator
The Project was aimed at analyzing a class of short non-binary low-density parity-check (LDPC) codes proposed for the CCSDS Next Generation Uplink (NGU) and at developing an outline for a CCSDS Green Book on the serially concatenated convolutional codes (SCCCs) included in the CCSDS recommendation. Partners: Polytechnic of Turin, Marche Polytechnic University, University of Bologna. Period: 2012.

Non Invasive Monitoring by Ultra wide band Radar of Respiratory Activity of people inside a spatial environment (NIMURRA)
Funded by the Italian Space Agency (ASI)

Role: Collaborator
The Project was aimed at studying the feasibility and performance of a radar exploiting ultra-short pulses for non-invasive monitoring of some vital signs of astronauts, like their breathing frequency. Marco Baldi took part in a research unit that studied and optimized suitable digital signal processing algorithms to extract the breathing parameters from the received waveforms. Partners: University of Rome La Sapienza, Marche Polytechnic University, University of L'Aquila, University of Bologna, Advanced Computer Systems (ACS) and Kayser Italia. Period: 2011.

Support to Channel Coding Services
Funded by the European Space Agency (ESA/ESOC)

Role: Collaborator
The Project had several goals: to update the estimates of the coding gain achievable by the recommended techniques for use in space missions, to evaluate the feasibility of asynchronous data packetization between transport protocols and coding techniques, to evaluate the performance of ARQ techniques based on the go-back-n scheme, to evaluate the consequences of some possible choices for the synchronization patterns, to study the performance of the LDPC codes proposed by NASA for new generation uplink channels. Moreover, the project activity has included the revision of the documents aimed at updating the current CCSDS standards on modulation and coding techniques for space telecommand and telemetry data. Partners: Marche Polytechnic University. Period: 2010.

Randomizer for High Data Rates
Funded by the European Space Agency (ESA/ESOC)

Role: Collaborator
The Project had the aim to study some issues concerning the presence of spurious frequencies in satellite transmissions towards the Earth. In more detail, the study has been focused on a transmission randomization system included in the CCSDS recommendations, and some new possible solutions have been proposed, for such component, in order to reduce the presence of spurious frequencies in randomized transmissions. Partners: Polytechnic of Turin, Marche Polytechnic University. Period: 2009.

DIGIMarche.Dt: regional portal for T-Government services (in Italian)
Funded by Marche Regional Administration

Role: Collaborator
The aim of the Project was to implement a hardware and software infrastructure for broadcasting interactive contents on the digital terrestrial television platform. Such infrastructure allows to use the digital terrestrial television medium to provide regional services and information. This provides the citizens with several services from the local government, already available through the Internet, also via the digital terrestrial television medium, and to experiment applications for the health care. Partners: Marche Polytechnic University, University of Macerata, University of Camerino, University of Urbino, TV Centro Marche, Teleadriatica, R.T.M - PicusTv and Tvrs. Period: 2007-2009.

Responsibility of local research projects

Marco Baldi has been responsible of the following projects funded by Marche Polytechnic University through the competitive (on a department basis) annual call "University Scientific Research of type A":

- Post-quantum techniques for information security
  - Year: 2012
  - Financing: Euro 6'249.094
- Code-based encryption and digital signature schemes
  - Year: 2013
  - Financing: 7'322.00 Euro 1'269.00 Euro + (exceptional contribution)
- Information security techniques for distributed systems
  - Year: 2014
  - Financing: 4'248.40 Euro
- New solutions for the security and reliability of digital transmissions
  - Year: 2015
  - Financing: 4'103.41 Euro
- Coding techniques for information security at the physical layer
  - Year: 2016
  - Financing: 3'575.98 Euro

Collaborations with companies and research institutions

Company/Institution

Description

Videx Electronics S.p.A.

Role: Responsible
Project aimed at the analysis of the state of the art of design techniques of systems and protocols for reliability and security of multimedia communications. In particular, the activity was focused on networks based on IP protocols, with particular reference to the transmission of signaling and media data necessary for the implementation of communication services such as telephony and video over IP.
Partners: Marche Polytechnic University. Period: 2016.

CNIT

Role: Collaborator
Analysis of alternative encoding schemes to those currently in use for telecommand and telemetry in space missions in presence of solar scintillation.
Period: June-July 2016.

CNIT

Role: Collaborator
Optimization of simulation programs for decoding the new LDPC codes proposed for telecommands in space missions.
Period: November 2015.

Telecom Italia S.p.A.

Role: Collaborator
Project aimed at the optimization of vectored DMT techniques and the study of methods for the protection from impulsive noise. Within this project, the contribution of the Università Politecnica delle Marche has been to develop analytical models and numerical simulators for studying the effects of vectored transmission techniques in VDSL systems. The study has aimed at estimating the effective advantage achievable by such transmission techniques in some scenarios of practical interest. Partners: Polytechnic of Turin, Marche Polytechnic University. Period: 2009.

Siemens S.p.A.

Role: Collaborator
Project aimed at the study and design of LDPC codes with structured parity-check matrices for the usage in medium and high data rate radio links. The activity has been focused on quasi-cyclic (QC) LDPC codes, and on the QC-LDPC codes included in the IEEE 802.16e standard. Furthermore, techniques for designing QC-LDPC codes have been studied, aimed at satisfying specific requirements on complexity and channel adaptation. Partners: Centro Radioelettrico Sperimentale G. Marconi, Marche Polytechnic University.
Period: 2006.

Siemens S.p.A.

Role: Collaborator
Project aimed at the analysis and design of LDPC codes for application in radio links. For this purpose, specific families of LDPC codes have been studied and designed, in order to be able to adapt their characteristics to the channel quality. Partners: Centro Radioelettrico Sperimentale G. Marconi, Marche Polytechnic University.
Period: 2005.

COST Actions

IC1306 (Cryptography for Secure Digital Interaction)

Role: MC Substitute for Italy.

IC1104 (Random Network Coding and Designs over GF(q))

Role: Member of the Working Group 3 on "Cryptographic Aspects of Network Codes".

Professional Memberships and Services

Institute of Electrical and Electronics Engineers (IEEE)

Member since 2009 and Senior Member since 2013.

Italian Federation of Electrotechnics, Electronics, Automatics, Informatics and Telecommunications (AEIT)	Member since 2009 and secretary of the Adriatic section for the period 2011-2013.
European Association for Communications & Networking (EURACON)	Member since 2013.
National Inter-University Consortium for Telecommunications (CNIT)	Member since 2010.
Italian Group of Telecommunications and Information Technology (GTTI)	Member since 2009.
National Association of Engineers - Macerata branch	Member since 2004 and member of the Information Technology Commission since 2016.

University Teaching

Privacy and Security of Biomedical Data
Master of Science in Biomedical Engineering of Marche Polytechnic University.
Academic Years: 2016-2017.
Hours: 48, language: English.
Role: Professor

Topics:
Principles of information theory. Principles of data reliability. Principles of security and cryptography. Symmetric and asymmetric encryption. DES, AES, RSA, ElGamal cryptographic systems. Hash functions and digital signatures. Network security protocols. Privacy, reliability and security in biomedical systems. Software excercises on security techniques.

Telecommunications Network Security
Master of Science in Electronic Engineering of Marche Polytechnic University.
Academic Years: 2012-2013, 2013-2014, 2014-2015, 2015-2016, 2016-2017.
Hours: 72, language: Italian.
Role: Professor

Topics:
Principles of information security and cryptography. Principles of number theory. Principles of information and coding theory. Private-key and public-key cryptography (DES, AES, RSA). Cryptographic systems based on error correcting codes. Hash functions. Digital signatures. Protocols for networks security. Physical layer security.

Octave for PhD students
Octave course for PhD students of Marche Polytechnic University.
Academic year: 2016-2017.
Hours: 18, language: English.
Role: Professor

Topics:
Introduction to Octave, variables, data structures and their manipulation. Writing scripts and using the debugger. Reading and writing of data files. Tools for creating and controlling the appearance of graphics and two-dimensional and three-dimensional figures. Evaluation of functions. Numerical solution, integration and optimization. Software excercises.

Matlab / Octave
Advanced course for "Technician for the application of home automation technologies for living environments" of Marche Polytechnic University.
Year: 2016.
Hours: 12, language: Italian.
Role: Professor

Topics:
Introduction to Matlab and Octave, installation and user interface. Variables and data structures. Scripts and functions. Data analysis tools. Graphic design tools. Writing basic programs.

Matlab / Octave
Advanced course for "Technician-Researcher for the development of home automation technologies for living environments" of Marche Polytechnic University.
Year: 2016.
Hours: 12, language: Italian.
Role: Professor

Topics:
Introduction to Matlab and Octave, installation and user interface. Variables and data structures. Scripts and functions. Overview of the functions included in the library. Data analysis and statistical tools. Graphic functions. Writing advanced programs.

Wireless Networks
Master of Science in Electronic Engineering of Marche Polytechnic University.
Academic Years: 2007-2008, 2008-2009, 2009-2010.
Hours: 72, language: Italian.
Role: Professor

Topics:
Principles of telecommunications networks. Principles of antennas and propagation. Spread spectrum techniques. IEEE 802.11 and 802.15.4 standards. Wired and wireless network protocols. Wireless network configurations. Security techniques for wired and wireless networks.

Signal Theory
Bachelor in Information Technology and Automation Engineering of Marche Polytechnic University.
Academic Years: 2005-2006, 2006-2007.
Hours: $\approx$ 70, language: Italian.
Role: Assistant

Topics:
Spectral analysis of signals. Principles of the fast Fourier transform. Using Matlab for the spectral analysis of signals. Supervision of students and tutorials.

Telecommunications
Bachelor in Electronic Engineering of Marche Polytechnic University.
Academic Years: 2005-2006.
Hours: ≈ 70, language: Italian.
Role: Assistant

Topics:
Using Matlab and Simulink for the implementation and simulation of transmission schemes with modulation and coding over Gaussian channels. Supervision of students and tutorials.

Telecommunication Systems
Bachelor in Electronic Engineering of Marche Polytechnic University.
Academic Years: 2004-2005.
Hours: ≈ 70, language: Italian.
Role: Assistant

Topics:
Use of Matlab and Simulink to implement and simulate telecommunication systems. Supervision of students and tutorials.

Other
Lectures, tutorials and seminars on specific topics for courses of Bachelor and Master of Science of Marche Polytechnic University.

Courses:

- Information Theory and Codes
- Numerical Transmissions
- Signal Theory
- Telecommunications
- Telecommunications II
- Telecommunication Services
- Telecommunication Systems II
- Wireless Networks

Participation in PhD Course Committees

- Committee member of the PhD course in Information Engineering of Marche Polytechnic University.
  - Academic years: 2013-2014, 2014-2015, 2015-2016, 2016-2017.

Participation in PhD Exam Commissions abroad

- Extern examiner for Ian Mulholland's PhD final exam at University College Dublin.
  - January-March 2016

Supervision of Research Fellows

- Supervisor of **Dr. Nicola Maturo** (2016), Research Fellow at the Department of Information Engineering of Marche Polytechnic University on the topic "Design and analysis of techniques for reliability and security of space telecommunications".
- Supervisor of **Dr. Marco Bianchi** (2013), Research Fellow at the Department of Information Engineering of Marche Polytechnic University on the topic "Design and analysis of new telecommunications security techniques at the physical layer".

Supervision of PhD students

- Co-supervisor of **Massimo Battaglioni**, PhD student at the Department of Information Engineering of Marche Polytechnic University on the topic "Design and analysis of LDPC convolutional codes".
- Co-supervisor of **Linda Senigagliesi**, PhD student at the Department of Information Engineering of Marche Polytechnic University on the topic "Coding and information processing techniques for security of cloud storage systems".
- Co-supervisor of **Giacomo Ricciutelli**, PhD student at the Department of Information Engineering of Marche Polytechnic University on the topic "Advanced coding techniques for reliability and security".

Supervision of Contract Researchers

- Supervisor of the research activity of **Giacomo Ricciutelli** (2014) at the Department of Information Engineering of Marche Polytechnic University on the topic "Development of tools and algorithms for the study of coded transmissions over broadcast channels with confidential messages".

Participation in University Boards

Master of Science Examination Committee at Marche Polytechnic University

- Member of the Master of Science in Electronic Engineering Examination Committee, 19/10/2016.
- Member of the Master of Science in Electronic and Telecommunications Engineering Examination Committee, 18/02/2016.
- Member of the Master of Science in Electronic Engineering Examination Committee, 20/10/2015.
- Member of the Master of Science in Electronic Engineering Examination Committee, 17/12/2014.
- Member of the Master of Science in Electronic and Telecommunications Engineering Examination Committee, 19/02/2014.
- Member of the Master of Science in Electronic and Telecommunications Engineering Examination Committee, 16/10/2013.

Evaluation boards at Marche Polytechnic University

- Chairman of the Selection Committee for Research Fellowship at Marche Polytechnic University, designated by D.R. n. 1065 of 11.30.2015.
- Chairman of the Selection Committee for Research Fellowship at Marche Polytechnic University, designated by D.R. n. 353 of 15/02/2013.
- Member of the Selection Committee for the assignment to persons outside the University of a job with freelance work contract of occasional nature - notice made public on 9/10/2012.

Supervision of BSc and MSc Dissertations (in Italian)

BSc = three-year Laurea degree, equivalent to BSc.
MSc = two-year post-BSc Laurea degree, equivalent to MSc.
MSc* = five-year Laurea degree, equivalent to BSc+MSc.

Academic Year	Student	Title	Type	Role
2015-2016	D. Sciarroni	Blockchain techniques for digital signatures	MSc	Supervisor
2015-2016	L. Incipini	Secret key distillation techniques for passive optical networks	MSc	Supervisor
2015-2016	P. Santini	Design of QC-LDPC code-based cryptosystems with compact keys	MSc	Supervisor
2015-2016	A. Baazoui	Design of LDPC codes optimized for binary symmetric channels	BSc	Supervisor
2015-2016	R. Vaira	Analysis of the properties of ordered statistics decoding algorithms	MSc	Asst. supervisor
2014-2015	L. Ribichini	Optimization of decoding algorithms based on ordered lists	BSc	Asst. supervisor
2014-2015	G. Fabi	Space-time codes and their application in space links	BSc	Asst. supervisor
2014-2015	D. Sampaolo	Role and problems of molecular communications in the field of nano-networks	BSc	Asst. supervisor
2014-2015	L. Gorgoni	Advanced design schemes LDPC convolutional codes	MSc	Asst. supervisor
2014-2015	L. Senigagliesi	Physical layer security achievable through practical coding and modulation schemes	MSc	Supervisor
2014-2015	M. Battaglioni	LDPC convolutional codes: analysis and design through approaches based on number theory	MSc	Supervisor
2014-2015	L. Cinti	Analysis and design of LDPC and CRC concatenated coding schemes for error detection	MSc	Supervisor
2014-2015	S. Felici	Computation of generator matrices for array QC-LDPC codes	BSc	Asst. supervisor
2014-2015	M. Romiti	Analysis and simulation of phase errors for coherent modulations over fading channels	BSc	Asst. supervisor

2013-2014	L. Bordoni	Analysis of finite length polar codes for transmission security at the physical layer	MSc	Supervisor
2013-2014	P. Santini	Attacks against the McEliece cryptosystem based on continuous alphabets	BSc	Supervisor
2013-2014	L. Visconti	Analysis of cryptographic primitives for cryptocurrency protocols	BSc	Supervisor
2013-2014	N. Bacchetti	Design of concatenated McDonald codes for error detection in numerical transmissions	BSc	Asst. supervisor
2013-2014	M. Tarquini	Analysis of error correcting codes for space missions affected by solar scintillation	BSc	Asst. supervisor
2012-2013	M. Esposito	Cryptanalysis of a new digital signature system based on error correcting codes	MSc	Supervisor
2012-2013	D. Viozzi	McEliece-like cryptosystems on continuous alphabets	MSc	Supervisor
2012-2013	E. Montali	Cloud security: techniques based on error correcting codes	MSc	Asst. supervisor
2012-2013	G. Ricciutelli	LDPC codes with unequal error protection for physical layer security	MSc	Asst. supervisor
2012-2013	E. Casagrande	Study of differentiated protection classes in LDPC codes	BSc	Asst. supervisor
2011-2012	A. Mengaroni	Performance assessment of physical layer security protocols on the OpenWRT platform	BSc	Asst. supervisor
2011-2012	A. Paolucci	Physical layer security in 802.11 wireless networks	BSc	Asst. supervisor
2011-2012	M. Mengoni	Analysis and simulation of an analog UWB radar for vital parameters monitoring	MSc	Asst. supervisor
2011-2012	M. Luciani	Jamming effects in satellite communications	MSc	Asst. supervisor
2011-2012	N. Maturo	Efficiency of physical layer security in 802.11 wireless networks	MSc	Asst. supervisor
2011-2012	T. Altomeni	Theoretical limits for OFDM systems with physical layer security	MSc	Asst. supervisor
2011-2012	W. Gualà	Physical layer security for 802.11 transmissions	MSc	Asst. supervisor
2011-2012	R. Lombardi	Implementation of Linux applications and integration into open source 802.11 wireless routers	BSc	Asst. supervisor
2010-2011	F. Amabili	Analysis of Davydov codes for error detection	BSc	Asst. supervisor
2010-2011	G. Rogante	Coding techniques for physical layer security	MSc	Asst. supervisor
2010-2011	A. Colabella	Software simulations of an optical network client	BSc	Asst. supervisor
2010-2011	G. Scarpetti	Dynamic bandwidth allocation in passive optical networks	MSc	Asst. supervisor
2010-2011	M. Ciarrocchi	Analysis and simulation of passive optical networks	MSc	Asst. supervisor
2010-2011	T. Zulli	Analysis of the properties of codes to be used in digital signature systems	BSc	Asst. supervisor
2010-2011	F. Venieri	Simulation of techniques for respiration monitoring through wearable UWB radars	BSc	Asst. supervisor
2010-2011	E. Montali	Physical layer security in OFDM systems	BSc	Asst. supervisor
2010-2011	M. Mengoni	Analysis and simulation of an analog UWB radar for vital parameters monitoring	BSc	Asst. supervisor
2010-2011	F. Appignani	Effects of movement in the estimation of vital parameters through UWB radars	BSc	Asst. supervisor
2009-2010	V. La Mantia	Optimization of algorithms for monitoring the vital functions through UWB radars	BSc	Asst. supervisor
2009-2010	G. Ricciutelli	Modified WEP protocol for the IEEE 802.11 standard	BSc	Asst. supervisor
2009-2010	G. Pierpaoli	Genetic sequences: possible role of channel coding	MSc	Asst. supervisor
2009-2010	A. Perelli	Permutation-based coding for flash memories applications	MSc	Asst. supervisor
2009-2010	F. Di Bartolomeo	Performance analysis of error correcting codes for NAND flash memories	BSc	Asst. supervisor
2009-2010	V. Xheka	Implementation and verification of the AES algorithm	BSc	Asst. supervisor
2009-2010	V. Lamaj	Implementation and verification of the RSA algorithm	BSc	Asst. supervisor
2008-2009	L. Belfiori	Study of truncation effects on pseudo-random binary sequences	BSc	Asst. supervisor
2008-2009	C. Bianconi	Acquisition of analog and digital signals and their modulation through Matlab/Simulink	BSc	Asst. supervisor
2008-2009	A. Annibaldi	Analog and digital modulation techniques and schemes in Matlab/Simulink	BSc	Asst. supervisor
2008-2009	N. Maturo	Implementation of chaotic algorithms for generating pseudo-random sequences	BSc	Asst. supervisor

2008-2009	L. De Rosa	OpenVPN: a solution for security in wireless networks	MSc*	Asst. supervisor
2008-2009	Y. Toto	New attacks to cryptographic protocols for wireless systems	MSc*	Asst. supervisor
2007-2008	L. Gianfelici	Numerical analysis of low density codes for error correction	MSc*	Asst. supervisor
2007-2008	M. Moretti	Performance analysis of UWB radars for estimating physiological parameters	BSc	Asst. supervisor
2007-2008	F. Lucconi	Algorithms for breath monitoring through UWB signals	BSc	Asst. supervisor
2006-2007	M. Ciarrocchi	Soft-iterative decoding of binary cyclic codes	BSc	Asst. supervisor
2005-2006	F. Costantini	Implementation of advanced functions on object carousel generation servers	BSc	Asst. supervisor
2004-2005	L. Gramillano	Automatic updating of the interactive contents of DVB transmissions	MSc*	Asst. supervisor
2004-2005	S. Rossetti	Implementation aspects of iterative decoding algorithms	BSc	Asst. supervisor
2004-2005	G. La Porta	Algorithms for estimating the minimum distance of LDPC codes	MSc*	Asst. supervisor
2004-2005	D. Possanzini	Analysis of error correcting codes for asymmetric channels	MSc*	Asst. supervisor
2004-2005	G. Morlacchi	MHP application for dynamic content browsing in DVB-T	MSc*	Asst. supervisor
2004-2005	G. Alessandrelli	Linux-based applications for managing interactive contents in DVB	MSc*	Asst. supervisor
2004-2005	A. De Santis	Remote control of video-surveillance applications	MSc*	Asst. supervisor
2004-2005	M. Menzietti	Organization of the Audio/Video/Data steam in a DVB-T Transport Stream	BSc	Asst. supervisor
2004-2005	M. Baldini	Spreading techniques for Wireless LAN systems	MSc*	Asst. supervisor
2004-2005	N. Volgarino	Interleavers and codecs for high data rate radio links	MSc*	Asst. supervisor

Presentations given at international conferences

With reference to the list of publications reported below, Marco Baldi has presented the following works at international conferences: [44, 46, 47, 63, 68, 71, 75, 77, 80, 82, 84, 87, 97, 99, 101, 98, 108, 113, 109, 116].

Contributions to meetings of the Consultative Committee for Space Data Systems (CCSDS)

- CCSDS Fall 2015 meeting, Darmstadt, Germany, November 2015:
  - M. Bertinelli, M. Baldi, F. Chiaraluce, N. Mature, E. Paolini, R. Garello, "CLTU termination issues".
- CCSDS Fall 2014 meeting, London, UK, October 2014:
  - M. Bertinelli, M. Baldi, F. Chiaraluce, N. Mature, E. Paolini, M. Chiani, R. Garello, P. Dhakal, "CLTU termination techniques for TC links".
  - M. Bertinelli, M. Baldi, F. Chiaraluce, N. Mature, E. Paolini, M. Chiani, R. Garello, P. Dhakal, "Performance / complexity trade-offs for TC LDPC codes".
- CCSDS Spring 2014 meeting, Noordwijkerhout, The Netherlands, April 2014:
  - M. Baldi, F. Chiaraluce, R. Garello, E. Paolini, M. Chiani, M. Navarro, S. Pfletschinger "Analysis of some issues in TC coding update".
- CCSDS Spring 2013 meeting, Bordeaux, France, April 2013:
  - M. Baldi, M. Bianchi, F. Chiaraluce, "Performance Assessment of the (128, 64) Binary LDPC Code with MRB Decoding".
  - R. Garello, F. Chiaraluce, M. Baldi, M. Bianchi, I. Aguilar Sanchez, S. Cioni, "Alternative Coding Options for TC".
  - M. Baldi, M. Bianchi, F. Chiaraluce, E. Paolini, M. Chiani, G. P. Calzolari, "Performance and Complexity Assessment of Some Decoding Strategies for Non-Binary LDPC codes".
  - R. Garello, F. Chiaraluce, M. Baldi, M. Bianchi, I. Aguilar Sanchez, S. Cioni, "TC Advanced Coding for Direct Sequence Spread Spectrum".
- CCSDS Fall 2012 meeting, Cleveland, USA, October 2012:
  - M. Baldi, M. Chiani, F. Chiaraluce, E. Paolini, "Some results on NGU coding schemes".
- CCSDS Fall 2011 meeting, Boulder, Colorado, USA, November 2011:

  - Marco Baldi, Franco Chiaraluce, Gian Paolo Calzolari, "Updates to TC Green Book CCSDS 230.1-G-2 - Boulder version".
  - Marco Baldi, Franco Chiaraluce, Gian Paolo Calzolari, "Updates to TM Green Book CCSDS 130.1-G - Boulder version".
- CCSDS Spring 2011 meeting, Berlin, Germany, May 2011:
  - Marco Baldi, Franco Chiaraluce, Gian Paolo Calzolari, "Updates to TC Green Book CCSDS 230.1-G-2".
  - Marco Baldi, Franco Chiaraluce, Gian Paolo Calzolari, "Choice of truncation length for convolutional decoding".
  - Marco Baldi, Franco Chiaraluce, Gian Paolo Calzolari, "Updates to TM Green Book CCSDS 130.1-G-1".
  - Marco Baldi, Franco Chiaraluce, Gian Paolo Calzolari, "Effect of randomization on the ASM".
- CCSDS Fall 2010 meeting, London, England, October 2010:
  - Marco Baldi, Franco Chiaraluce, Gian Paolo Calzolari, "Effect of some non-idealities on the performance of channel codes for space missions".
- CCSDS Fall 2009 meeting, Noordwijk, The Netherlands, November 2009:
  - Marco Baldi, Franco Chiaraluce, Gian Paolo Calzolari, "Performance evaluation of a go-back-n scheme with multiple copies".
- CCSDS Spring 2009 meeting, Colorado Springs, USA, April 2009:
  - Roberto Garello, Marco Baldi, Franco Chiaraluce, Gian Paolo Calzolari, "Summary of High Data Rate Randomizer investigations".
- CCSDS Fall 2008 meeting, Berlin, Germany, October 2008:
  - Marco Baldi, Franco Chiaraluce, Gian Paolo Calzolari, Roberto Garello "Randomizer for high data rates - Some proposals against the problem of spectral spurious".

Contributions to revision and updating of CCSDS Green Books and Blue Books

- CCSDS Green Book on TM Synchronization and Channel Coding (CCSDS 130.1-G-1)
- CCSDS Green Book on TC Synchronization and Channel Coding (CCSDS 230.1-G-2)

Bibliometric Indices

Google scholar: h-index 16 (total citations 871)
Scopus: h-index 11 (total citations 531)

Publications

Journal Publications

[1] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani. "Enhanced Public Key Security for the McEliece Cryptosystem". In: *Journal of Cryptology* 29.1 (2016), pp. 1–27.

[2] M. Baldi, N. Maturo, E. Paolini, and F. Chiaraluce. "On the use of ordered statistics decoders for low-density parity-check codes in space telecommand links". In: *EURASIP Journal on Wireless Communications and Networking* 2016.272 (2016), pp. 1–15.

[3] M. Baldi, F. Chiaraluce, R. Garello, N. Maturo, I. Aguilar Sanchez, and S. Cioni. "Analysis and performance evaluation of new coding options for space telecommand links - Part I: AWGN channels". In: *International Journal of Satellite Communications and Networking* 33.6 (2015), pp. 509–525.

[4] M. Baldi, F. Chiaraluce, R. Garello, N. Maturo, I. Aguilar Sanchez, and S. Cioni. "Analysis and performance evaluation of new coding options for space telecommand links - Part II: jamming channels". In: *International Journal of Satellite Communications and Networking* 33.6 (2015), pp. 527–542.

[5] M. Baldi, G. Cerri, F. Chiaraluce, L. Eusebi, and P. Russo. "Non-invasive UWB sensing of astronauts' breathing activity." In: *Sensors (Basel, Switzerland)* 15.1 (2015), pp. 565–91.

[6] M. Baldi, N. Maturo, G. Ricciutelli, and F. Chiaraluce. "Security gap analysis of some LDPC coded transmission schemes over the flat and fast fading Gaussian wire-tap channels". In: *EURASIP Journal on Wireless Communications and Networking* 2015.1 (2015), p. 232.

[7] M. Baldi, G. Cancellieri, and F. Chiaraluce. "Array Convolutional Low-Density Parity-Check Codes". In: *IEEE Communications Letters* 18.2 (2014), pp. 336–339.

[8] M. Baldi, F. Chiaraluce, N. Laurenti, S. Tomasin, and F. Renna. "Secrecy Transmission on Parallel Channels: Theoretical Limits and Performance of Practical Codes". In: *IEEE Transactions on Information Forensics and Security* 9.11 (2014), pp. 1765–1779.

[9] M. Baldi, F. Chiaraluce, N. Maturo, G. Liva, and E. Paolini. "A Hybrid Decoding Scheme for Short Non-Binary LDPC Codes". In: *IEEE Communications Letters* 18.12 (2014), pp. 2093–2096.

[10] M. Baldi, M. Bianchi, N. Maturo, and F. Chiaraluce. "A Physical Layer Secured Key Distribution Technique for IEEE 802.11g Wireless Networks". In: *IEEE Wireless Communications Letters* 2.2 (2013), pp. 183–186.

[11] M. Baldi, F. Chiaraluce, and M. Bianchi. "Security and complexity of the McEliece cryptosystem based on quasi-cyclic low-density parity-check codes". In: *IET Information Security* 7.3 (2013), pp. 212–220.

[12] M. Baldi, M. Bianchi, G. Cancellieri, and F. Chiaraluce. "Progressive Differences Convolutional Low-Density Parity-Check Codes". In: *IEEE Communications Letters* 16.11 (2012), pp. 1848–1851.

[13] M. Baldi, M. Bianchi, and F. Chiaraluce. "Coding With Scrambling, Concatenation, and HARQ for the AWGN Wire-Tap Channel: A Security Gap Analysis". In: *IEEE Transactions on Information Forensics and Security* 7.3 (2012), pp. 883–894.

[14] M. Baldi, M. Bianchi, F. Chiaraluce, and T. Klove. "A Class of Punctured Simplex Codes Which Are Proper for Error Detection". In: *IEEE Transactions on Information Theory* 58.6 (2012), pp. 3861–3880.

[15] M. Baldi, G. Cancellieri, and F. Chiaraluce. "Interleaved Product LDPC Codes". In: *IEEE Transactions on Communications* 60.4 (2012), pp. 895–901.

[16] M. Baldi, F. Chiaraluce, A. de Angelis, R. Marchesani, and S. Schillaci. "A comparison between APSK and QAM in wireless tactical scenarios for land mobile systems". In: *EURASIP Journal on Wireless Communications and Networking* 2012.1 (2012), p. 317.

[17] M. Baldi, F. Bambozzi, and F. Chiaraluce. "On a Family of Circulant Matrices for Quasi-Cyclic Low-Density Generator Matrix Codes". In: *IEEE Transactions on Information Theory* 57.9 (2011), pp. 6052–6067.

[18] M. Baldi, F. Chiaraluce, R. Garello, M. Polano, and M. Valentini. "Analytical evaluation of the role of estimation and quantization errors in downstream vectored VDSL systems". In: *International Journal On Advances in Telecommunications* 4.1 and 2 (2011), pp. 24–33.

[19] M. Baldi, E. Zanaj, and F. Chiaraluce. "Performance Evaluation of Some Distributed Averaging Algorithms for Sensor Networks". In: *International Journal of Distributed Sensor Networks* 2011 (2011), pp. 1–11.

[20] M. Baldi, G. Cancellieri, F. Chiaraluce, and A. De Amicis. "Regular and irregular Multiple Serially-Concatenated Multiple-Parity-Check codes for wireless applications". In: *Journal of Communications Software and Systems* 5.4 (2010), pp. 140–148.

[21] M. Baldi, G. Cancellieri, and F. Chiaraluce. "Exploiting Concatenation in the Design of Low-Density Parity-Check Codes". In: *International Journal On Advances in Telecommunications* 3.1 and 2 (2010), pp. 28–38.

[22] M. Baldi, F. Chiaraluce, N. Boujnah, and R. Garello. "On the Autocorrelation Properties of Truncated Maximum-Length Sequences and Their Effect on the Power Spectrum". In: *IEEE Transactions on Signal Processing* 58.12 (2010), pp. 6284–6297.

[23] M. Baldi, F. Chiaraluce, R. Garello, M. Polano, and M. Valentini. "Simple Statistical Analysis of the Impact of Some Nonidealities in Downstream VDSL with Linear Precoding". In: *EURASIP Journal on Advances in Signal Processing* 2010.1 (2010), pp. 1–14.

[24] M. Baldi, G. Cancellieri, A. Carassai, and F. Chiaraluce. "LDPC codes based on serially concatenated multiple parity-check codes". In: *IEEE Communications Letters* 13.2 (2009), pp. 142–144.

[25] M. Baldi, F. Chiaraluce, and G. Cancellieri. "Finite-Precision Analysis of Demappers and Decoders for LDPC-Coded M-QAM Systems". In: *IEEE Transactions on Broadcasting* 55.2 (2009), pp. 239–250.

[26] M. Baldi, E. Gambi, and S. Spinsante. "Delivery of Academic Lectures Through DVB-T and MHP Applications". In: *IEEE Broadcast Technology Society Newsletter* 17.1 (2009), pp. 24–25.

[27] E. Zanaj, M. Baldi, and F. Chiaraluce. "Optimal share factors in the push-sum algorithm for ring and random geometric graph sensor networks". In: *Journal of Communications Software and Systems* 5.1 (2009), pp. 9–18.

[28] M. Baldi, G. Cancellieri, and F. Chiaraluce. "Iterative soft-decision decoding of binary cyclic codes". In: *Journal of Communications Software and Systems* 4 (2) (2008), pp. 142–149.

[29] M Baldi and F Chiaraluce. "A simple scheme for belief propagation decoding of BCH and RS codes in multimedia transmissions". In: *International Journal of Digital Multimedia Broadcasting* (2008).

[30] M. Baldi, F. Chiaraluce, and T. Klove. "Exact and Approximate Expressions for the Probability of Undetected Errors of Varshamov–Tenengol'ts Codes". In: *IEEE Transactions on Information Theory* 54.11 (2008), pp. 5019–5029.

[31] E. Zanaj, M. Baldi, and F. Chiaraluce. "Efficiency of unicast and broadcast gossip algorithms for wireless sensor networks". In: *Journal of Communications Software and Systems* 4 (2008), pp. 105–112.

[32] M. Baldi and F. Chiaraluce. "On the design of punctured low density parity check codes for variable rate systems". In: *Journal of Communications Software and Systems* 1 (2005), pp. 88–100.

Books

[33] M. Baldi. *QC-LDPC Code-Based Cryptography*. Springer, 2014, p. 120.

Book Chapters

[34] M. Baldi, F. Chiaraluce, N. Maturo, and S. Tomasin. "Performance Analysis of Transmission over AWGN Wiretap Channels with Practical Codes". In: *Physical and Data-Link Security Techniques for Future Communication Systems - Vol. 358 of Lecture Notes in Electrical Engineering*. Ed. by M. Baldi and S. Tomasin. Springer, 2016. Chap. 4, pp. 53–68.

[35] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani. "Using LDGM Codes and Sparse Syndromes to Achieve Digital Signatures". In: *Post-Quantum Cryptography*. Ed. by P. Gaborit. Vol. 7932. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 1–15.

[36] M. Baldi, F. Chiaraluce, and E. Zanaj. "Performance of Gossip Algorithms in Wireless Sensor Networks". In: *Solutions on Embedded Systems*. Ed. by M. Conti, S. Orcioni, N. Martínez Madrid, and R. E. Seepold. Vol. 81. Lecture Notes in Electrical Engineering. Dordrecht: Springer Netherlands, 2011, pp. 3–16.

[37] M. Baldi and E. Gambi. "MAC Protocols for RFID Systems". In: *Radio Frequency Identification Fundamentals and Applications Bringing Research to Practice*. Ed. by C. Turcu. Vienna: InTech, 2010, pp. 73–86.

[38] M. Baldi. "LDPC Codes in the McEliece Cryptosystem: Attacks and Countermeasures". In: *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes - Vol. 23 of NATO Science for Peace and Security Series (D: Information and Communication Security)*. Ed. by B. Preneel, S. Dodunekov, V. Rijmen, and S. Nikova. IOS Press, 2009, pp. 160–174.

[39] M. Baldi, M. Bodrato, and F. Chiaraluce. “A New Analysis of the McEliece Cryptosystem Based on QC-LDPC Codes”. In: *Security and Cryptography for Networks*. Ed. by R. Ostrovsky, R. De Prisco, and I. Visconti. Vol. 5229. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 246–262.

Conference Proceedings Publications

[40] M. Baldi, L. Senigagliesi, and F. Chiaraluce. “Achieving semantic security without keys through coding and all-or-nothing transforms over wireless channels”. In: *Proc. IEEE Global Conference on Signal and Information Processing (GlobalSIP 2016)*. Greater Washington, D.C., USA, 2016, pp. 964–969.

[41] M. Baldi, M. Battaglioni, F. Chiaraluce, and G. Cancellieri. “Time-Invariant Spatially Coupled Low-Density Parity-Check Codes with Small Constraint Length”. In: *Proc. 4th IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom 2016)*. Varna, Bulgaria, 2016.

[42] M. Baldi, A. Cucchiarelli, L. Senigagliesi, L. Spalazzi, and F. Spegni. “Parametric and Probabilistic Model Checking of Confidentiality in Data Dispersal Algorithms”. In: *Proc. 11th International Workshop on Security and High Performance Computing Systems (SHPCS 2016)*. Innsbruck, Austria, 2016.

[43] M. Baldi, N. Maturo, G. Ricciutelli, and F. Chiaraluce. “On the error detection capability of combined LDPC and CRC codes for space telecommand transmissions”. In: *Proc. 21st IEEE Symposium on Computer and Communications (ISCC 2016)*. Messina, Italy, 2016, pp. 1105–1112.

[44] M. Baldi, P. Santini, and F. Chiaraluce. “Soft McEliece: MDPC code-based McEliece cryptosystems with very compact keys through real-valued intentional errors”. In: *Proc. IEEE International Symposium on Information Theory (ISIT 2016)*. Barcelona, Spain, 2016, pp. 795–799.

[45] M. Battaglioni, M. Baldi, and G. Cancellieri. “Design of Spatially Coupled LDPC Codes based on Symbolic Hyper-Graphs”. In: *Proc. International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2016)*. Split, Croatia: To be presented, 2016.

[46] M. Baldi, F. Chiaraluce, J. Rosenthal, and D. Schipani. “A modification of the McEliece cryptosystem based on Generalized Reed-Solomon codes”. In: *Effective Methods in Algebraic Geometry (MEGA 2015)*. Trento, Italy, 2015.

[47] M. Baldi, G. Ricciutelli, N. Maturo, and F. Chiaraluce. “Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel”. In: *Proc. IEEE International Conference on Communications (ICC 2015) - Workshop on Wireless Physical Layer Security*. London, UK, 2015, pp. 446–451.

[48] M. Baldi and G. Cancellieri. “Low-rate LDPC Convolutional Codes with Short Constraint Length”. In: *Proc. International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2015)*. Split-Bol, Croatia, 2015.

[49] M. Baldi, F. Chiaraluce, E. Paolini, and N. Maturo. “On the applicability of the most reliable basis algorithm for LDPC decoding in telecommand links”. In: *Proc. International Conference on Information and Communication Systems (ICICS 2015)*. Amman, Jordan, 2015.

[50] G. Ricciutelli, M. Baldi, N. Maturo, and F. Chiaraluce. “LDPC Coded Modulation Schemes with Largely Unequal Error Protection”. In: *Proc. IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom 2015)*. Costanta, Romania, 2015.

[51] M. Baldi, G. Cancellieri, and F. Chiaraluce. “Sparse generator matrices for some families of quasi-cyclic low-density parity-check codes”. In: *Proc. International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2014)*. Split, Croatia, 2014.

[52] M. Baldi, N. Maturo, E. Montali, and F. Chiaraluce. “AONT-LT: A data protection scheme for Cloud and cooperative storage systems”. In: *Proc. International Conference on High Performance Computing & Simulation (HPCS 2014)*. Bologna, Italy, 2014, pp. 566–571.

[53] M. Baldi, N. Maturo, G. Ricciutelli, and F. Chiaraluce. “LDPC coded transmissions over the Gaussian broadcast channel with confidential messages”. In: *Proc. 21st IEEE International Conference on Telecommunications (ICT 2014)*. Lisbon, Portugal, 2014, pp. 52–56.

[54] M. Baldi, N. Maturo, G. Ricciutelli, and F. Chiaraluce. “Practical LDPC coded modulation schemes for the fading broadcast channel with confidential messages”. In: *Proc. IEEE International Conference on Communications Workshops (ICC 2014)*. Sydney, Australia, 2014, pp. 759–764.

[55] E. Frontoni, M. Baldi, P. Zingaretti, V. Landro, and P. Misericordia. “Security issues for data sharing and service interoperability in eHealth systems: The Nu.Sa. test bed”. In: *Proc. International Carnahan Conference on Security Technology (ICCST 2014)*. Rome, Italy, 2014, pp. 1–6.

[56] M. Baldi, M. Bianchi, F. Chiaraluce, R. Garello, N. Maturo, I. A. Sanchez, and S. Cioni. "Advanced Coding Schemes against Jamming in Telecommand Links". In: *Proc. 2013 IEEE Military Communications Conference (MILCOM 2013)*. San Diego, USA, 2013, pp. 1220–1226.

[57] M. Baldi, M. Bianchi, F. Chiaraluce, R. Garello, I. A. Sanchez, and S. Cioni. "Advanced Channel Coding for Space Mission Telecommand Links". In: *Proc. IEEE 78th Vehicular Technology Conference (VTC Fall 2013)*. Las Vegas, USA, 2013, pp. 1–5.

[58] M. Baldi, M. Bianchi, and F. Chiaraluce. "Optimization of the parity-check matrix density in QC-LDPC code-based McEliece cryptosystems". In: *Proc. IEEE International Conference on Communications Workshops (ICC 2013)*. Budapest, Hungary, 2013, pp. 707–711.

[59] M. Baldi, M. Bianchi, N. Maturo, and F. Chiaraluce. "A practical viewpoint on the performance of LDPC codes over the fast Rayleigh fading wire-tap channel". In: *Proc. IEEE Symposium on Computers and Communications (ISCC 2013)*. Split, Croatia, 2013, pp. 000287–000292.

[60] M. Baldi, M. Bianchi, N. Maturo, and F. Chiaraluce. "A tight estimation of the security gap over the fast fading wiretap channel". In: *Proc. 9th IEEE International Wireless Communications and Mobile Computing Conference (IWCMC)*. Cagliari, Italy, 2013, pp. 143–148.

[61] M. Baldi, M. Bianchi, N. Maturo, and F. Chiaraluce. "Improving the efficiency of the LDPC code-based McEliece cryptosystem through irregular codes". In: *Proc. IEEE Symposium on Computers and Communications (ISCC 2013)*. Split, Croatia, 2013, pp. 000197–000202.

[62] N. Maturo, M. Baldi, M. Bianchi, and F. Chiaraluce. "Security gap assessment for the fast fading wiretap channel". In: *Proc. 20th IEEE International Conference on Telecommunication (ICT 2013)*. Casablanca, Morocco, 2013, pp. 1–5.

[63] N. Maturo, M. Baldi, M. Bianchi, and F. Chiaraluce. "Security gap performance of some LDPC code constructions". In: *Proc. IEEE 36th International Conference on Telecommunications and Signal Processing (TSP 2013)*. Rome, Italy, 2013, pp. 77–81.

[64] F. Renna, N. Laurenti, S. Tomasin, M. Baldi, N. Maturo, M. Bianchi, F. Chiaraluce, and M. Bloch. "Low-power secret-key agreement over OFDM". In: *Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy (HotWiSec 2013)*. Budapest, Hungary: ACM Press, 2013, p. 43.

[65] M. Baldi, F. Appignani, B. Zanaj, and F. Chiaraluce. "Body movement compensation in UWB radars for respiration monitoring". In: *Proc. 1st IEEE AESS European Conference on Satellite Telecommunications (ESTEL 2012)*. Rome, Italy, 2012.

[66] M. Baldi, M. Bianchi, G. Cancellieri, F. Chiaraluce, and T. Kløve. "On the generator matrix of array LDPC codes". In: *Proc. 20th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2012)*. Split, Croatia, 2012.

[67] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani. "A variant of the McEliece cryptosystem with increased public key security". In: *Proc. 7th International Workshop on Coding and Cryptography (WCC 2011)*. Paris, France, 2011, pp. 173–182.

[68] M. Baldi, F. Chiaraluce, B. Zanaj, and M. Moretti. "Analysis and simulation of algorithms for vital signs detection using UWB radars". In: *Proc. IEEE International Conference on Ultra-Wideband (ICUWB 2011)*. Bologna, Italy, 2011, pp. 341–345.

[69] M. Baldi, M. Bianchi, and F. Chiaraluce. "Increasing Physical Layer Security through Scrambled Codes and ARQ". In: *Proc. IEEE International Conference on Communications Workshops (ICC 2011)*. Kyoto, Japan, 2011, pp. 1–5.

[70] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani. "On fuzzy syndrome hashing with LDPC coding". In: *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2011)*. Barcelona, Spain, 2011, pp. 1–5.

[71] M. Baldi, F. Chiaraluce, A. de Angelis, R. Marchesani, and S. Schillaci. "Performance of APSK modulation in wireless tactical scenarios for land mobile systems". In: *Proc. IEEE Symposium on Computers and Communications (ISCC 2011)*. Corfu, Greece, 2011, pp. 591–596.

[72] M. Baldi, F. Chiaraluce, M. Moretti, F. Venieri, and B. Zanaj. "Signal modeling and processing for physiological sensing through UWB radars". In: *Proc. International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2011)*. Split-Hvar-Dubrovnik, Croatia, 2011, pp. 66–70.

[73] M. Baldi, M. Bianchi, and F. Chiaraluce. "Non-systematic codes for physical layer security". In: *Proc. IEEE Information Theory Workshop (ITW 2010)*. Dublin, Ireland, 2010, pp. 1–5.

[74] M. Baldi, G. Cancellieri, F. Chiaraluce, and A. De Amicis. "Design of permuted serially concatenated multiple parity-check codes". In: *Proc. International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2010)*. Split-Bol, Croatia, 2010, pp. 285–289.

[75] M. Baldi, G. Cancellieri, F. Chiaraluce, and A. De Amicis. “Irregular M-SC-MPC codes for wireless applications”. In: *Proc. IEEE European Wireless Conference (EW 2010)*. Lucca, Italy, 2010, pp. 369–376.

[76] M. Baldi, F. Chiaraluce, R. Garello, M. Polano, and M. Valentini. “On the Effect of Estimation and Quantization Errors in Downstream VDSL Systems”. In: *Proc. Third International Conference on Communication Theory, Reliability, and Quality of Service (CTRQ 2010)*. Athens, Greece, 2010, pp. 49–54.

[77] M. Baldi, G. Cancellieri, and F. Chiaraluce. “A Class of Low-Density Parity-Check Product Codes”. In: *Proc. First International Conference on Advances in Satellite and Space Communications (SPACOMM 2009)*. Colmar, France, 2009, pp. 107–112.

[78] M. Baldi, G. Cancellieri, and F. Chiaraluce. “New LDPC Codes Based on Serial Concatenation”. In: *Proc. Fifth Advanced International Conference on Telecommunications (AICT 2009)*. Venice, Italy, 2009, pp. 310–315.

[79] M. Baldi, G. Cancellieri, F. Chiaraluce, and A. D. Amicis. “Design of multiple serially concatenated multiple parity-check codes for wireless applications”. In: *Proc. 17th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2009)*. Split-Hvar-Korcula, Croatia, 2009, pp. 126–130.

[80] M. Baldi and F. Chiaraluce. “Performance and complexity of ψ-unitary QC-LDGM codes”. In: *Proc. IEEE Information Theory Workshop (ITW 2009)*. Taormina, Italy, 2009, pp. 198–202.

[81] M. Baldi, F. Chiaraluce, N. Boujnah, and R. Garello. “Impact of truncation on the statistical properties of LFSR sequences”. In: *Proc. 3rd International Conference on Signals, Circuits and Systems (SCS 2009)*. Djerba, Tunisia, 2009, pp. 1–6.

[82] M. Baldi, F. Chiaraluce, G. P. Calzolari, and R. Garello. “Some Remarks on the Problem of Spurious Frequencies in High Data Rate Space Missions”. In: *Proc. First International Conference on Advances in Satellite and Space Communications (SPACOMM 2009)*. Colmar, France, 2009, pp. 24–29.

[83] M. Baldi, F. Chiaraluce, and E. Zanaj. “Fault tolerance in sensor networks: Performance comparison of some gossip algorithms”. In: *Proc. 7th Workshop on Intelligent Solutions in Embedded Systems (WISES 2009)*. Ancona, Italy, 2009, pp. 10–19.

[84] M. Baldi. “LDPC Codes in the McEliece Cryptosystem: attacks and countermeasures”. In: *NATO Advanced Research Workshop*. Veliko Tarnovo, Bulgaria, 2008, p. 17.

[85] M. Baldi, G. Cancellieri, E. Gambi, G. Rascioni, and S. Spinsante. “Interactive Contents Protection in Digital Terrestrial Television”. In: *Proc. 4th International Conference on Automated Solutions for Cross Media Content and Multi-Channel Distribution (AXMEDIS 2008)*. Florence, Italy, 2008, pp. 13–18.

[86] M. Baldi, F. Bambozzi, and F. Chiaraluce. “A class of invertible circulant matrices for QC-LDPC codes”. In: *Proc. International Symposium on Information Theory and Its Applications (ISITA 2008)*. 2008, pp. 1–6.

[87] M. Baldi, G. Cancellieri, F. Chiaraluce, and A. Carassai. “Easily encodable LDPC codes based on polynomial codes”. In: *Proc. 16th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2008)*. Split, Croatia, 2008, pp. 324–328.

[88] M. Baldi, F. Chiaraluce, and E. Zanaj. “Comparison of Averaging Algorithms for Wireless Sensor Networks”. In: *Proc. 3rd International Conference on Information and Communication Technologies: From Theory to Applications (ICTTA 2008)*. Damascus, Syria, 2008, pp. 1–6.

[89] M. Baldi, S. Morichetti, and E. Gambi. “A distributed binary tree protocol for medium access control in RFID systems”. In: *Proc. 16th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2008)*. Split, Croatia, 2008, pp. 228–232.

[90] M. Baldi, S. Morichetti, and E. Gambi. “Analysis of a quality of service framework for home area networks”. In: *Proc. 4th International Telecommunication Networking Workshop (IT-NEWS) on QoS in Multiservice IP Networks (QoS-IP)*. Venice, Italy, 2008, pp. 173–178.

[91] G. Giorgetti, E. Gambi, S. Spinsante, M. Baldi, S. Morichetti, and I. Magnifico. “An integrated solution for home automation”. In: *Proc. IEEE International Symposium on Consumer Electronics (ISCE 2008)*. Las Vegas, USA, 2008, pp. 1–4.

[92] S. Spinsante, M. Baldi, G. Giorgetti, I. Magnifico, E. Gambi, P. P. Ajo, and N. C. Escalona. “An Integrated System for Domotics and Building Automation: the XENO Project”. In: *Proc. FIE ’08*. Santiago de Cuba, Cuba, 2008.

[93] S. Spinsante, M. Baldi, G. Rascioni, C. Alfonsi, G. Cancellieri, and E. Gambi. “DigiMarche.DT: Public Administration Goes TV”. In: *Proc. EuroITV 2008*. Salzburg, Austria, 2008.

[94] E. Zanaj, M. Baldi, and F. Chiaraluce. “Share factors optimization in the Push-Sum algorithm for sensor networks”. In: *Proc. 16th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2008)*. Split, Croatia, 2008, pp. 174–178.

[95] M. Baldi, F. Chiaraluce, R. Garello, and F. Mininni. “Quasi-Cyclic Low-Density Parity-Check Codes in the McEliece Cryptosystem”. In: *Proc. IEEE International Conference on Communications (ICC 2007)*. Glasgow, Scotland, 2007, pp. 951–956.

[96] M. Baldi, F. Chiaraluce, and E. Zanaj. “Fault tolerance in wireless sensor networks based on the gossip algorithm”. In: *Proc. IEEE Conference on Wireless Rural and Emergency Communications (WRECOM 2007)*. Rome, Italy, 2007.

[97] M. Baldi, G. Cancellieri, and F. Chiaraluce. “Iterative soft-decision decoding of binary cyclic codes based on spread parity-check matrices”. In: *Proc. 15th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2007)*. Split-Dubrovnik, Croatia, 2007, pp. 1–5.

[98] M. Baldi and F. Chiaraluce. “Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC Codes”. In: *Proc. IEEE International Symposium on Information Theory (ISIT 2007)*. Nice, France, 2007, pp. 2591–2595.

[99] M. Baldi, S. Morichetti, and E. Gambi. “Quality of Service in local area networks intended for home entertainment and domotic applications”. In: *Proc. 15th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2007)*. Split-Dubrovnik, Croatia, 2007, pp. 1–5.

[100] F. Chiaraluce, M. Baldi, S. Spinsante, and T. Klove. “The Probability of Undetected Error for Varshamov-Tenengol’ts Codes”. In: *Proc. IEEE International Conference on Communications (ICC 2007)*. Glasgow, Scotland, 2007, pp. 1119–1124.

[101] E. Zanaj, M. Baldi, and F. Chiaraluce. “Efficiency of the gossip algorithm for wireless sensor networks”. In: *Proc. 15th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2007)*. Split-Dubrovnik, Croatia, 2007, pp. 1–5.

[102] M. Baldi, A. De Santis, D. Falcone, E. Gambi, and S. Spinsante. “A T-Learning Platform based on Digital Terrestrial Television”. In: *Proc. International Conference on Software in Telecommunications and Computer Networks (SoftCOM 2006)*. Split-Dubrovnik, Croatia, 2006, pp. 347–351.

[103] M. Baldi, G. Cancellieri, and F. Chiaraluce. “Variable Rate LDPC Codes for Wireless Applications”. In: *Proc. International Conference on Software in Telecommunications and Computer Networks (SoftCOM 2006)*. Split-Dubrovnik, Croatia: IEEE, 2006, pp. 301–305.

[104] M. Baldi, F. Chiaraluce, and R. Garello. “On the Usage of Quasi-Cyclic Low-Density Parity-Check Codes in the McEliece Cryptosystem”. In: *Proc. First International Conference on Communications and Electronics (ICCE 2006)*. Vol. PART 1. Hanoi, Vietnam, 2006, pp. 305–310.

[105] G. Bosco, R. Garello, F. Mininni, M. Baldi, and F. Chiaraluce. “Non-Binary Low Density Parity Check Codes for Satellite Communications”. In: *Proc. 11th IEEE Symposium on Computers and Communications (ISCC 2006)*. Cagliari, Italy, 2006, pp. 1019–1024.

[106] G. Bosco, R. Garello, F. Mininni, M. Baldi, and F. Chiaraluce. “Performance of non-binary Low Density Parity Check Codes for space applications”. In: *Proc. SpaceOps 2006 Conference*. Rome, Italy, 2006.

[107] E. Gambi, S. Spinsante, M. Baldi, G. Righi, and G. Ronzino. “A system level integration for remote learning services based on DVB-T platform”. In: *Proc. 24th IASTED International Conference on Internet and Multimedia Systems and Applications*. Vol. 2006. Innsbruck, Austria, 2006, pp. 13–18.

[108] F. Chiaraluce and M. Baldi. “Local cycles optimization: a technique for designing low density parity check codes”. In: *Proc. International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2005)*. Split-Marina Frapa, Croatia, 2005.

[109] F. Chiaraluce and M. Baldi. “New quasi cyclic low density parity check codes based on difference families”. In: *Proc. 8th International Symposium on Communication Theory and Applications (ISCTA 2005)*. Ambleside, UK, 2005, pp. 244–249.

[110] F. Chiaraluce, M. Baldi, A. Carassai, S. Bianchi, and G. Cancellieri. “Rate adaptive low density parity check codes in radio links”. In: *Proc. International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2005)*. Split-Marina Frapa, Croatia, 2005.

[111] F. Chiaraluce, G. Bosco, R. Garello, and M. Baldi. “Decoding complexity and iteration number statistics in low density parity check codes”. In: *Proc. International Symposium on Information and Communication Technology (WISICT 2005)*. Cape Town, South Africa, 2005, pp. 81–86.

[112] E. Gambi, M. Baldi, G. Ronzino, and S. Spinsante. “Integration of videoconference and DVB-T systems for remote learning applications”. In: *Proc. International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2005)*. Split-Marina Frapa, Croatia, 2005.

[113] S. Spinsante, F. Chiaraluce, and M. Baldi. “Performance evaluation of LDPC codes over the Z channel”. In: *Proc. International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2005)*. Split-Marina Frapa, Croatia, 2005.

[114] S. Spinsante, G. Righi, F. Chiaraluce, E. Gambi, and M. Baldi. "Evaluation of authentication and encryption algorithms for telecommand and telemetry in space missions". In: *Proc. 23rd AIAA International Communications Satellite Systems Conference (ICSSC-2005)*. Rome, Italy, 2005.

[115] S. Spinsante, G. Righi, F. Chiaraluce, E. Gambi, and M. Baldi. "On the usage of chaotic signals to increase the efficiency of long range radars for automotive applications". In: *Proc. EMC Europe Workshop on Electromagnetic Compatibility of Wireless Systems*. Rome, Italy, 2005, pp. 131–134.

[116] M. Baldi, F. Chiaraluce, and R. Garello. "On the usage of statistical analysis for the number of decoding iterations in LDPC codes". In: *Proc. ISBC '04*. Harrogate, U.K., 2004, p. 43.

National Publications

[117] M. Baldi and M. Elia. "La crittografia. Da raffinata arte rinascimentale a moderna scienza." In: *GNOSIS*. Vol. 3. 2015, pp. 134–143.

[118] M. Baldi, M. Elia, and M. Sala. "I pratici effetti dell'astrazione matematica nella crittografia". In: *GNOSIS*. Vol. 4. 2015, pp. 112–119.

[119] M. Baldi, M. Elia, and M. Sala. "La sicurezza nell'impero delle comunicazioni". In: *GNOSIS*. Vol. 2. 2015, pp. 118–121.

[120] M. Baldi. "Sistemi Crittografici Post-Quantici per la Sicurezza delle Telecomunicazioni". In: *Atti della Giornata di Studio per Giovani Ricercatori su Innovazione Tecnico Scientifica in Italia nei Settori dell'Energia Elettrica e ICT*. Ed. by R. Fantacci. Florence, Italy: Firenze University Press, 2009, pp. 69–72.

Patents

[1] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani. "Method and apparatus for public-key cryptography based on error correcting codes". Pat. WO/2012/139919 – US/9191199. Oct. 2015.

[2] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani. "Method and system for the digital signature". Pat. WO/2014/188336. May 2014.

January 4th, 2017

Marco Baldi