UNIVERSITÀ
POLITECNICA
DELLE MARCHE

Design and cryptanalysis of post-quantum cryptographic schemes based on codes

Supervisor: Prof. Marco Baldi

Department of Information Engineering
(https://dii.univpm.it/)

Supervisor: Prof. Marco Baldi
CV and publications

Prof. Marco Baldi (Associate Professor in Telecommunications)

Website: https://www.univpm.it/marco.baldi
Publications: https://www.tinyurl.com/marcobaldipublications
ORCID: https://orcid.org/0000-0002-8754-5526

Research interests: Coding, Cryptography, Cybersecurity, Blockchain.

Teaching activity: Teaching professor for courses on coding, cryptography and cybersecurity for Bachelor's, Master's and PhD students at Univpm since 2007, Director of the postgraduate course on “Cybersecurity, Cyber Risk and Data Protection”, jointly organized by Univpm and Unimc since 2021.

COST actions: CA22168 (Physical layer security for trustworthy and resilient 6G systems), IC1306 (Cryptography for Secure Digital Interaction), IC1104 (Random Network Coding and Designs over GF(q)).

Research grants: Principal investigator for the following research projects.

- (2023-) “Quantum-safe cryptographic tools for the protection of national data and information technology assets” (**QSAFEIT**), national competitive project, funded by Italian Ministry of University and Research.
- (2023) “Graph Based Intrusion Detection System” (**GiBIDS**), international competitive project, funded by GEANT Vereniging.
- (2020-2022) “Cyber Risk Assessment Models and Algorithms” (**CybeRAMA**), national competitive competitive project, funded by the Cariverona Foundation.
- (2012-2016) “Enhancing communication security by cross-layer physical and data-link techniques” (**ESCAPADE**) national competitive project, funded by the Ministry of Education, University and Research.

Recent relevant publications:

- Santini, Baldi, Chiaraluce, “Computational Hardness of the Permuted Kernel and Subcode Equivalence Problems”, (2024) IEEE Transactions on Information Theory, 70 (3), pp. 2254-2270.
- Baldi, Chiaraluce, Santini, “SPANSE: Combining sparsity with density for efficient one-time code-based digital signatures”, (2023) Journal of Algebra and its Applications, art. no. 2550099.
- Santini, Persichetti, Baldi, “Reproducible families of codes and cryptographic applications”, (2022) Journal of Mathematical Cryptology, 16 (1), pp. 20-48.
- Aragon, Baldi, Deneuville, Khathuria, Persichetti, Santini, “Cryptanalysis of a code-based full-time signature”, (2021) Designs, Codes, and Cryptography, 89 (9), pp. 2097-2112.
- Hu, Baldi, Santini, Zeng, Ling, Wang, “Lightweight Key Encapsulation Using LDPC Codes on FPGAs” (2020) IEEE Transactions on Computers, 69 (3), art. no. 8877876, pp. 327-341.

Supervisor: Prof. Marco Baldi
Research Group Description

Secure Communications Research Group @Univpm

- **Research areas**: post-quantum cryptography, blockchain, network security.
- Active in research in post-quantum cryptography for more than **fifteen years**.
- Authors of **scientific publications** that have appeared in leading publishing venues in the field.
- Organizers of relevant scientific events in the area, such as **CBCrypto** (https://www.cb-crypto.org/).
- Active collaborations with **companies** and **research institutions**:
    - European Space Agency (ESA)
    - German Aerospace Center (DLR)
    - Thales Alenia Space Italy (TASI)
- Active collaborations with leading **universities**:
    - University of Zurich (UZH)
    - Technical University of Munich (TUM)
    - Florida Atlantic University (FAU)
    - Politecnico di Milano (Polimi)
    - University of Trento (Unitn)
- Participating in the current **NIST** process for standardization of post-quantum cryptographic primitives with three candidates: **LEDAcrypt**, **CROSS** and **LESS**

https://www.ledacrypt.org/

https://www.cross-crypto.com/

https://www.less-project.com/

UNIVERSITÀ
POLITECNICA
DELLE MARCHE

The Department of Information Engineering

Director: Prof. Franco Chiaraluce

The Department of Information Engineering (DII) was established in 2011 following the merge of the previous DIBET (Department of Biomedical, Electronics and Telecommunication engineering) and DIIGA (Department of Computer, Management and Automation engineering).

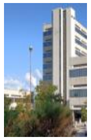
The Department is a self-managing organizational branch of the university which is dedicated to scientific research, teaching, and contributing to the so called Third Mission of the Higher Education Institution through the dissemination of scientific research findings amongst the community.

Its main aims are to plan, organize and regularly assess the quality of the research activities carried out in the scientific sectors and disciplines under its jurisdiction; to plan, organize and manage bachelor and master courses in Information Engineering and, last but not least, to provide cultural and educational activities and contribute to training and guidance issues according to the students needs.

https://www.dii.univpm.it

AT A GLANCE

DII



2023

250+ Publications

11 Scientific Area
ING-INF/01 ING-INF/02
ING-INF/03 ING-INF/04
ING-INF/05 ING-INF/06
ING-INF/07 ING-IND/31
ING-IND/35 MAT/09
SECS-P/06

65 Staff

> 4 M€
Research income

100 PhD, Post-doc, Research fellows

Bachelor Degree in: Biomedical Engineering, Electronic Engineering and Digital Technologies, Computer and Automation Engineering, Information Engineering for Videogame and Virtual Reality.
Master Degree in: Biomedical Engineering (in english), Electronic Engineering, Computer and Automation Engineering.

Bachelor Degree with professional orientation in Industrial and Information Systems (based in Pesaro).

DII coordinates the PhD in Information Engineering, organized in two curricula:
- Biomedical, Electronics, Telecommunication Engineering and Nanotechnologies (IBETN)
- Computer, Management and Automation Engineering (IIGA)

Research laboratorie s 32

UNIVERSITÀ
POLITECNICA
DELLE MARCHE

Project Idea

Design and cryptanalysis of post-quantum cryptographic schemes based on codes

Challenges tackled:

- Devising new, efficient post-quantum cryptographic primitives based on codes.
- Assessing their security.

Background:

- Codes and lattices are the primary mathematical objects employed in post-quantum cryptosystems.
- Lattices are already efficiently used for both encryption and signatures.
- Codes are mostly efficient for encryption.
- Existing digital signatures based on codes are either inefficient or susceptible to security vulnerabilities.

Expected outcomes:

- Establishment of new, improved alternatives based on codes to offer robust replacements for lattice-based schemes.
- Enhancement of the diversity and robustness of post-quantum digital signature schemes.
- Revision of current post-quantum encryption schemes based on codes for improving their efficiency.
- Achievement of more robust security guarantees against chosen ciphertext attacks.