Supervisor Project Idea

Supervisor

Insert a brief CV and/or external link, the total number of publications, the ORCID link, 5 of the most significant/recent publications, and a list of funded projects and awards. max 300 words

Marco Baldi is an Associate Professor in Telecommunications at Univpm. He is a member of the management committee of the CINI Cybersecurity National Laboratory and founding member and scientific committee member of the National Cryptologic Association De Componendis Cifris. His research activity concerns communications reliability and security, with focus on coding and post-quantum cryptography. He is co-author of over 200 scientific papers, one book and four patents.

He is Principal Investigator of 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.

Five relevant publications:

1. 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, DOI: 10.1142/S0219498825500999.
2. Santini, Baldi, Chiaraluce, "Computational Hardness of the Permuted Kernel and Subcode Equivalence Problems", (2024) IEEE Transactions on Information Theory, 70 (3), pp. 2254-2270, DOI: 10.1109/TIT.2023.3323068.
3. Santini, Persichetti, Baldi, "Reproducible families of codes and cryptographic applications", (2022) Journal of Mathematical Cryptology, 16 (1), pp. 20-48, DOI: 10.1515/jmc-2020-0003.
4. Aragon, Baldi, Deneuville, Khathuria, Persichetti, Santini, "Cryptanalysis of a code-based full-time signature", (2021) Designs, Codes, and Cryptography, 89 (9), pp. 2097-2112, DOI: 10.1007/s10623-021-00902-7.
5. 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, DOI: 10.1109/TC.2019.2948323.

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

Research Group Description

Provide the name the reference department and a brief description of the research group, including external links, and available instrumentations and infrastructures. max 300 words

Università Politecnica delle Marche (https://www.univpm.it/) is one of the most important technical universities in Italy, with 12 Departments, related mostly to STEM disciplines, hosting about 16.000 students and about 500 research permanent staff. Over 50 spin-off companies have been created since 2001, and over 75 patents have been filed since 2003, 32 at international level.

The research group involved in this proposal is the **secure communications** research unit hosted by the Department of Information Engineering (https://dii.univpm.it/), which is active in the research areas of post-quantum cryptography, blockchain and network security.

In particular, the proposing research group has already been active in the area of post-quantum cryptography for more than fifteen years, both in terms of scientific and applied research projects, and in collaboration with both national and international organizations and companies. The group is also participating in the current NIST process for standardization of post-quantum cryptographic primitives with the candidates LEDAcrypt, CROSS and LESS. This provides a solid foundation for the inclusion of the potential candidate within the relevant scientific and technological networks. Existing collaborations in which she or he will be involved include those currently in place with the European Space Agency (ESA), the German Aerospace Center (DLR) and Thales Alenia Space Italy, on the corporate side, and with the University of Zurich (UZH), Florida Atlantic University (FAU) and the Technical University of Munich (TUM) on the academic side.

Title and goals

Provide the title of the topic and a short summary of the project idea. max 200 words

Title: “Design and cryptanalysis of post-quantum cryptographic schemes based on codes”.

The research project will address the challenge of devising new, efficient post-quantum cryptographic primitives based on codes and assessing their security.

In fact, codes and lattices are the primary mathematical objects employed in the development of post-quantum cryptosystems. Although lattices are already efficiently used for both encryption and signatures, codes are mostly efficient for encryption. The main reason for this limitation is that existing digital signature schemes relying on codes are either inefficient or susceptible to security vulnerabilities.

However, from the literature we notice that attacks on lattice-based cryptosystems are not yet fully consolidated, leaving room for a relatively high likelihood of new advancements in their cryptanalysis. Based on these premises, the project aims to establish new, improved alternatives based on codes to offer robust replacements for lattice-based schemes. This target is pivotal for enhancing the diversity and robustness of post-quantum digital signature schemes.

In addition to this, current post-quantum encryption schemes based on codes will be revised, with focus on those using iteratively decoded codes (like QC-LDPC and QC-MDPC codes), with the aim of improving their efficiency and providing more robust security guarantees against chosen ciphertext attacks by accurately predicting their decryption failure rate.

Contact details (*including email address of the supervisor*)

Marco Baldi, Ph.D.

Università Politecnica delle Marche
Dipartimento di Ingegneria dell'Informazione
Via Brecce Bianche 12
I-60131 Ancona, Italy

Tel: (+39) 071 220 4894
Email: m.baldi@univpm.it
www.univpm.it/marco.baldi