# Paolo Santini

curriculum vitae

**Citizenship:** Italian

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

Phone: (+39) 392 5870169
Email: p.santini@staff.univpm.it

## Short Biography

Paolo Santini received a Laurea degree in Electronic Engineering (summa cum laude) in 2014, a Laurea Magistrale degree in Electronic Engineering (summa cum laude) in 2016 and a PhD in Information Engineering in 2020, with a thesis entitled "On the use of structured codes for cryptographic applications", by Marche Polytechnic University. Since 2019 he is a postdoctoral researcher in Information Engineering at the Department of Information Engineering of Marche Polytechnic University.
His research activity is focused on coding theory and cryptography, with particular attention to LDPC and MDPC codes and post-quantum cryptography.
In 2018 he has been a visiting student for two months at the Department of Mathematical Sciences, Florida Atlantic University; in 2020/2021, he has been a research fellow for four months in the same department. He has participated, as a co-author of two proposals, to the 2017 NIST process for standardization of post-quantum public key cryptosystems. He serves as Guest Editor for Cryptography and as a reviewer for many international journals and conferences. He has been co-organizer of the seventh Code-Based Cryptography workshop in 2019, and the first and fourth editions of CBCrypto in 2020 and 2023, respectively.

## Training

**PhD**
(March 20, 2020)

PhD in Information Engineering (curriculum: Biomedical, Electronics and Telecommunications Engineering) from Università Politecnica delle Marche, with a thesis entitled "*On the use of structured codes for cryptographic applications*" ("*Sull'utilizzo di codici strutturati per applicazioni crittografiche*"), advisor Prof. Marco Baldi.

**Visiting PhD student**
(March-April 2018)

Visiting PhD student at Florida Atlantic University, Boca Raton, Florida, USA, under the supervision of Prof. Edoardo Persichetti.

**Master's Degree**
(October 19, 2016)

Two-year Laurea Magistrale Degree (equivalent to Master's Degree) in Electronic Engineering obtained with grade 110/110 and honors from Università Politecnica delle Marche with a thesis entitled "*Progetto di sistemi crittografici basati su codici QC-LDPC con chiavi compatte*", advisor Prof. Marco Baldi.

**Bachelor's Degree**
(October 18, 2014)

Three-year Laurea Degree (equivalent to Bachelor's Degree) in Electronic Engineering obtained with grade 110/110 and honors from Università Politecnica delle Marche with a thesis entitled "*Attacchi al sistema di McEliece basato su alfabeti continui*", advisor Prof. Marco Baldi.

---

## Current Position

**Università Politecnica delle Marche**
(01/11/2019 - present)

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 "Metodi e strumenti innovativi per il REACTive Product Design and Manufacturing".

---

## Language knowledge

| | |
|---|---|
| **English** | Good command of spoken and written language. Frequent contacts and speeches delivered in English. |
| **French** | Scholastic knowledge of spoken and written language. |
| **Italian** | Mother language. |

## Editorial activity

**Participation in the Organizing Committee of International Conferences**

- 7th Code-Based Cryptography Workshop, Edition: 2019;
- CBCrypto - International Workshop on Code-Based Cryptography, Editions: 2020 and 2023;

**Participation in the Technical Program Committee of International Conferences**

- Algebra, Codes and Cryptology (A2C), 2019
- CBCrypto, Editions: 2021, 2022, 2023, 2024
- AAC24 - Workshop on Advances in Asymmetric Cryptanalysis

**Editorial activity**

**Editor**

- Cryptography (MDPI) special issue, entitled "Public-Key Cryptography in the Post-quantum Era"
- Springer volume, book series: Lecture Notes in Computer Science (LNCS, volume 11666): "Code-Based Cryptography 7th International Workshop", CBC 2019, Darmstadt, Germany, May 18–19, 2019, Revised Selected Papers
- Springer volume, book series: Lecture Notes in Computer Science (LNCS, volume 12087): "CBCrypto 2020", Zagreb, Croatia, May 9–10, 2020, Revised Selected Papers
- Springer volume, book series: Lecture Notes in Computer Science (LNCS, volume 12087): "CBCrypto 2023", Lyon, France, April 22–23, 2023, Revised Selected Papers

**Reviewer** for international journals, including:

- IEEE Communication Letters
- IEEE Transactions on Circuits and Systems
- IEEE Transactions on Information Theory
- IEEE Transactions on Information Forensics and Security
- IEEE Transactions on Very Large Scale Integration Systems
- IEEE Open Journal of the Communications Society
- Designs, Codes and Cryptography
- Cryptography MDPI
- Entropy MDPI
- Security and Communication Networks
- Optical and Quantum Electronics
- International Journal of Communication Systems

**Reviewer** of many contributions submitted for presentation at international conferences.

## Participation in research projects

**Post Quantum Cryptography Algorithms for Satellite Telecommunication Applications**
*Funded by the European Space Agency (ESA)*

**Role: Key Person**
The main objective of this project is to evaluate the performance of post-quantum cryptography algorithms for satellite telecommunication applications. The project aims to take into account realistic scenarios, derive the associated requirements on post-quantum cryptographic algorithms and networking protocols and, finally, evaluate their performances.

**Over the air CRYPTOgraphic keys exchange for secure governmental SATellite communications (CRYPTOSAT)**
*Funded by the European Space Agency (ESA)*

**Role: Key Person**
The project fits in the scenario of Governmental Satellite Communications (GOVSATCOM), which are crucial both for civil and military purposes and, consequently, deserve a high standard of security and reliability. CRYPTOSAT aims at endowing GOVSATCOM with a secure and efficient keys exchange infrastructure, studying the performances of internet protocols (such as IKEv2) when employed in satellite channels.

**Human Digital Flexible – Factory of the Future Laboratory (HD3FLAB) - Progetto: MERCURY- sMart sEcuRe deCentralized indUstRY**
*Funded by Marche Region*

**Role: Collaborator**
The project proposes the design and construction of an industrial automation platform that integrates edge computing with cybersecurity and blockchain techniques. The blockchain is employed to let nodes communicate, with the aim of increasing data exchange and network efficiency, while still guaranteeing its security. To realize these functions, it is necessary to carefully study the cryptographic primitives with which the nodes must be equipped, in order to guarantee security and efficiency (taking into account the reduced computational capabilities of some of the nodes participating in the network).

**Metodi e strumenti innovativi per il REACTive Product Design and Manufacturing–REACT**
*Funded by PON-PNR 2015-2020*

**Role: Collaborator**
The project aims to develop innovative methods to react to the analysis of the information content that is detectable on Smart Factory production lines, where an enormous amount of data is typically exchanged.

---

## Other research activities and awards

**CROSS: candidate for NIST Post-Quantum Standardization process**
June 2023 - Ongoing

**Role: Co-author**
CROSS is a digital signature scheme based on the restricted syndrome decoding, which is in the firt round of the NIST additional call for digital signatures (official website `https://www.cross-crypto.com/`)

**LESS: candidate for NIST Post-Quantum Standardization process**
June 2023 - Ongoing

**Role: Co-author**
LESS is a digital signature scheme based on the code equivalence problem, which is in the firt round of the NIST additional call for digital signatures (official website `https://www.less-project.com/`)

**LEDAcrypt: candidate for NIST Post-Quantum Standardization process**
December 2016 - March 2020

**Role: Co-author**
LEDAcrypt is a suite of post-quantum encryption and key encapsulation algorithms, based on QC-LDPC codes, which has been admitted to the first and second rounds of the NIST competition (official website `https://www.ledacrypt.org/`)

**Collaborations and scientific visits**

- **Research Associate** at Math Department at Florida Atlantic University, Boca Raton, Florida, USA, November 2019 - February 2020

- **Scientific visits**:
  - Coding and Cryptography Group, Technical University of Munich, Munich, Germany, October 2022
  - Math Department at Florida Atlantic University, Boca Raton, Florida, USA, September 2019
  - Applied Algebra Group at University of Zurich, Zurich, Switzerland, November 2018

**Awards**

- **Best paper award** for work [1], accepted in International Joint Conference on e-Business and Telecommunications (ICETE) 2020
- **Best paper award** for work [2], accepted in 2022 IEEE International Conference on Omni-layer Intelligent Systems (COINS)

## Professional Memberships and Services

| | |
|---|---|
| **Institute of Electrical and Electronics Engineers (IEEE)** | Member since 2017. |
| **National Inter-University Consortium for Telecommunications (CNIT)** | Member since 2017. |
| **Italian Group of Telecommunications and Information Technology (GTTI)** | Member since 2017. |

## University Teaching

**Cryptography and Blockchain**
Master of Science in Electronic Engineering of Marche Polytechnic University.
Academic years: 2021-2022, 2022-2023
Hours: 72, language: Italian
Role: Professor

Topics:
Private key cryptography, public key encryption, hash function, digital signatures, post-quantum cryptography, modern cryptographic applications and functionalities, blockchain networks.

**Coding and Cryptography**
Master of Science in Computer and Automation Engineering, Ecampus.
Academic year: 2020-2021, 2021-2022, 2022-2023
Hours: 72, language: Italian
Role: Professor

Topics:
Source coding, error correction codes, private and public key cryptography, hash functions, digital signatures, post-quantum cryptography.

**Mobile Operating Systems**
Master of Science in Computer and Automation Engineering, Ecampus.
Academic year: 2020-2021, 2021-2022
Hours: 48, language: Italian
Role: Professor

Topics:
Principles of programming for embedded devices, programming for mobile devices (Android).

**Other**
Lectures and tutorials on specific topics for courses of Master of Science of Università Politecnica delle Marche.

Courses:
- Telecommunications
- Signal theory
- Digital communications
- Information theory and codes
- Security in telecommunications networks
- Octave course for PhD students of Marche Polytechnic University

## 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.

| Academic Year | Student | Title | Type | Role |
|---|---|---|---|---|
| 2022-2023 | Chen Lei | Study of new attacks on the Code Equivalence Problem | MSc | Supervisor |
| 2021-2022 | Tommaso Casoni | Optimisation of Patterson decoding algorithm through Intel's AVX2 instrinsic instructions with application on Classic McEliece quantum-resistant cryptosystem | MSc | Co-Supervisor |
| 2021-2022 | Valeria Vetrano | Design and implementation of blockchain protocols for biometric identification | MSc | Co-Supervisor |
| 2021-2022 | Vito Scaraggi | Design and implementation of blockchain protocols for biometric identification | BSc | Supervisor |
| 2020-2021 | Domenico Andrea Giliberti | Blockchain Transaction Implementation on ARM Cortex-M4 Platform | MSc | Co-Supervisor |
| 2020-2021 | Davide Bevilacqua | Performance Assessment of a Private Blockchain Network Infrastructure for Industry 4.0 | MSc | Co-Supervisor |
| 2020-2021 | Daniela Voltattorni | Implementation of Ethereum blockchain transactions on ARM Cortex-M4 embedded processors | MSc | Co-Supervisor |
| 2020-2021 | Rebecca Giuliani | Design and optimization of a code-based post-quantum digital signature scheme | BSc | Co-Supervisor |
| 2020-2021 | Chen Lei | Implementation of a code-based post-quantum digital signature scheme | BSc | Co-Supervisor |
| 2019-2020 | Renat Kermenov | LDPC code optimization with Lee metric-based decoding | MSc | Co-Supervisor |
| 2019-2020 | Francesco Ciotti | Microcontroller implementation of codebased post-quantum cryptographic primitives | MSc | Co-Supervisor |
| 2019-2020 | Gianmarco Mascilongo | Attacks based on weak keys against post-quantum cryptographic systems based on sparse codes | MSc | Co-Supervisor |

## Presentations and seminaries

**Presentations given at international conferences (with proceedings)**

With reference to the list of publications reported below, Paolo Santini has presented the following works at international conferences: [3, 4, 5, 6]

**Presentations given at international workshops (without proceedings)**

- Speaker at Post-Quantum Cryptography Workshop, Oxford, September 5, 2023,
  "*CROSS: Codes & Restricted Objects Signature Scheme*"

- Speaker at SIAM AG 2023, Eindhoven, July 12,
  "*Zero Knowledge Protocols and Signatures from the Restricted Syndrome Decoding Problem* "

- Speaker at PQCifris 2022 - Workshop on Post-Quantum Cryptography, Trento, October 14, 2022,
  "*Recent Advances in the Code Equivalence Problem and Applications to Cryptography*"

- Speaker at 4th Distributed Ledger Technology" Workshop, Rome, Italy, June 20 2022,
  "*Implementation of Ethereum Accounts and Transactions on Embedded IoT Devices*"

- Speaker at FOCODILE 2022 - 3rd International Workshop on Foundations of Consensus and Distributed Ledgers, IMT School for Advanced Studies Lucca , Lucca, Italy, June 13 2022, title:
  "*Clearing Fuzzy Signatures: a Proof of Work Blockchain Protocol for Biometric Identification*"

- Speaker at Code-Based Cryptography workshop, Trondheim, Norway, May 30 2022,
  "*A Coding Theory Approach to the Solution of the Permuted Kernel Problem*"

- Speaker at SIAM Conference on Applied Algebraic Geometry, online event, August 17, 2021,
  "*The Restricted Syndrome Decoding Problem, and its Application to Digital Signatures*"

- Invited speaker at HiPEAC 2020, Bologna, January 20, 2020,
  "*Tackling the problem of large public keys in post-quantum encryption schemes based on codes*"

- Speaker at SIAM Conference on Applied Algebraic Geometry, University of Bern, Bern, Switzerland, July 13, 2019,
  "*Public key encryption and key exchange from LDPC codes: LEDAcrypt*"

- Speaker at ESIT 2018, Bertinoro, Italy, May 11, 2018,
  "*Hindering reaction attacks by using monomial codes in the McEliece cryptosystem*"

- Speaker at workshop "Celebrating the influence of Ruud Pellikaan", at Technische Universiteit Eindhoven, Eindhoven, Netherlands, March 8, 2019,
  "*Structured codes with cryptographic applications*"

- Speaker at workshop CBC 2018, at Florida Atlantic University, Fort Lauderdale, Florida, USA, April 5-6, 2018, with two talks:
  "*LEDAkem and LEDApkc: key encapsulation and public-key cryptography based on QC-LDPC codes*,"
  "*A QC-LDPC code-based public-key cryptosystem resistant to reaction attacks*"

**Invited Seminaries**

- TUM ICE Doctoral Seminar, Technical University of Munich, Munich, July 25, 2023:
  "*Proving without revealing: code-based signatures from Zero Knowledge protocols*"

- Seminary at Technical University of Munich, Munich, October 11, 2022,
  "*Recent Advances in Code Equivalence: Attacks, Applications and Open Questions*"

- Online RTG research seminar at Clemson University, November 29, 2021,
  "*The code equivalence problem and its applications to cryptography*"

- Online seminary for Post-Quantum Cifris, November 2, 2021,
  "*Recent advances in code-based encryption and digital signatures*"

- Seminary at University of Zurich, Switzerland, November 7, 2018,
  "*Structured Codes with Cryptographic Applications*"

- Seminary at Florida Atlantic University, Boca Raton, Florida, USA, March 30, 2018,
  *LEDAkem and LEDApkc: post-quantum cryptosystems based on QC-LDPC codes*

**Keynote Speechs**

- Keynote speaker at the Second International Workshop on Post-quantum Cryptography (IWPQC 2021), held during 10-11 December 2021 in conjunction with Indocrypt 2021

## Attended Workshops and Conferences

- *First PQC Standardization Conference*, 2018 (Fort Lauderdale, Florida, USA).
- *Second PQC Standardization Conference*, 2019 (Santa Barbara, California, USA).
- *Celebrating the influence of Ruud Pellikaan*, 2019 (Technische Universiteit Eindhoven, Eindhoven, Netherlands).
- *CBCrypto - International Workshop on Code-Based Cryptography Workshop (CBC)*, 2018 (Florida Atlantic University, Davie, Florida), 2019 (Darmstadt, Germany), 2020 (Online event), 2021 (Online event) and 2022 (Hybrid event, Trondheim, Norway).
- *International Workshop on Code-Based Cryptography (CBCrypto)*, 2020 (Zagreb, Croatia) and 2021 (Munich, Germany).
- *2018 IEEE International Symposium on Information Theory (ISIT)*, 2018 (Vail, Colorado)
- *Quantum Cryptanalysis of Post-Quantum Cryptography*, 2020 (Simons Institute for the Theory of Computing, University of California, Berkeley, California, USA).
- Dagstuhl Seminar 21421 "Quantum Cryptanalysis", 2021 (Schloss Dagstuhl - Leibniz Center for Informatics, Germany).
- *2022 IEEE International Symposium on Information Theory (ISIT)*, 2022 (Aalto University, Espoo, Finland).
- *FOCODILE 2022 - 3rd International Workshop on Foundations of Consensus and Distributed Ledgers*, 2022 ( IMT School for Advanced Studies, Lucca, Italy).
- *4th Distributed Ledger Technology Workshop*, 2022 (Rome, Italy).
- *PQCifris 2022: School & Workshop on Post-Quantum Cryptography*, 2022 (Fondazione Bruno Kessler, Trento, Italy)
- *CBCrypto 2023- International Workshop on Code-Based Cryptography*, 2023 (ENS Lyon, Lyon, France)
- *Workshop in Coding Theory & Cryptography*, 2023 (VT Steger Center for International Scholarship, Riva San Vitale, Switzerland).

- *SIAM Conference on Applied Algebraic Geometry (AG23)*, 2023 (Eindhoven University of Technology, Eindhoven, The Netherlands).

---

## Bibliometric Indices

Google scholar: h-index 17 (total citations 738)
Scopus: h-index 11 (total citations 302)

---

## Publications


[1] M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, and P. Santini, "Analysis of in-place randomized bit-flipping decoders for the design of ldpc and mdpc code-based cryptosystems," *Communications in Computer and Information Science*, vol. 1484 CCIS, pp. 151–174, 2021.

[2] G. Rafaiani, P. Santini, M. Baldi, and F. Chiaraluce, "Implementation of ethereum accounts and transactions on embedded iot devices," 2022.

[3] P. Santini, M. Baldi, G. Cancellieri, and F. Chiaraluce, "Hindering reaction attacks by using monomial codes in the mceliece cryptosystem," vol. 2018-June, pp. 951–955, 2018.

[4] P. Santini, M. Baldi, and F. Chiaraluce, "Assessing and countering reaction attacks against post-quantum public-key cryptosystems based on qc-ldpc codes," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11124 LNCS, pp. 323–343, 2018.

[5] P. Santini, M. Battaglioni, F. Chiaraluce, and M. Baldi, "Analysis of reaction and timing attacks against cryptosystems based on sparse parity-check codes," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11666 LNCS, pp. 115–136, 2019.

[6] P. Santini, M. Baldi, and F. Chiaraluce, "A novel attack to the permuted kernel problem," vol. 2022-June, pp. 1441–1446, 2022.

[7] A. Barenghi, J.-F. Biasse, E. Persichetti, and P. Santini, "On the computational hardness of the code equivalence problem in cryptography," *Advances in Mathematics of Communications*, vol. 17, no. 1, pp. 23–55, 2023.

[8] P. Santini, M. Baldi, and F. Chiaraluce, "Computational hardness of the permuted kernel and subcode equivalence problems," *IEEE Transactions on Information Theory*, pp. 1–1, 2023.

[9] S. Bitzer, A. Pavoni, V. Weger, P. Santini, M. Baldi, and A. Wachter-Zeh, "Generic decoding of restricted errors," vol. 2023-June, pp. 246–251, 2023.

[10] E. Persichetti, T. Randrianarisoa, and P. Santini, "An attack on a non-interactive key exchange from code equivalence," *Tatra Mountains Mathematical Publications*, vol. 82, no. 2, pp. 53–64, 2022.

[11] S. Gueron, E. Persichetti, and P. Santini, "Designing a practical code-based signature scheme from zero-knowledge proofs with trusted setup," *Cryptography*, vol. 6, no. 1, 2022.

[12] M. Battaglioni, P. Santini, G. Rafaiani, F. Chiaraluce, and M. Baldi, "Analysis of a blockchain protocol based on ldpc codes," vol. 3166, pp. 7–17, 2022.

[13] P. Santini, G. Rafaiani, M. Battaglioni, F. Chiaraluce, and M. Baldi, "Optimization of a reed-solomon code-based protocol against blockchain data availability attacks," pp. 31–36, 2022.

[14] A. Barenghi, J.-F. Biasse, T. Ngo, E. Persichetti, and P. Santini, "Advanced signature functionalities from the code equivalence problem," *International Journal of Computer Mathematics: Computer Systems Theory*, vol. 7, no. 2, pp. 112–128, 2022.

[15] M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, and P. Santini, "Performance bounds for qc-mdpc codes decoders," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13150 LNCS, pp. 95–122, 2022.

[16] P. Santini, E. Persichetti, and M. Baldi, "Reproducible families of codes and cryptographic applications," *Journal of Mathematical Cryptology*, vol. 16, no. 1, pp. 20–48, 2022.

[17] M. Baldi, J.-C. Deneuville, E. Persichetti, and P. Santini, "Cryptanalysis of a code-based signature scheme based on the schnorr-lyubashevsky framework," *IEEE Communications Letters*, vol. 25, no. 9, pp. 2829–2833, 2021.

[18] N. Aragon, M. Baldi, J.-C. Deneuville, K. Khathuria, E. Persichetti, and P. Santini, "Cryptanalysis of a code-based full-time signature," *Designs, Codes, and Cryptography*, vol. 89, no. 9, pp. 2097–2112, 2021.

[19] M. Battaglioni, G. Cancellieri, and P. Santini, "On the use of code-based cryptography in automotive applications," 2021.

[20] A. Barenghi, J.-F. Biasse, E. Persichetti, and P. Santini, "Less-fm: Fine-tuning signatures from the code equivalence problem," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12841 LNCS, pp. 23–43, 2021.

[21] K. Koleci, P. Santini, M. Baldi, F. Chiaraluce, M. Martina, and G. Masera, "Efficient hardware implementation of the ledacrypt decoder," *IEEE Access*, vol. 9, pp. 66223–66240, 2021.

[22] P. Santini, M. Battaglioni, M. Baldi, and F. Chiaraluce, "Analysis of the error correction capability of ldpc and mdpc codes under parallel bit-flipping decoding and application to cryptography," *IEEE Transactions on Communications*, vol. 68, no. 8, pp. 4648–4660, 2020.

[23] P. Santini, M. Battaglioni, F. Chiaraluce, M. Baldi, and E. Persichetti, "Low-lee-density parity-check codes," vol. 2020-June, 2020.

[24] P. Santini, M. Baldi, and F. Chiaraluce, "Complexity of statistical attacks on qc-ldpc code-based cryptosystems," *IET Information Security*, vol. 14, no. 3, pp. 304–312, 2020.

[25] J. Hu, M. Baldi, P. Santini, N. Zeng, S. Ling, and H. Wang, "Lightweight key encapsulation using ldpc codes on fpgas," *IEEE Transactions on Computers*, vol. 69, no. 3, pp. 327–341, 2020.

[26] M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, and P. Santini, "A failure rate model of bit-flipping decoders for qc-ldpc and qc-mdpc code-based cryptosystems," vol. 3, pp. 238–249, 2020.

[27] D. Apon, R. Perlner, A. Robinson, and P. Santini, "Cryptanalysis of ledacrypt," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12172 LNCS, pp. 389–418, 2020.

[28] M. Baldi, E. Persichetti, and P. Santini, "Preface," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12087 LNCS, pp. v–vi, 2020.

[29] J.-F. Biasse, G. Micheli, E. Persichetti, and P. Santini, "Less is more: code-based signatures without syndromes," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12174 LNCS, pp. 45–65, 2020.

[30] G. Banegas, P. Barreto, E. Persichetti, and P. Santini, "Designing efficient dyadic operations for cryptographic applications," *Journal of Mathematical Cryptology*, vol. 14, no. 1, pp. 95–109, 2020.

[31] M. Battaglioni, P. Santini, M. Baldi, and G. Cancellieri, "Obtaining structured generator matrices for qc-ldpc codes," 2019.

[32] M. Baldi, G. Cancellieri, F. Chiaraluce, E. Persichetti, and P. Santini, "Using non-binary ldpc and mdpc codes in the mceliece cryptosystem," 2019.

[33] P. Santini, M. Baldi, and F. Chiaraluce, "Cryptanalysis of a one-time code-based digital signature scheme," vol. 2019-July, pp. 2594–2598, 2019.

[34] M. Baldi, F. Chiaraluce, J. Rosenthal, P. Santini, and D. Schipani, "Security of generalised reed–solomon code-based cryptosystems," *IET Information Security*, vol. 13, no. 4, pp. 404–410, 2019.

[35] P. Santini, M. Battaglioni, M. Baldi, and F. Chiaraluce, "Hard-decision iterative decoding of ldpc codes with bounded error rate," vol. 2019-May, 2019.

[36] M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, and P. Santini, "A finite regime analysis of information set decoding algorithms," *Algorithms*, vol. 12, no. 10, 2019.

[37] M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, and P. Santini, "Ledacrypt: Qc-ldpc code-based cryptosystems with bounded decryption failure rate," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11666 LNCS, pp. 11–43, 2019.

[38] S. Samardjiska, P. Santini, E. Persichetti, and G. Banegas, "A reaction attack against cryptosystems based on lrpc codes," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11774 LNCS, pp. 197–216, 2019.

[39] P. Santini, G. Gottardi, M. Baldi, and F. Chiaraluce, "A data-driven approach to cyber risk assessment," *Security and Communication Networks*, vol. 2019, 2019.

[40] M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, and P. Santini, "Ledakem: A post-quantum key encapsulation mechanism based on qc-ldpc codes," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10786 LNCS, pp. 3–24, 2018.

[41] M. Baldi, P. Santini, and G. Cancellieri, "Post-quantum cryptography based on codes: State of the art and open challenges," vol. 2017-January, pp. 1–6, 2017.

[42] M. Baldi, P. Santini, and F. Chiaraluce, "Soft mceliece: Mdpc code-based mceliece cryptosystems with very compact keys through real-valued intentional errors," vol. 2016-August, pp. 795–799, 2016.

Paolo Santini