



## Curriculum Vitae Europass

### Informazioni personali

Nome / Cognome

Email

Nazionalità

**Santini Paolo**

p.santini@staff.univpm.it

Italiana

### Esperienza professionale

Data

Funzione o posto occupato

Principali mansioni e  
responsabilità

Nome e indirizzo del datore di  
lavoro

1 Novembre 2019 - presente

#### **Assegnista di ricerca**

Attuazione del progetto di ricerca "Primitive e protocolli crittografici per industrial Internet of things", nell'ambito del Settore s.d. ING-INF/03 (Telecomunicazioni).

Università Politecnica delle Marche

## Istruzione e formazione

Data  
Certificato o diploma ottenuto

Nome e tipo d'istituto di  
istruzione o formazione

Livello nella classificazione  
nazionale o internazionale

Novembre 2016 - Ottobre 2019

**Dottorato di Ricerca in Ingegneria dell'Informazione (curriculum Biomedica, Elettronica e Telecomunicazioni)**, conseguito a Marzo 2020, Titolo della tesi: "*On the Use of Structured Codes for Cryptographic Applications*"

Università Politecnica delle Marche

Ph.D.

Data  
Certificato o diploma ottenuto

Nome e tipo d'istituto di  
istruzione o formazione

Livello nella classificazione  
nazionale o internazionale

Ottobre 2014 - Ottobre 2016

**Laurea Magistrale in Ingegneria Elettronica (indirizzo Elettronica) conseguita con la votazione di 110/110 e lode**, Titolo della tesi: "*Progetto Di Sistemi Crittografici Basati su Codici QC-LDPC con Chiavi Compatte*"

Università Politecnica delle Marche

Laurea Magistrale

Data  
Certificato o diploma ottenuto

Nome e tipo d'istituto di  
istruzione o formazione

Livello nella classificazione  
nazionale o internazionale

Ottobre 2011 - Ottobre 2014

**Laurea Triennale in Ingegneria Elettronica (indirizzo Elettronica) conseguita con la votazione di 110/110 e lode**, Titolo della tesi: "*Attacchi Al Sistema di McEliece Basato su Alfabeti Continui*"

Università Politecnica delle Marche

Laurea Triennale

Data  
Certificato o diploma ottenuto

Nome e tipo d'istituto di  
istruzione o formazione

Livello nella classificazione  
nazionale o internazionale

Settembre 2006 - Luglio 2011

**Diploma di Maturità Scientifica conseguito con la votazione di 98/100**

Liceo scientifico G. Galilei - Ancona

Diploma di scuola superiore

## Capacità e competenze professionali

Madrelingua

Altra/e lingua/e

Autovalutazione  
Livello europeo<sup>(\*)</sup>

**Inglese**

**Italiano**

Comprensione				Parlato				Scritto	
Ascolto		Lettura		Interazione		Produzione orale			
C1	Livello avanzato	C2	Livello avanzato	C1	Livello avanzato	C1	Livello avanzato	C2	Livello avanzato

<sup>(\*)</sup> Quadro comune europeo di riferimento per le lingue (ERL)

## Capacità e competenze informatiche

Linguaggi di programmazione conosciuti

**C, C++, Matlab, Octave, SageMath, PARI/GP**

## Attività editoriale

Attività di revisione per riviste

Dal 2018

Dal 2019

Dal 2020

IEEE Communication Letters, Security and Communication Networks

IEEE Transactions on Very Large Scale Integration Systems, Designs, Codes and Cryptography (DES), Cryptography MDPI, IEEE Transactions on Circuits and Systems I: Regular Papers, IEEE Transactions on Information Theory

IEEE Transactions on Information Forensics & Security, Entropy MDPI

Organizzazione di special issue in riviste internazionali

2021

Co-organizzatore di una special issue intitolata "*Public-Key Cryptography in the Post-quantum Era*", per rivista internazionale Cryptography (MDPI)

## Partecipazione in comitati di conferenze internazionali

International Workshop on Code-Based Cryptography (CBCrypto)

Membro dell'Organizing Committee per le edizioni 2019 e 2020, membro del Technical Program Committee per le edizioni 2019, 2020 e 2021

## Premi e riconoscimenti

Best Paper Award

Best Paper Award come co-autore dell'articolo "*A Failure Rate Model of Bit-flipping Decoders for QC-LDPC and QC-MDPC Code-based Cryptosystems*", presentato alla conferenza internazionale "International Joint Conference on e-Business and Telecommunications (ICETE)", Luglio 2020

## Attività di ricerca

Settembre 2019, Novembre 2019 - Marzo 2020

Research fellow presso Florida Atlantic University, Boca Raton, Florida, USA

Novembre 2018

Visita scientifica presso University of Zurich, Zurigo, Svizzera

Marzo 2018 - Aprile 2018

Visita scientifica presso Florida Atlantic University, Boca Raton, Florida, USA

Dicembre 2016 - Luglio 2020

Partecipazione ad iniziativa di standardizzazione per algoritmi crittografici post quantum a chiave pubblica, promossa dal NIST, come co-autore della suite di algoritmi di cifratura LEDAcrypt.

## Partecipazione in progetti di ricerca

**Human Digital Flexible – Factory of the Future Laboratory (HD3FLAB) - Progetto: MERCURY- sMart sEcuRe deCentralized indUstRY**  
Finanziato da Regione Marche

**Ruolo: collaboratore.**

Il progetto propone la progettazione e realizzazione di una piattaforma di automazione industriale che integri edge computing con tecniche di cybersecurity e DLT. Lo scopo dell'utilizzo della tecnologia blockchain è quello di far comunicare i nodi che partecipano alla rete, aumentando lo scambio di dati e l'efficienza della rete stessa, garantendone comunque la sicurezza. Per poter realizzare queste funzionalità, è necessario studiare accuratamente le primitive crittografiche con cui i nodi devono essere equipaggiati, in modo da garantire sicurezza ed efficienza (tenendo conto delle ridotte capacità computazionali di alcuni dei nodi che partecipano alla rete).

**Metodi e strumenti innovativi  
per il REACTIVE Product  
Design and  
Manufacturing-REACT**  
Finanziato tramite PON-PNR  
2015-2020

## Didattica

Supporto alla didattica

## Ruolo: collaboratore.

Il progetto mira a sviluppare metodi e strumenti innovativi per reagire in modo efficace all'analisi del contenuto informativo rilevabile sulle linee di produzione della Smart Factory, dove tipicamente transita un'enorme mole di dati.

Attività di supporto alla didattica per i corsi di *Teoria dei Segnali* (ELE), *Telecomunicazioni* (ELE), *Trasmissioni numeriche* (ELE), *Teoria dell'informazione e codici* (ELE), *Sicurezza delle Telecomunicazioni* (ELE), *Octave Phd Course*, presso l'Università Politecnica delle Marche.

## Pubblicazioni

Rivista Internazionale

2021

K. Koleci, **P. Santini**, M. Baldi, F. Chiaraluca, M. Martina and G. Masera, "*Efficient Hardware Implementation of the LEDAcrypt Decoder*," in *IEEE Access*, vol. 9, pp. 66223-66240, 2021, doi: 10.1109/ACCESS.2021.3076245.

2020

G. Banegas, P. S. L. M. Barreto, E. Persichetti, and **P. Santini**, "*Designing Efficient Dyadic Operations for Cryptographic Applications*," *Journal of Mathematical Cryptology*, vol. 14, no. 1, 2020, pp. 95-109, doi: 10.1515/jmc-2015-0054.

2020

**P. Santini**, M. Battaglioni, M. Baldi and F. Chiaraluca, "*Analysis of the error correction capability of LDPC and MDPC codes under parallel bit-flipping decoding and application to cryptography*", *IEEE Trans. on Commun.*, early access, Apr. 2020, DOI: 10.1109/TCOMM.2020.2987898.

2020

**P. Santini**, M. Baldi, and F. Chiaraluca, "*Complexity of statistical attacks on QC-LDPC code-based cryptosystems*," *IET Information Security* 14.3 (2020): 304-312, doi:10.1049/iet-ifs.2019.0420.

2019

J. Hu, M. Baldi, **P. Santini**, N. Zeng, S. Ling and H. Wang, "*Lightweight Key Encapsulation Using LDPC Codes on FPGAs*," in *IEEE Transactions on Computers*, vol. 69, no. 3, pp. 327-341, 1 March 2020, doi: 10.1109/TC.2019.2948323.

2019

M. Baldi, A. Barengi, F. Chiaraluca, G. Pelosi, and **P. Santini**, "*A finite regime analysis of information set decoding algorithms*," *Algorithms*, 12(10), 209, 2019, doi: 10.3390/a12100209.

2019

M. Baldi, F. Chiaraluca, J. Rosenthal, **P. Santini**, and D. Schipani, "*Security of generalised Reed-Solomon code-based cryptosystems*," *IET Information Security*, 13(4), 404-410, 2019, doi: 10.1049/iet-ifs.2018.5207.

Conferenza Internazionale

2020

D. Apon, R. Perlner, A. Robinson, and **P. Santini**, "*Cryptanalysis of LEDAcrypt*," in *Annual International Cryptology Conference* (pp. 389-418), August 2020, Springer, Cham., doi: 10.1007/978-3-030-56877-1\_14.

2020

J.F. Biasse, G. Micheli, E. Persichetti, **P. Santini**, "*LESS is more: Code-based signatures without syndromes*," in *International Conference on Cryptology in Africa* (pp. 45-65), July 2020. Springer, Cham., doi: 10.1007/978-3-030-51938-4\_3.

2020

M. Baldi, A. Barengi, F. Chiaraluca, G. Pelosi, **P. Santini**, "*A Failure Rate Model of Bit-flipping Decoders for QC-LDPC and QC-MDPC Code-based Cryptosystems*," in *SECURITY 2020-17th International Conference on Security and Cryptography* (pp. 238-249), 2020, ScitePress, doi: 10.5220/0009891702380249.

2020

**P. Santini**, M. Battaglioni, F. Chiaraluca, M. Baldi and E. Persichetti, "*Low-Lee-Density Parity-Check Codes*," *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9148812.

2019

S. Samardjiska, **P. Santini**, E. Persichetti, G. Banegas, "*A reaction attack against cryptosystems based on LRPC codes*," in *International Conference on Cryptology and Information Security in Latin America* (pp. 197-216), October 2019, Springer, Cham, doi: 10.1007/978-3-030-30530-7\_10.

- 2019 M. Baldi, G. Cancellieri, F. Chiaraluca, E. Persichetti and **P. Santini**, "*Using Non-Binary LDPC and MDPC Codes in the McEliece Cryptosystem*," 2019 AEIT International Annual Conference (AEIT), 2019, pp. 1-6, doi: 10.23919/AEIT.2019.8893339.
- 2019 **P. Santini**, M. Baldi and F. Chiaraluca, "*Cryptanalysis of a One-Time Code-Based Digital Signature Scheme*," 2019 IEEE International Symposium on Information Theory (ISIT), 2019, pp. 2594-2598, doi: 10.1109/ISIT.2019.8849244.
- 2019 M. Battaglioni, **P. Santini**, M. Baldi and G. Cancellieri, "*Obtaining structured generator matrices for QC-LDPC codes*", in Proc. AEIT international annual conference 2019, Florence, Italy, Sep. 2019, doi: 10.23919/AEIT.2019.8893395.
- 2019 M. Baldi, A. Barengi, F. Chiaraluca, G. Pelosi, **P. Santini**, "*LEDAcrypt: QC-LDPC code-based cryptosystems with bounded decryption failure rate*," in Code-Based Cryptography Workshop (pp. 11-43), May 2019, Springer, Cham, doi:10.1007/978-3-030-25922-8\_2.
- 2019 **P. Santini**, M. Battaglioni, M. Baldi, and F. Chiaraluca, "*Hard-decision iterative decoding of LDPC codes with bounded error rate*", in Proc. ICC 2019, Shanghai, China, May 2019, doi: 10.1109/ICC.2019.8761536.
- 2019 **P. Santini**, M. Battaglioni, F. Chiaraluca, and M. Baldi, "*Analysis of reaction and timing attacks against cryptosystems based on sparse parity-check codes*", Code-Based Cryptography, Jan. 2019, doi: 10.1007/978-3-030-25922-8\_7.
- 2018 **P. Santini**, M. Baldi, F. Chiaraluca, "*Assessing and countering reaction attacks against post-quantum public-key cryptosystems based on QC-LDPC codes*," in International Conference on Cryptology and Network Security (pp. 323-343), September 2018, Springer, Cham, doi:10.1007/978-3-030-00434-7\_16.
- 2018 **P. Santini**, M. Baldi, G. Cancellieri and F. Chiaraluca, "*Hindering Reaction Attacks by Using Monomial Codes in the McEliece Cryptosystem*," 2018 IEEE International Symposium on Information Theory (ISIT), 2018, pp. 951-955, doi: 10.1109/ISIT.2018.8437553.
- 2018 M. Baldi, A. Barengi, F. Chiaraluca, G. Pelosi, **P. Santini**, "*LEDAkem: A post-quantum key encapsulation mechanism based on QC-LDPC codes*," in International Conference on Post-Quantum Cryptography (pp. 3-24). Springer, Cham, April 2018, doi: 10.1007/978-3-319-79063-3\_1.
- 2017 M. Baldi, **P. Santini** and G. Cancellieri, "*Post-quantum cryptography based on codes: State of the art and open challenges*," 2017 AEIT International Annual Conference, 2017, pp. 1-6, doi: 10.23919/AEIT.2017.8240549.
- 2016 M. Baldi, **P. Santini** and F. Chiaraluca, "*Soft McEliece: MDPC code-based McEliece cryptosystems with very compact keys through real-valued intentional errors*," 2016 IEEE International Symposium on Information Theory (ISIT), 2016, pp. 795-799, doi: 10.1109/ISIT.2016.7541408.

## Talk

- Gennaio 2020 Invited speaker alla conferenza HiPEAC 2020, Bologna.
- Luglio 2019 Speaker alla conferenza SIAM Conference on Applied Algebraic Geometry, presso University of Bern, Berna, Svizzera.
- Maggio 2019 Speaker alla conferenza CBC 2019, presso Darmstadt, Germania.
- Marzo 2019 Speaker al workshop "Celebrating the influence of Ruud Pellikaan", presso Technische Universiteit Eindhoven, Eindhoven, Olanda.
- Novembre 2018 Seminario presso University of Zurich, Svizzera.
- Ottobre 2018 Speaker alla conferenza CANS 2018, presso Napoli, Italia.
- Luglio 2018 Speaker alla conferenza ISIT 2018, presso Vail, Colorado, USA.
- Aprile 2018 Speaker al workshop CBC 2018, presso Florida Atlantic University, Fort Lauderdale, Florida, USA.
- Aprile 2018 Seminario presso Florida Atlantic University, Boca Raton, Florida, USA.

## Autorizzazione per la pubblicazione sul web

Il sottoscritto Paolo Santini autorizza la pubblicazione del curriculum della sua attività scientifica, didattica e professionale nel sito di ateneo.