Curriculum Vitae

Part I – General Information

Part II – Education

Type	Year	Institution	Notes (Degree,,…)
University graduation	2002-2005	Universita' "Sapienza" Rome	Mathematics Bachelor
Post-graduate studies	2005-2007	Universita' "Sapienza" Rome	Mathematics Master
PhD	2009-2013	University of Auckland	Mathematics PhD
Specialty			
Pre-doctorate training			
Licensure 01			
Licensure 02			

Part III – Appointments

IIIA – Academic Appointments

Start	End	Institution	Position
2012	2014	University of Warsaw	Postdoc
2014	2017	Dakota State University	Assistant Professor
2017	present	Florida Atlantic University	Assistant Professor

IIIB – Other Appointments

Start	End	Institution	Position
2020	2020	CBCrypto 2020 - International Workshop on Code-Based Cryptography.	Chair
2019	2019	A2C - Algebra, Codes and Cryptology conference.	Program Chair
2019	2019	PQCrypto 2019 - Post-Quantum Cryptography Confernece	Program Committee Member
2019	2019	CBC 2019 - Code-Based Cryptography Workshop.	Chair
2018	2018	PQCrypto 2018 - Post-Quantum Cryptography Conference	Program Committee Member

Part IV – Teaching experience

Year	Institution	Lecture/Course
2021	Florida Atlantic University	Algebra I
2020	Florida Atlantic University	Discrete Mathematics
2020	Florida Atlantic University	Engineering Mathematics
2020	Florida Atlantic University	Methods of Calculus
2019	Florida Atlantic University	Calculus III
2019	Florida Atlantic University	Calculus I
2019	Florida Atlantic University	Introduction to Cryptology
2019	Florida Atlantic University	Calculus II
2018	Florida Atlantic University	Modern Algebra
2018	Florida Atlantic University	Calculus I
2018	Florida Atlantic University	Coding Theory
2017	Florida Atlantic University	Introduction to Cryptology
2017	Florida Atlantic University	Calculus II
2016	Dakota State University	Discrete Mathematics
2016	Dakota State University	Mathematics of Cyber Operations
2016	Dakota State University	Introduction to Discrete Mathematics
2015	Dakota State University	Discrete Mathematics
2015	Dakota State University	Trigonometry
2014	Dakota State University	Introduction to Discrete Mathematics
2014	Dakota State University	College Algebra
2014	Dakota State University	Discrete Mathematics
2014	University of Warsaw	Public-Key Cryptography

Part V - Society memberberships, Awards and Honors

Year	Title
2019	Gary Perry Academic Partnership Award
2011	Aitken Prize

Part VI - Funding Information [grants as PI-principal investigator or I-investigator]

Year	Title	Program	Grant value
2019-2022	Secure and Efficient Solutions for Post-Quantum Cryptography from Codes with Compact Representations	NSF SaTC	$499,946
2019	CBCrypto 2020	ORAU Event Sponsorship	$4,000
2019	Young CryptograpHERS: a Cybersecurity Summer Camp for K-12 Girls	Florida Center for Cybersecurity	$73,930
2018	The 7th Code-based Cryptography Workshop	ORAU Event Sponsorship	$4,000
2018-2020	A Platform for the Evaluation of Post-Quantum Primitives	NIST	$194,980

Part VII – Research Activities

Keywords	Brief Description
Cryptography	Research on the design and security of Post-Quantum cryptographic schemes from mathematical foundations using linear codes and lattices
Post-Quantum	
Coding Theory	

Part VIII – Summary of Scientific Achievements

Product type	Number	Data Base	Start	End
Papers [international]	28	Scopus	2012	2021
Papers [national]				
Books [scientific]	2	Scopus	2019	2020
Books [teaching]				

Total Impact factor	5,624
Total Citations	152
Average Citations per Product	5
Hirsch (H) index	8
Normalized H index*	1

*H index divided by the academic seniority.

Part IX– Selected Publications

List of the publications selected for the evaluation. For each publication report title, authors, reference data, journal IF (if applicable), citations, press/media release (if any).

N. Aragon, M. Baldi, J.-C. Deneuville, K. Khathuria, E. Persichetti, P. Santini
Cryptanalysis of a code-based full-time signature.
Designs, Codes and Cryptography, 2021, ISSN:1573-7586, DOI:10.1007/s10623-021-00902-7

N. Drucker, S. Gueron, D. Kostic, E. Persichetti
On the applicability of the Fujisaki-Okamoto transformation to the BIKE KEM.
International Journal of Computer Mathematics: Computer Systems Theory, 2020, Vol.Mathematics of Cryptography and Coding in the Quantum Era, ISSN:2379-9935, DOI:10.1080/23799927.2021.1930176

J.-F. Biasse, G. Micheli, E. Persichetti and P. Santini
LESS is More: Code-Based Signatures Without Syndromes.
Progress in Cryptology - AFRICACRYPT 2020 - 12th International Conference on Cryptology in Africa, Cairo, Egypt, July 20-22, 2020, Proceedings. Lecture Notes in Computer Science 12174, Springer 2020, ISBN 978-3-030-51937-7, pp 45-65

G. Banegas, P. S. L. M. Barreto, E. Persichetti and P. Santini
Designing Efficient Dyadic Operations for Cryptographic Applications.
Journal of Mathematical Cryptology 14(1), pp 95-109 (2020)

E. Persichetti, R. Steinwandt, A. Suarez Corona
From key encapsulation to authenticated group key establishment - A compiler for post-quantum primitives.
Entropy, 2019, ISSN:1099-4300, DOI:10.3390/e21121183

N. Bindel, M. Hamburg, K. Hövelmanns, A. Hülsing and E. Persichetti:
Tighter Proofs of CCA Security in the Quantum Random Oracle Model.
Theory of Cryptography - 17th International Conference, TCC 2019, Nuremberg, Germany, December 1-5, 2019, Proceedings, Part II. Lecture Notes in Computer Science 11892, Springer 2019, ISBN 978-3-030-36032-0 2019, pp 61-90

S. Samardjiska, P. Santini, E. Persichetti and G. Banegas
A Reaction Attack against Cryptosystems based on LRPC Codes.
Progress in Cryptology - LATINCRYPT 2019 - 6th International Conference on Cryptology and Information Security in Latin America, Santiago de Chile, Chile, October 2-4, 2019, Proceedings. Lecture Notes in Computer Science 11774, Springer 2019, ISBN 978-3-030-30529-1, pp 197-216

G. Banegas, P. S. L. M. Barreto, B. Odilon Boidje, P.-L. Cayrel, G. N. Dione, K. Gaj, C. T. Gueye, R. Haeussler, J. B. Klamti, O. N'diaye, D. T. Nguyen, E. Persichetti and J. E. Ricardini
DAGS: Key Encapsulation using Dyadic GS Codes.
Journal of Mathematical Cryptology, 12(4), pp 221-239 (2018)

P. S. L. M. Barreto, S. Gueron, T. Guneysu, R. Misoczki, E. Persichetti, N. Sendrier and J.-P. Tillich
CAKE: Code-based Algorithm for Key Encapsulation.
Cryptography and Coding - 16th IMA International Conference, IMACC 2017, Oxford, UK, December 12-14, 2017, Proceedings. Lecture Notes in Computer Science 10655, Springer 2017, ISBN 978-3-319-71044-0, pp 207-226

E. Persichetti
Secure and Anonymous Hybrid Encryption from Coding Theory.
Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings. Lecture Notes in Computer Science 7932, Springer 2013, ISBN 978-3-642-38615-2, pp 174-187

P.-L. Cayrel, G. Hoffmann and E. Persichetti
Efficient implementation of a CCA2-secure variant of McEliece using generalized Srivastava codes.
Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012. Proceedings. Lecture Notes in Computer Science 7293, Springer 2012, ISBN 978-3-642-30056-1, pp 138-155

E. Persichetti
Compact McEliece keys based on Quasi-Dyadic Srivastava codes.
Journal of Mathematical Cryptology, 6(2), pp 149-169 (2012)