Curriculum vitae

Edoardo Persichetti
Address : Department of Mathematical Sciences, Florida Atlantic University,
777 Glades Road, Boca Raton, FL 33431, USA.
e-mail : epersichetti@fau.edu
web : http ://persichetti.webs.com
07 November 1984 in Rome, Italy

Academic Career

Jan 2014 - present	Assistant Professor. *Florida Atlantic University, USA*
Aug 2014 - Dec 2016	Assistant Professor. *Dakota State University, USA*
Dec 2012 - Jul 2014	Adiunkt Naukowy (Assistant Professor). *University of Warsaw, Poland*

Education

Nov 2009 - Sep 2012	PhD in Mathematics. Supervisor : Steven Galbraith. *University of Auckland, New Zealand*
Nov 2005 - Sep 2007	Master of Science in Mathematics. Supervisor : M. J. de Resmini. *Università degli Studi "La Sapienza", Rome, Italy*
Oct 2002 - Nov 2005	Bachelor of Science in Mathematics. Supervisor : Claudio Bernardi. *Università degli Studi "La Sapienza", Rome, Italy*

Research Interests

Public-Key Cryptography, Provable Security, Coding Theory, Number Theory.

Published papers

— Efficient Implementation of Hybrid Encryption from Coding theory [1].
C2SI Carlet 2017

— On lower bounds for Information Set Decoding over $\mathbb{F}_q$ and on the effect of Partial Knowledge [2].
International Journal of Information and Coding Theory

— Leakage-Resilient Cryptography over Large Finite Fields : Theory and Practice [3].
ACNS 2015

— Code-based public-key encryption resistant to key leakage.
MoCrySEn 2013

— Secure and Anonymous Hybrid Encryption from Coding Theory.
PQCrypto 2013

— Improving the Efficiency of Code-Based Cryptography.
PhD thesis, University of Auckland 2012

— Efficient implementation of a CCA2-secure variant of McEliece using generalized Srivastava codes [4].
PKC 2012

— Compact McEliece keys based on Quasi-Dyadic Srivastava codes.
Journal of Mathematical Cryptology

1. with Pierre-Louis Cayrel, Cheikh T. Gueye, Modou Mboup and Ousmane Ndiaye.
2. with Robert Niebuhr, Pierre-Louis Cayrel and Stanislav Bulygin.
3. with Marcin Andrychowicz and Daniel Masny.
4. with Pierre-Louis Cayrel and Gerhard Hoffmann.

Submitted Papers

— An Improvement of Information-Set Decoding for Codes with a Non-trivial Automorphism Group [5].

— Homomorphic Obfuscation [6].

Preprints

— On a CCA2-secure variant of McEliece in the standard model.
http ://eprint.iacr.org/2012/268.

Honors and Awards

December 2011	Aitken Prize for Best Contributed Talk by a student. *NZMS Colloquium 2011*
November 2011	"People's Choice" award for Best Talk. *NZMASP 2011*
September 2011	High Distinction award. *Faculty of Science Postgraduate Poster Competition 2011*
November 2010	Best Pure Mathematics Talk award. *NZMASP 2010*
September 2010	Certificate of Merit. *Faculty of Science Postgraduate Poster Competition 2010*

Selected Talks given at Conferences and Workshops

July 2016	DIMACS Workshop on Cryptography and its Interactions. *Rutgers University, New Jersey, USA*
June 2015	ACNS 2015. *Columbia University, New York, USA*
September 2013	MoCrySEn 2013. *Regensburg, Germany*
June 2013	CBC - Code Based Cryptography Workshop. *INRIA, Rocquencourt, France*
June 2013	PQCrypto 2013. *Limoges, France*
May 2012	PKC 2012. *Darmstadt, Germany*
May 2012	CBC - Code Based Cryptography Workshop. *DTU, Copenhagen, Denmark*
December 2011	NZMS Colloquium. *University of Auckland, New Zealand*
October 2011	SP-ASCrypto, the São Paulo Advanced School of Cryptography. *Atibaia, SP, Brasil*
November 2010	NZMASP 2010 - New Zealand Mathematics and Statistics Postgraduate conference. *University of Canterbury, Christchurch, New Zealand*

Organized Conferences and Events

NZMASP 2012 - New Zealand Mathematics and Statistics Postgraduate conference.
University of Auckland, New Zealand

12-16 November, 2012.

5. with Pierre-Louis Cayrel, Cheikt Gueye and Jean Belo Klamti.
6. with Vincenzo Iovino and Francesco Rossi.

Teaching Experience

Florida Atlantic University

— MAC 2312 (Calculus II).
Spring 2017

Dakota State University

— MATH 102 (College Algebra).
Fall 2014

— MATH 120 (Trigonometry).
Spring 2015

— MATH 201 (Introduction to Discrete Mathematics).
Fall 2014 and 2015, Spring 2015 and 2016, Summer 2015 and 2016 (face to face and online)

— MATH 204 (Mathematics for Cyber Operations).
Spring 2016

— MATH 316 (Discrete Mathematics).
Fall 2014, Spring 2015 and 2016

— MATH 318 (Advanced Discrete Mathematics).
Spring 2016

University of Warsaw

— Public-Key Cryptography : a Mathematical Insight (Graduate course).
Semester 2, AY 2013-2014

University of Auckland

— Superstart intensive course.
Academic Years 2010, 2011 and 2012

— MATHS 108 (General Mathematics 1).
Semester 1 and 2, 2011, Semester 1, 2012

— MATHS 208 (General Mathematics 2).
Semester 2, 2012 and Summer School Term, 2012

— COMPSCI 225 (Discrete Structures in Mathematics and Computer Science).
Semester 2, 2010 and Semester 1, 2012

— MATHS 253 (Advancing Mathematics 3).
Semester 1, 2011

— MATHS 255 (Principles of Mathematics).
Semester 2, 2011

— MATHS 315 (Mathematical Logic).
Semester 2, 2012

— MATHS 328 (Algebra and Applications).
Semester 1, 2012

— MATHS 714 (Number Theory).
Semester 2, 2010 and Semester 2, 2011

Committee Work

— Assessment Coordinating Committee, Curriculum Committee, Diversity Committee, Code of Conduct Board, Cyber Operations Faculty Search.
Ongoing

— Mathematics Faculty Search.
Spring 2015, Summer 2016

Invitations and Visits

July 2017	Invited talk at SIAM Conference on Applied Algebraic Geometry (AG17).
June 2016	Invited by Nigel Boston at UW - Madison (USA) for a workshop on Cybersecurity.
March 2016	Invited by Elisa Gorla at Université de Neuchâtel (CH) for a talk on Code-Based Cryptography.
January 2014	Visited Jonathan Katz at University of Maryland (USA) to give a talk about my work on Leakage-Resilient LPN-based Authentication Schemes.
October 2013	Visited Eike Kiltz at Ruhr-Universität Bochum (Germany) for a research project on leakage-resilient authentication schemes.
April 2011	Visited Pierre-Louis Cayrel at CASED, Center for Advanced Security Darmstadt (Germany) to present my paper "Compact McEliece keys based on Quasi-Dyadic Srivastava codes".

Grants

January 2016	College Research Award, Faculty of Arts and Sciences. *1000 US$*
June 2012	Travel Grant, New Zealand Mathematical Society (NZMS). *800 NZ$*
May 2012	Travel Grant, European Network of Excellence in Cryptology II (ECRYPT-II). *Full cost of travel and accommodation at the CBC - Code Based Workshop in Copenhagen*
April 2012	Performance-Based Research Fund (PBRF). *1500 NZ$*
October 2011	Travel Grant, University of Campinas/University of São Paulo. *Full cost of travel and accommodation at the São Paulo Advanced School of Cryptography*
May 2011	PostGraduate Student Association (PGSA) Travel Grant. *500 NZ$*
March 2011	Performance-Based Research Fund (PBRF). *1500 NZ$*

Refereeing

— WCS 2017, ISIT 2014, ISC 2013, ACISP 2013, Eurocrypt 2010, 2012, 2013, 2014, Crypto 2011, 2013, Asiacrypt 2012, 2014, PQCrypto 2011, 2016, SAC 2011

— Design, Codes and Cryptography, Journal of Algebra Combinatorics Discrete Structures and Applications

— IACR book reviews (several books)

Other Professional Experiences and Skills

Present	Editor of the IACR book review system. *Since January 2014*
Aug 2012, 2011, 2010	Organization of Courses and Careers Day (Mathematics Department). *University of Auckland, New Zealand*
December 2011	Helped organizing NZMS Colloquium 2011. *University of Auckland, New Zealand*
Jan - Aug 2005	Erasmus project for study abroad. *Universidade de Lisboa, Lisbon, Portugal*

Languages spoken

Italian (Mother Tongue), English, Portuguese (Fluent), Spanish (Good).

Professional society memberships

AMS, NZMS, IACR.