Giacomo Micheli

Curriculum Vitae

Department of Mathematics,
University of South Florida,
Tampa.
+1 813 974 8967
gmicheli@usf.edu
gmicheli.myweb.usf.edu/

Updated: June 21, 2022

Personal information

Name:	Giacomo
Surname:	Micheli
Birthplace:	Italy, Rome
Birthdate:	October 20, 1988
Citizenship:	Italian
Current Position:	Tenure-Track Assistant Professor at University of South Florida
Previous Positions:	Postdoctoral Fellow at Massachusetts Institute of Technology, Research Fellow at University of Oxford, Scientist at EPFL.

Education

1st of October 2015	**Ph.D. diploma issued** (awarded with distinction: top 5%)
10th of June 2015	Ph.D. thesis defended. Title: *Densities over Global Fields, Arithmetic of Subfield Preserving Maps and Applications to Cryptography.*
October 2012 - June 2015	Ph.D. program at the **Zurich Graduate School in Mathematics** under the supervision of Prof. J. Rosenthal.
July, 2012	**Master degree in Mathematics.** *Summa cum Laude.* Master Thesis Title: *Noncommutative Algebraic Varieties* co-supervised by Prof. C. De Concini (University of Rome "La Sapienza") and Prof. J. T. Stafford (University of Manchester)
September, 2011 - June, 2012	**Erasmus Program:** "University of Manchester"
July, 2010	**Bachelor degree in Mathematics.** *Summa cum Laude* University of Rome, "La Sapienza"

Grants and Awards

Spring 2022	Course Improvement Grant: $3'000 (PI)
Spring 2022	Proposal Enhancement Grant: $25'000 (PI)
Summer 2021	NSF grant 2127742: $500'000 (PI)
Summer 2021	Simons Foundation Collaboration Grant, pre-award notification (PI): $42000 (declined because of the NSF grant above).
Spring 2020	Strategic Investment Proposal $95'000 (CO-PI)
October 2018	Swiss National Science Foundation return grant number 171249 (awarded in December 2016) roughly $109'000 (PI)
June 2017	Elsevier Award at Fq13 conference.
April 2017	Swiss National Science Foundation grant number 171248 (awarded in December 2016) roughly $80'000 (PI)

October 2015	Swiss National Science Foundation grant number 161757 roughly $70'000 (PI)
October 2015	Ph.D. Thesis awarded with Distinction (with cash prize)
February, 2012	**"Master Excellence Path"** in Mathematics at "La Sapienza" University, Tuition fees reimbursement for the academic year 2011/2012 (10 positions available)
September 2011	Erasmus grant, University of Manchester
2008/2010	**"Excellence Path"** in Mathematics at "La Sapienza" University. Tuition fees reimbursement for the academic year 2009/2010 (30 positions available).

Selected Research Stays

September 2021	Columbia University, New York, US.
July 2021	Scuola Normale Superiore, Pisa, IT.
October 2018	RICAM, Linz, AT.
September 2018	Columbia University, New York, US.
April 2017	Pierre and Marie Curie University, Paris, FR.

Previous Positions

October 2012 - October 2015	Ph.D. student at the Zurich Graduate School in Mathematics
October 2015 - February 2016	Postdoctoral Fellow at MIT
February 2016 - October 2018	Research Fellow at University of Oxford
October 2018 - August 2019	SNF Fellowship at EPFL

Areas of interest

Applied Algebra:	Finite Fields, Cryptography, Coding Theory.
Number Theory:	Arithmetic of Global Fields.

Research Talks

May 18, 2022, Rome, IT	University of Rome "La Sapienza", Algebra seminar *An Equivariant Isomorphism Theorem for Arboreal Galois Representations*
April 25-29, 2022, hybrid, Oaxaca, MX	Algebraic Methods in Coding Theory and Communication, *An introduction to the theory of locally recoverable codes.*
March 19-20, 2022, online (formerly at Tufts University, Medford, US)	AMS Spring Eastern Sectional Meeting, *A Galois Theoretical Perspective on APN functions.*
December 17, 2021, online	Roma 3 University, Number Theory Seminar, *Data Storage Using Galois Theory*
November 9, 2021, online	Universty of Ohio, Colloquium talk, *Data Storage Using Galois Theory*
May 28, 2021, online	CrypTO, *Understanding polynomial maps over finite fields*
January 7, 2021, online	Joint Mathematical Meeting, *Understanding polynomial maps over finite fields*
October 10-11, 2020, online (formerly at University of Tennessee at Chattanooga)	AMS Fall Southeastern Sectional Meeting, *An Equivariant Isomorphism Theorem for Arboreal Galois Representations.*

September 17, 2020, online	ACCESS seminar series: Algebraic Coding and Cryptography on the East coast Seminar Series `https://sites.google.com/view/access-seminar/home` *Algebraic constructions of complete m-arcs.*
July 23, 2020, Tampa, US	Graduate Colloquium *Doing research as a student: tips and tricks.*
February 21, 2020, Tampa, US	Analysis Seminar, USF *The density of shifted and affine Eisenstein polynomials*
January 15, 2020, Denver, US	Joint Mathematics Meeting of the AMS. *Optimal Locally Recoverable Codes via Chebotarev Density Theorem.*
November 19, 2019, Virginia Tech, US	Algebra Seminar. *Two applications of the theory of finite fields*
October 18, 2019, Virginia Tech, US	Algebra Seminar. *An Equivariant Isomorphism Theorem for Arboreal Galois Representations*
September 30, 2019, University of South Florida, US	Discrete Mathematics Seminar. *An Equivariant Isomorphism Theorem for Arboreal Galois Representations*
July 13, 2019, Bern, CH	SIAM Conference on Applied Algebraic Geometry, *Applications of the Theory of Finite Fields.*
July 10, 2019, Bern, CH	SIAM Conference on Applied Algebraic Geometry, *Optimal Locally Recoverable Codes via Chebotarev Density Theorem.*
June 12, 2019, University of South Florida, US	Discrete Mathematics Seminar. *Two Applications of the Theory of Finite Fields.*
June 6, 2019, Vancouver, CA	Fq14 *The Algebraic Theory of Fractional Jumps*
May 7, 2019, EPFL, CH	Number Theory Seminar. *Arboreal Galois representations attached to quadratic arithmetic dynamical systems.*
January 14, 2019, University of South Florida, US	Discrete Mathematics Seminar. *Applications of Chebotarev Density Theorem to Computer Science.*
October 20, 2018, University of Michgan, US	AMS Sectional Meeting, *Fractional Jumps.*
October 16, 2018, RICAM, AT	Pseudorandomness and Finite Fields, *Fractional Jumps.*
September 24, 2018, Brown University, US	Number Theory Seminar, *Permutations and codes from a density method.*
September 21, 2018, City University of New York, US	Algebra and Cryptography Seminar, *Permutations and codes from a density method.*
September 14, 2018, Columbia University, US	Number Theory Seminar, *Permutations and codes from a density method.*
14-16 June, 2018, Bergen, NO	WAIFI 2018, *Fractional jumps: complete characterization and an explicit infinite family.*
March 8, 2018, Oxford, UK	Number Theory Seminar, *Permuting F_q with a density method.*
February 21, 2018, Oxford, UK	Cryptography Seminar, *Full Orbit sequences in the Affine Space.*
October 12, 2017, Rostock, DE	*Regular patterns among primes in function fields.*
August 1, 2017, Atlanta, US	SIAM Conference on Applied Algebraic Geometry *On the selection of polynomials for the DLP algorithm.*
June 6, Gaeta, IT	Fq13 *Regular patterns in $F_q[x]$.*
April 28 2017, Paris, FR	Paris 6 *Irreducible compositions of degree two polynomials over finite fields have regular structure.*
April 27 2017, Paris, FR	Paris 8 *Irreducible compositions of degree two polynomials over finite fields have regular structure.*

April 12 2017, Neuchatel, CH	University of Neuchatel *Galois Theory for Discrete Logarithm Problems.*
October 24, 2016, Oxford, UK	Junior Number Theory Seminar, *On sets of irreducible polynomials closed by composition.*
July 13, 2016, Ghent, BE	International Workshop on Arithmetic of Finite Fields (WAIFI 2016) *Semigroups of Irreducible Polynomials Closed by Composition.*
May 17, 2016, University of Oxford, UK	Research seminar series: Number Theory Tools for Cryptographic applications. *Galois theory over global function fields for discrete logarithm problems.*
May 26, 2016, University of Oxford, UK	Research seminar series: Number Theory Tools for Cryptographic applications. *A local to global principle for density computations over global function fields.*
May 31, 2016, University of Oxford, UK	Research seminar series: Number Theory Tools for Cryptographic applications. *Applications of the local to global principle.*
July 14, 2015, Saratoga Sprigs, Skidmore College, US	Fq12, the biannual conference on Finite Fields and Applications *The density of Unimodular Matrices over Integrally closed Subrings of Function Fields.*
June 10, 2015, University of Zurich, CH	Ph.D. Defense *Densities over Global Fields, Arithmetic of Subfield Preserving Maps, and Applications to Cryptography.*
May 18, 2015, University of Neuchatel, CH	*The density of Shifted Eisenstein Polynomials.*
January 13, 2015, Rutgers University, US	DIMACS Workshop on The Mathematics of Post-Quantum Cryptography *Hidden Field Knapsack Problems.*
December 2, 2014, ETH, CH	*Hidden Field Knapsack Schemes.*
May 24, 2014, Universitat Autonoma de Barcelona, ES	Workshop on Polynomials over Finite Fields: Functional and Algebraic Properties, *Canonical Subfield Preserving Maps.*

Memberships

Since January 2020	Member of the American Mathematical Society
Since June 2020	Member of the Center for Cryptographic Research 40.1720 (Co-Founder and Co-Director)

Service

Research seminar series: Applied algebra	Fall Semester 2013-Spring semester 2015, University of Zurich (Co-organizer)
Since 2015	Reviewer for *Mathematical Reviews (MathSciNet)*
2017-2018	Antiharassment advisor, University of Oxford
Spring 2017	Co-organizer of the Spring School on Lattice-Based Cryptography, University of Oxford (main organizer: Dr. Ali El-Kaafarani)
External examiner for M.Sc. thesis (University of Oxford)	Cyprien Delpech de Saint Guilhem, Jan Henrik Wiik, Chan Bae, Carl Mackintosh.
Exam checker (University of Oxford)	B3.4-Algebraic Number Theory, 2016-2017 and 2017-2018, Lecturer: Prof. Minhyong Kim)
Paris 6, June 24-27, 2019	In the program commitee of Number-Theoretic Methods in Cryptology 2019 `http://nutmic2019.imj-prg.fr/PC.php` (chairs: Antoine Joux and Jacek Pomykała)

University of Bern, July 15-19, 2019	Co-organizer of the symposium “Applications of Finite Fields Theory” at the SIAM AG conference
Code Based Cryptography	In the program committee of CBC2020
Code Based Cryptography	In the program committee of CBC2021
CodeBreakHers 2021	Co-organizer
SIAM conference on Applied Algebraic Geometry, August 16-20, 2021	Co-organizer of the symposium “Algebraic Methods for Cryptography” at the SIAM AG conference
Code Based Cryptography	In the program committee of CBC2022

Teaching Experience

Constructing Locally Recoverable Codes using Galois Theory over global function fields	Summer 2022, This is a sequence of lectures I gave for the doctoral program in Mathematics at the University of Rome "La Sapienza" (Lecturer)
Graduate Algebra II	Spring Semester 2022, University of South Florida (Lecturer)
Graduate Algebra I	Fall Semester 2021, University of South Florida (Lecturer)
Elementary Abstract Algebra II	Spring Semester 2021, University of South Florida (Lecturer)
Elementary Abstract Algebra	Fall Semester 2020, University of South Florida (Lecturer)
Elementary Abstract Algebra II	Spring Semester 2020, University of South Florida (Lecturer)
Elementary Abstract Algebra	Fall Semester 2019, University of South Florida (Lecturer)
Cryptography: a hands-on course	Spring 2018, University of Rome “La Sapienza” (Lecturer).
Galois Theory	Michaelmas term 2017, University of Oxford (Lecturer)
Galois Theory	Michaelmas term 2016, University of Oxford (Lecturer)
Research seminar series: number theory tools for cryptographic applications	Trinity Term 2016, University of Oxford (Lecturer and organizer)
Cryptography	Spring Semester 2015, University of Zurich (Teaching Assistant and Tutor)
Curves over finite fields	Fall Semester 2014, University of Zurich (Lecturer)
Seminar series: Riemann Hypothesis for curves over finite fields	Fall Semester 2014, University of Zurich (Organizer)
Seminar series: Selected Topics on arithmetic of Finite Fields	Spring Semester 2014, University of Zurich (Lecturer and organizer)
Cryptography	Fall Semester 2013, University of Zurich (Teaching Assistant and Tutor)
Linear Algebra II	Spring Semester 2013, University of Zurich (Teaching Assistant and Tutor)
Linear Algebra I	Fall Semester 2012, University of Zurich (Teaching Assistant and Tutor)
Undergraduate students supervised (University of Oxford)	○ Daniel Hart (with C. Petit), ○ DoHoon Kim (with C. Petit), ○ Guillermo Pascual Perez (with C. Petit), ○ Yuxuan Quek (with C. Petit). ○ Carl Mackintosh. ○ Amber Borowiec.

Master students supervised (University of Zurich)
- Edoardo Dotti, project title: *Eisenstein Polynomials over Function Fields* https://link.springer.com/article/10.1007/s00200-015-0275-2

Ph.D. students supervised on specific projects
- Federico Amadio Guidi, University of Oxford, (Ph.D. advisor: Prof. Sir Andrew Wiles FRS), project title: *Full Orbit Sequences on Affine Spaces via Fractional Jumps.*
- Violetta Weger, University of Zurich (Ph.D. advisor: Prof. Joachim Rosenthal), project title: *Cryptanalysis of the CLR Cryptosystem.*
- Sofia Lindqvist (Ph.D. advisor: Prof. Ben Green FRS), project title: *The discrepancy of fractional jumps.*

Individual tutorials
- Matthew McGray (Finite Fields, RSA and Factoring algorithms, Pseudorandomnumber generation)

List of Publications

34 A. Ferraguti, A. Dukes, G. Micheli, Optimal Selection for Good Polynomials of Degree up to Five, *Designs Codes and Cryptography* https://arxiv.org/abs/2104.01434

33 D. Bartoli, G. Micheli, G. Zini, F. Zullo, r-fat linearized polynomials over finite fields, *Journal of Combinatorial Theory Series A*, https://arxiv.org/abs/2012.15357

32 G. Micheli, S. Schraven, V. Weger, Local to global principle for expected values, *Journal of Number Theory* https://arxiv.org/abs/2008.06235

31 D. Goldfeld, G. Micheli, The Algebraic Theory of Fractional Jumps, *Finite Fields and Their Applications: 14th International Conference on Finite Fields* https://doi.org/10.1515/9783110621730-009

30 D. Bartoli, G. Micheli. Algebraic constructions of complete m-arcs, *Combinatorica* https://arxiv.org/abs/2007.00911

29 F. Biasse, G. Micheli, E. Persichetti, and P. Santini. LESS is More: Code-Based Signatures without Syndromes, *Lecture Notes in Computer Science*, 12th International Conference on Cryptology in Africa, Cairo, Egypt, July 20-22, 2020 https://eprint.iacr.org/2020/594.pdf.

28 A. Ferraguti, G. Micheli. Exceptional scatterdness in prime degree, *Journal of Algebra* https://www.sciencedirect.com/science/article/pii/S0021869320304993?via%3Dihub

27 A. Ferraguti, G. Micheli. An equivariant isomorphism theorem for mod p reductions of arboreal Galois representations. *Transactions of the American Mathematical Society* https://www.ams.org/journals/tran/0000-000-00/S0002-9947-2020-08247-6/

26 G. Micheli, A. Neri. New Lower Bounds for Permutation Codes using Linear Block Codes *IEEE Transactions on Information Theory* vol. 66, no. 7, pp. 4019-4025, 2020 https://ieeexplore.ieee.org/document/8920027

25 K. Khathuria, G. Micheli, V. Weger. On the algebraic structure of Epm and applications to cryptography, *Applicable Algebra in Engineering Communication and Computing* https://link.springer.com/article/10.1007/s00200-019-00410-1.

24 G. Micheli. Constructions of Locally Recoverable Codes which are Optimal, *IEEE Transactions on Information Theory* https://ieeexplore.ieee.org/document/8823942

23 F. Amadio Guidi, G. Micheli. Fractional jumps: complete characterisation and an explicit infinite family, Arithmetic of Finite Fields, *Lecture Notes in Computer Science* (2018). https://link.springer.com/chapter/10.1007/978-3-030-05153-2_14

22 A. Ferraguti, G. Micheli. Complete Classification of permutation rational functions of degree three over finite fields *Designs Codes and Cryptography* https://arxiv.org/abs/1805.03097

21 G. Micheli, V. Weger. On Rectangular Unimodular Matrices over the algebraic integers. *SIAM Journal on Discrete Mathematics*, 33(1), 425-437. https://epubs.siam.org/doi/abs/10.1137/18M1177093

20 G. Micheli. On the Selection of Polynomials for the DLP Quasi-Polynomial Time Algorithm for Finite Fields of Small Characteristic. *SIAM Journal on Applied Algebra and Geometry* 3(2) (2019): 256-265. https://epubs.siam.org/doi/abs/10.1137/18M1177196

19 F. Amadio Guidi, S. Lindqvist, G. Micheli. Full Orbit Sequences in Affine Spaces via Fractional Jumps and Pseudorandom Number Generation. *Mathematics of Computation* http://www.ams.org/journals/mcom/0000-000-00/S0025-5718-2018-03400-7/).

18 G. Micheli, V. Weger. Cryptanalysis of the CLR Cryptosystem, *Designs Codes and Cryptography*, https://link.springer.com/article/10.1007/s10623-018-0500-7.

17 G. Micheli. A local to global principle for densities over function fields https://arxiv.org/abs/1701.01178 (submitted).

16 D. Hart, D. Kim, G. Micheli, G. Pascual Perez, C. Petit, and Y. Quek. A Practical Cryptanalysis of WalnutDSA$^{\text{TM}}$. *Lecture Notes in Computer Science* PKC 2018 https://eprint.iacr.org/2017/1160

15 A. Ferraguti, G. Micheli, and R. Schnyder. Irreducible compositions of degree two polynomials over finite fields have regular structure, *The Quarterly Journal of Mathematics* https://academic.oup.com/qjmath/advance-article-abstract/doi/10.1093/qmath/hay015/4955874?redirectedFrom=fulltext.

14 D.R. Heath-Brown, G. Micheli. Irreducible polynomials over finite fields produced by composition of quadratics, *Revista Matématica Iberoamericana.*

13 A. Ferraguti, G. Micheli. On the existence of infinite, non-trivial F-sets, *Journal of Number Theory*, Volume 168, November 2016, Pages 1–12, http://www.sciencedirect.com/science/article/pii/S0022314X16300786.

12 G. Micheli, R. Schnyder. The Density of Shifted and Affine Eisenstein Polynomials, *Proceedings of the American Mathematical Society* issue 11, volume 144, Pages 4651-4661 http://www.ams.org/journals/proc/0000-000-00/S0002-9939-2016-13097-9/).

11 A. Ferraguti, G. Micheli and R. Schnyder. On sets of irreducible polynomials closed by composition, *Lecture Notes in Computer Science: Arithmetic of Finite Fields* https://link.springer.com/chapter/10.1007/978-3-319-55227-9_6)

10 E. Dotti, G. Micheli. Eisenstein polynomials over function fields, *Applicable Algebra in Engineering Communication and Computing*, Springer, Volume 27, Issue 2, pp 159-168 http://link.springer.com/article/10.1007%2Fs00200-015-0275-2

9 G. Micheli, R. Schnyder. The density of unimodular matrices over integrally closed subrings of function fields, *Contemporary Developments in Finite Fields and Applications* (Review volume of Fq12, 20 out of 91 talks invited for paper contribution) co-edited by A. Canteaut, G. Effinger, S. Huczynska, D. Panario, L. Storme) http://www.worldscientific.com/worldscibooks/10.1142/9762

8 G. Micheli, R. Schnyder. On the density of coprime m-tuples over holomorphy rings,*International Journal of Number Theory*, 12, 833 http://www.worldscientific.com/doi/abs/10.1142/S1793042116500536

7 G. Micheli, J. Rosenthal, P. Vettori. Linear spanning sets for matrix spaces, *Linear Algebra and Its Applications* Volume 483, October 2015

6 A. Ferraguti, G. Micheli. On Mertens-Cesàro Theorem for number fields, *Bulletin of the Australian Mathematical Society*, Cambridge University Press, Volume 93, Issue 02, 2016, pp 199-210, `http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=10230876&fileId=S0004972715001288`

5 G. Micheli, J. Rosenthal, R. Schnyder. An Information Rate Improvement for a Polynomial Variant of the Naccache-Stern Knapsack Cryptosystem, *Lecture Notes in Electrical Engineering*: Physical and Data-Link Security Techniques for Future Communication Systems, Springer, (2016) Pages: 173-180

4 G. Micheli, D. Schipani. On Canonical Subfield Preserving Polynomials, *Acta Arithmetica* Volume 166, Number 1 (2014)

3 G. Micheli. Cryptanalysis of a noncommutative key exchange protocol, *Advances in Mathematics of Communications*, Volume 9, Issue 2, (2015)

2 G. Micheli. On coefficient constraints and evaluation restrictions for linearized polynomials, *Finite Fields and Their Applications*: Volume 34 (2015) Pages: 139–152

1 G. Micheli, M. Schiavina. A general construction for monoid-based knapsack protocols, *Advances in Mathematics of Communications*, Volume 8, Issue 3, (2014) Pages: 343 - 358