ELISA GORLA

Institut de mathématiques, Université de Neuchâtel
2000 Neuchâtel, Switzerland
Tel: +41-(0)32-7182820, Fax: +41-(0)32-7182801
elisa.gorla @ unine.ch

Generalities

Born on Aug. 20, 1976 in Genova (Italy), Italian citizen.

Education

Ph.D. in Mathematics, University of Notre Dame, May 2004.

M.Sc. in Mathematics, University of Notre Dame, January 2001.

M.Sc. (Italian Laurea) in Mathematics with grade "110/110" cum Laude, Università degli Studi di Genova (Italy), July 1999.

Positions Held

Oct. 2012 - present Full Professor, University of Neuchâtel, Switzerland.

Sept. 2009 - Sept. 2012 Swiss National Science Foundation Professor, University of Basel, Switzerland.

July 2008 - Aug. 2009 Lecturer, University of Zurich, Switzerland.

Aug. 2004 - June 2008 Postdoctoral fellow, University of Zurich, Switzerland.

Aug. 1999 - May 2004 Graduate/Teaching Assistant, University of Notre Dame, USA.

Visiting Positions in Research Centers

Nov.-Dec. 2012 Research Member at the Mathematical Science Research Institute (Berkeley, CA, USA),in connection with the 2012/13 program on "Commutative Algebra".

Jan.-Feb. 2011 Research Member at the Mittag Leffler Institute (Stockholm, Sweden), in connection with the Spring 2011 Program on "Algebraic Geometry with a view towards applications".

Sept.-Oct. 2006 Research Member at the Fields Institute (Toronto, Canada), in connection with the Fall 2006 Thematic Program in Cryptography.

Aug.-Oct. 2005, March 2006 Guest at the Max-Planck-Institut für Mathematik, Bonn.

Research Stays at other Institutions

University of Genova (Italy), University of Notre Dame (USA), University of Pisa (Italy), Max Planck Institut für Mathematik (Bonn, Germany), University College Dublin (Ireland), Fields Institute (Canada), Universität Osnabrück (Germany), Ohio University (Athens, OH, USA), Universitat de Barcelona (Spain), University of Kentucky (Lexington, KY, USA), University of Zurich (Switzerland), Mittag Leffler Institute (Stockholm, Sweden), Academia Sinica (Taipei, Taiwan), Mathematical Science Research Institute (Berkeley, CA, USA).

Selected Awards and Grants

Featured on "AcademiaNet - Expert Database of Outstanding Female Scientists and Scholars".

Representative of the Swiss node in the Management Committee of the ICT COST Action IC1104 "Random Network Coding and Designs over GF(q)" (Apr. 2012 -Apr. 2016).

Financial support from the Swiss Academy of Sciences – SCNAT for the organization of the conference "Trends in Coding Theory" (2'000 CHF).

Recipient of a grant from Centro Stefano Franscini (ETH, Zurich) to organize a conference on "Trends in Coding Theory" on Oct. 28 - Nov. 2, 2012. Main applicant. Co-applicants are Joachim Rosenthal (Univ. Zurich) and Amin Shokrollahi (EPF Lausanne). (PI, 35'000 CHF).

Selected Awards and Grants continued

Recipient of a Swiss National Science Foundation Professorship, grant no. 123393, Sept. 2009 - Aug. 2013 (PI, ca 1'294'000 CHF).

Invitation and financial support from the Mittag-Leffler Institute (Stockholm, Sweden) to participate to the program on "Algebraic Geometry with a view towards applications", Spring 2011.

Financial support for short term visitors from the Mathematics Department of the University of Kentucky awarded in 2010 and 2011 ($2000 per visit).

Recipient of the "Forschungskredit der Universität Zürich", grant no. 57104101, Jan.-Dec. 2008. This grant funded my postdoctoral position for 1 year (PI, ca 80'000 CHF).

Member of the consortium "Azione integrata Italia-Spagna" financed by MIUR (Italian Ministry for University and Research) in 2007–2009. The grant funded visits to Barcelona (Spain) and Genova (Italy) to speak at workshops and collaborate with other members of the consortium.

Invitation and financial support from the Fields Institute (Toronto, Canada) to participate to the Fall 2006 Thematic Program in Cryptography.

Member of the "Vigoni project" (EU-financed program for cooperation between Italy and Germany) in 2005-2006. The project financed a visit to the University of Osnabrück (Germany) to collaborate with Prof. W. Bruns.

Yearly stipend from the Max Planck Insitut für Mathematik - Bonn in 2005/06 (used only for 4 months).

Marie Curie Intra-European Fellowship for the proposal "Algebraic and Cohomological aspects of Algebraic Geometry", Individual grant, which would have completely funded my postdoctoral position for 2 years starting in 2005 (declined).

Fellowship from the Istituto Nazionale di Alta Matematica F. Severi (Italian National Institute for Higher Mathematics), August 1999-July 2002. The grant funded my doctoral studies for 3 years.

Languages

Italian (native), English (fluent), German and Spanish (good).

Postdoctoral Fellows supervised

Alexandru Constantinescu (since Sept. 2010).

Doctoral Students supervised

Maike Massierer (since Sept. 2009).

Matey Mateev (since Jan. 2010).

Alberto Ravagnani (since Sept. 2012).

External Examiner on Ph.D. Dissertations

Felice Manganiello, University of Zurich, defended in August 2011.

Joan Pons-Llopis, University of Barcelona, defended in June 2011.

Master Students supervised

Richard Köppel, Diplom Universität Zürich, 2007 (jointly with J. Rosenthal).

Andrés Gentzen, MS Degree Universität Zürich, 2007 (jointly with J. Rosenthal).

Vita Pasic, MS Degree Universität Zürich, 2009 (jointly with J. Rosenthal).

Judith Keller, Universität Zürich, in progress.

Other Graduate Research Projects supervised

Senior mentor for the research project "Tori in Cryptography", 2006 summer school on "Computational Number Theory and Applications to Cryptography", University of Wyoming (Laramie, WY), June 19-July 7, 2006.

Senior mentor for the research project "Algebraic Geometry Based Cryptosystems", during the "2004 IMA Summer Program for Graduate Students in Coding and Cryptography", June 8-26, 2004.

Conference and Seminars Organization

Organizer of the Colloquium Series at the University of Neuchâtel, since Jan. 2013.

Organizer (together with J. Rosenthal) of the Seminar in Coding Theory and Cryptography, joint between the Universities of Neuchâtel and Zurich (since 2013).

Organizer (together with I. Duursma and J. Rosenthal) of minisymposia on "Coding Theory and Geometry" and "Cryptography and Number Theory" at the "SIAM Conference on Applied Algebraic Geometry 2013", taking place at Colorado State University (USA) in August 2013.

Organizer (together with J. Rosenthal and A. Shokrollahi) of a conference on "Trends in Coding Theory", partially funded by the Center Stefano Franscini (ETH Zurich), which took place in the Monte Verita' Conference Center in October 2012.

Organizer (together with J. Blanc, H. Kraft, and F. Kutzschebauch) of the "Workshop Algebra and Geometry", which took place at the University of Bern in September 2012. The workshop was intended for PhD students and organized in cooperation with the Swiss Doctoral Program.

Organizer (together with G. Crippa) of the Perlen Seminar (Colloquium Series) at the University of Basel, for the Spring 2012.

Organizer (together with J. Blanc) of the Perlen Seminar (Colloquium Series) at the University of Basel, for the Fall 2010.

Organizer (together with J. Rosenthal) of the Seminar in Coding Theory and Cryptography, joint between the Universities of Basel and Zurich (2009-2012).

Organizer of the Seminar in Coding Theory and Cryptography at the University of Zurich (2006-2009).

Program Committee for SAC 2008 - Workshop on Selected Areas in Cryptography.

Program Committee for WAIFI 2008 - Workshop on the Arithmetic of Finite Fields.

University Service

Mathematics Department representative in the Committee for Equal Opportunities at the University of Basel (May 2011 - Sept. 2012).

Assistant representative in the Mathematikerrat (Counsel of the Mathematics Institute) at the University of Zurich (2008-2009).

Teaching Experience

I have taught both in English and German at the University of Neuchâtel, the University of Basel, the University of Zurich, and the University of Notre Dame.

Courses taught: Algebraic Geometry, Calculus, Coding Theory, Commutative Algebra, Computer Algebra, Cryptography, Elliptic Curves.

Student seminars which I planned and ran: Commutative Algebra, Computer Algebra, Cryptology, Elliptic Curve Cryptography.

Lectured in three **advanced training schools for graduate sctudents** on: Elliptic Curves, Torus-based Cryptography, Gröbner bases.

Invited Conference Talks

"Computation with Gröbner bases over finite fields", First European Training School on Network Coding, Autonomous University of Barcelona (Spain), February 2013.

"Initial ideals and linkage", Commutative Algebra and related topics, University of Genova (Italy), June 2012.

"An optimal algebraic construction for random network coding", Solving polynomial equations, KTH Stockholm (Sweden), February 2011 (part of the Mittag-Leffler Institute's program on "Algebraic Geometry with a view towards applications").

"An optimal algebraic construction for random network coding", Women in Computer Algebra, Aachen (Germany), October 2010.

"An optimal algebraic construction for random network coding", XII Encuentro de Álgebra Computacional y Aplicaciones - EACA 2010, Santiago de Compostela (Spain), July 2010.

"Gröbner bases of linked ideals", School and Workshop on Local Rings and Local Study of Algebraic Varieties, The Abdul Salam International Center for Theoretical Physics (ICTP), Trento (Italy), June 2010.

"Liaison and Gröbner bases of pfaffian ideals", Incontro Nazionale di Algebra Moderna, INdAM - Italian National Institute for Higher Mathematics, Roma (Italy), May 2010.

"Liaison and Gröbner bases of pfaffian ideals", Midwest Algebra, Geometry and their Interactions Conference - MAGIC'10, University of Notre Dame, IN (USA), April 2010.

"Linkage of schemes defined by minors and pfaffians", Giornate di Geometria Algebrica ed Argomenti Correlati IX, Trento (Italy), May 2008.

"Linkage of schemes defined by minors and pfaffians", Genova-Barcelona Workshop on Commutative Algebra and Applications, University of Genoa (Italy), May 2008.

"Linkage of schemes defined by minors and pfaffians", Conferencia Internacional sobre Álgebra Conmutativa, Combinatoria y Computacional en Honor de Pilar Pisón Casares, University of Sevilla (Spain), February 2008.

"Algebraic geometric instances of the Discrete Logarithm Problem", Workshop on Projective Geometry and Commutative Algebra in Applications, University of Genova (Italy), June 2007.

"Computational challenges in torus-based cryptography", Workshop on Computational Challenges Arising in Algorithmic Number Theory and Cryptography (part of the Fields Institute Fall 2006 Thematic Program in Cryptography), Fields Institute, Toronto (Canada), November 2006.

"Algebraic tori in cryptography" (series of 3 lectures), 2006 summer school on "Computational Number Theory and Applications to Cryptography", University of Wyoming (Laramie), June-July 2006.

"Algebraic Geometry instances of the Discrete Logarithm Problem", Boole Workshop in Coding and Cryptography, Boole Centre for Research in Informatics, UCC, Cork (Ireland), May 2006.

"Rationality questions in cryptography", Incontro di Algebra Commutativa e Computazionale, Università di Genova (Italy), November 2005.

"G-biliaison of determinantal schemes", MAGIC 05 - Midwest Algebra, Geometry and their Interactions Conference, October 2005.

"Introduction to Elliptic Curves", 2004 IMA Summer Program for Graduate Students in Coding and Cryptography, Notre Dame, IN (USA), June 2004.

"The general plane section of a curve in $\mathbb{P}^3$", AMS 2004 Spring Eastern Section Meeting, Lawrenceville, NJ (USA), April 2004.

Contributed Conference Talks

"Cryptanalysis of the CFVZ cryptosystem", 10th Rhein Workshop on Computer Algebra, University of Basel (Switzerland), March 2006.

"Some algebraic properties of curves in $\mathbb{P}^3$ via their general plane section", Geométrié Algébrique En Liberté XII, Luminy (France), April 2004.

"The general plane section of a space curve", Route 81 Conference, Syracuse University, Syracuse, NY (USA), October 2003.

Other Invited Talks

"Glicci ideals", Mathematical Science Research Institute, Berkeley, CA (USA), November 2012.

"Trace zero cryptosystems", Academia Sinica, Taipei (Taiwan), June 2012.

"Ideals of minors and pfaffians: liaison and initial ideals", University and Technical University of Torino (Italy), June 2012.

"Cryptography: from theory to practice", Swiss Academy of Science, September 2011.

"Elliptic curve cryptography and its applications to secrecy in communications", Colloquium, University of Neuchatel (Switzerland), May 2011.

"Minors, theory and practice", Technical University of Munich (Germany), March 2011.

"Minors, theory and practice", University of Magdeburg (Germany), March 2011.

"An introduction to coding theory and cryptography", Mittag Leffler Institute, Stockholm (Sweden), February 2011.

"Gorenstein Liaison", University of Luxembourg (Luxembourg), January 2011.

"Codes on the Grassmannian, or how to correct errors in a network", Colloquium, University of Fribourg (Switzerland), November 2010.

"Gorenstein Liaison and determinantal schemes", University of Freiburg (Germany), January 2010.

"Linkage of schemes defined by minors and pfaffians", Purdue University, IN (USA), October 2009.

"Gorenstein Liaison and determinantal ideals", Colloquium, University of Notre Dame, IN (USA), October 2009.

"Linkage of schemes defined by minors and pfaffians", University of Milan (Italy), April 2009.

"Finite fields in cryptography", Goethe University Frankfurt am Main (Germany), February 2009.

"Gorenstein Liaison", Christian-Albrechts-Universität zu Kiel (Germany), January 2009.

"Finite fields in cryptography", Technische Universität München (Germany), November 2008.

"Gorenstein Liaison", Humboldt University of Berlin (Germany), November 2008.

"Gorenstein Liaison", University of Exeter (UK), April 2008.

"Finite fields in cryptography", RWTH Aachen (Germany), April 2008.

"Coding for Random Linear Networks", University of Zurich Symposium in Mathematics, Zurich (Switzerland), April 2008.

"Elliptic curves, pairings, and the Discrete Logarithm Problem", University of Basel (Switzerland), May 2007.

"Algebraic geometric instances of the Discrete Logarithm Problem", Center for Ring Theory and its Applications, Ohio University (Athens, OH), April 2007.

"What is elliptic curve cryptography?", Center for Ring Theory and its Applications, Ohio University (Athens, OH), April 2007.

Other Invited Talks continued

"Cryptography and mathematics: from Cesar's cypher to the internet", Colloquium for the Math Awareness Week, Center for Ring Theory and its Applications, Ohio University (Athens, OH), April 2007.

"Linkage and determinantal schemes", Universität Osnabrück (Germany), November 2006.

"Gorenstein Liaison", Symposium in Pure Mathematics, University of Zurich (Switzerland), June 2006.

"The Discrete Logarithm Problem for matrices over elliptic curves", Università di Genova (Italy), April 2006.

"What is... Elliptic Curve Cryptography?", Zurich Graduate Colloquium, ETH Zurich (Switzerland), November 2005.

"Pairings on elliptic curves", b-it Bonn-Aachen International Center for Information Technology, October 2005.

"Cryptographic applications of elliptic curves", Università di Pisa (Italy), May 2005.

"Cryptographic applications of elliptic curves", Università degli Studi di Genova (Italy), March 2005.

"The G-biliaison class of symmetric determinantal schemes" (series of 3 talks), University of Notre Dame (USA), February-March 2005.

"Public key cryptography: applications of mathematics to secrecy in communication", Fachschaftstag der kantonalen Fachschaft Mathematik der Gymnasien des Kantons Luzern, Universität Zürich (Switzerland), December 2004.

"Determinantal ideals", Università degli Studi di Genova (Italy), July 2004.

"When is a curve Cohen-Macaulay?", Purdue University, IN (USA), November 2003.

"The general section of a non Cohen-Macaulay curve", University of Missouri-Columbia, MU (USA), October 2003.

"Lifting the Cohen-Macaulay property", University of Kansas, Lawrence, KS (USA), October 2003.

"The minimal free resolutions of the general section of a curve", Università degli Studi di Genova (Italy), July 2003.

Popularization of Mathematics

Teacher (together with H. Kraft) of a weekend workshop on coding theory and cryptography for non-mathematicians, in March 2013. The workshop is organized by the Swiss Study Foundation (Sweizerische Studienstiftung).

Address during the closing ceremony of "girls@science" in Jan. 2012. This is a one week program organized jointly by Schweizer Jugend Forscht and the University of Basel, where girls aged 11-13 spend a week engaded in science projects at the University of Basel.

Radio interview on Radio LoRa, November 2011. I was invited to participate in the program "The Hard Drive - science geeks in Zurich", a popular-science radio show focused on the cosmopolitan scientific community of Zurich. Each episode features two guests discussing science with a moderator for one hour.

Address on "Cryptography: from theory to practice" at the Swiss Academy of Science, September 2011.

Radio interview on DRS, February 2011. I was asked for an expert opinion on a letter written in code by the musician Edward Elgar.

Speaker at "Women in Computer Algebra", Aachen (Germany), October 2010.

Instructor for the "Junior Euler Society" (mathematics program for gifted high school students at the University of Zurich) for the academic year 2008/09.

Participated in a project about "Mathematicians and their jobs", promoted by the Italian Ministry for University and Research (MIUR). My professional story was featured in the book "Mathematicians at work" (in Italian), Sironi Editore (2008) and appears on the website of the project `http://mestieri.dima.unige.it/`.

Workshop aimed at introducing high school students to mathematical thinking, September 2008, Realgymnasium Rämibühl Zürich (Switzerland).

Talk for general public on "Cryptography and mathematics: from Cesar's cypher to the internet" in the context of the "Math Awareness Week". The talk was held at the Center for Ring Theory and its Applications, Ohio University, Athens, OH (USA) in April 2007.

3-days workshop aimed at introducing high school students to research in mathematics, April 2006, University of Genova (Italy).

Talk aimed at high school teachers on "Public key cryptography: applications of mathematics to secrecy in communication" in the context of the "Fachschaftstag der kantonalen Fachschaft Mathematik der Gymnasien des Kantons Luzern". The talk was held at the University of Zurich (Switzerland) in December 2004.