

Curriculum Vitae of Ilia Toli

December 3, 2006

Personal Data

Birth Date : January 24, 1972.
Birthplace : Toshkëz, Lushnje, Albania.
Citizenship : Albanian.
Green Card in the USA.
ilia.toli@gmail.com
<http://www.dm.unipi.it/~toli> (rarely updated)

Studies

2001 to 2004. PhD in Mathematics. Università di Pisa, Italy.

Advisor : Professor Carlo Traverso.

Thesis title : On Some Algebraic Methods in Cryptography.

1990 to 1995. MSc in Mathematics. University of Tirana, Albania.

Advisor : Professor Thoma Mitre.

Thesis topics : Optimization problems from Graph Theory.

1986 to 1990. High school. Krutje, Lushnje, Albania. For the years 1988, 1989 and 1990 I was awarded the first prize in the semifinal round of the National Mathematical Contests. For the year 1988 I ranked 9th in the final round.

Research Interests

Cryptography and Cryptanalysis in all their aspects: mathematical, software, hardware, Public and Private Key; especially AES.

Computer Arithmetic, Commutative Computer Algebra.

Computer Skills

C++, GAP, Macaulay2, Maple, Mathematica, Singular.

Language Skills

Albanian, English, French and Italian: spoken, read, written fluently.
Russian and Spanish: scholastic knowledge.

Professional Experiences

October to December 2006. Postdoctoral researcher with a grant of ST Microelectronics. Eurécom, Sophia Antipolis, France.

August and September 2006. Invited researcher with a grant of ST Microelectronics. BCRI, UCC, Cork, Ireland.

May 2005 to April 2006. Postdoctoral researcher. LIP, École Normale Supérieure de Lyon, France.

June to September 2004. Visiting PhD student within the framework of GTEM (Galois Theory and Explicit Methods in Arithmetic) network. School of Mathematics, Tel Aviv University, Israel.

February to May 2004. Visiting PhD student in the framework of ACE (Algebraic Combinatorics in Europe) network. LaBRI, Université de Bordeaux I, France.

November and December 2003. Research grant. Dipartimento di Matematica "Leonida Tonelli", Università di Pisa, Italy.

May 2001 to April 2003. Research grant. Dipartimento di Matematica "Leonida Tonelli", Università di Pisa, Italy.

June to October 1995. Programmer. Zollet Service scarl. Santa Giustina, Belluno (BL), Italy. Albanian branch in Tirana.

Papers

1. Ilia Toli and Alberto Zanoni. Looking Inside AES and BES. In "Exploring New Frontiers of Theoretical Informatics". Proceedings of the 18-th

- IFIP World Computer Congress – TC1 3-rd International Conference on Theoretical Computer Science (TCS2004). August 22 – 27, 2004 Toulouse, France. Edited by J.-J. Levy, E. W. Mayr, J. C. Mitchell. Kluwer, USA 2004. Pages 23 – 36. ISBN: 1-4020-8140-5, ISBN: 1-4020-8140-3 (eBook). <http://www14.in.tum.de/konferenzen/WCC2004-TCS/papers/zanoni.pdf> and <http://wwwmayr.informatik.tu-muenchen.de/konferenzen/WCC2004-TCS/papers/zanoni.pdf>.
2. Ilia Toli and Alberto Zanoni. An Algebraic Interpretation of AES-128. In "Advanced Encryption Standard – AES: 4th International Conference, AES 2004", Bonn, Germany, May 10 – 12, 2004, Revised Selected and Invited Papers. Hans Dobbertin, Vincent Rijmen, Aleksandra Sowa editors. Lecture Notes in Computer Science 3373. ISSN 0302-9743. Pages 84 – 97. ISBN: 3-540-26557-0. DOI: 10.1007/b137765, http://dx.doi.org/10.1007/11506447_8.
 3. Ilia Toli and Alberto Zanoni. Algebraic Aspects of AES-128. Survey. Coding and Cryptography Days. Università di Milano Bicocca, Italy. In "Industry Days 2003 – 2004". The Miriam Project outline. Aquilano et al. editors. Esculapio publishing house, Bologna, Italy, 2005. Pages 66 – 71. ISBN: 88-7488-109-6.
 4. Ilia Toli. The Cryptanalytic Use of Gröbner Bases. Research report. Università di Pisa, Italy. December 2003.
 5. Ilia Toli. Hidden Polynomial Cryptosystems. Submitted to Journal of Algebra and Its Applications.
 6. Massimiliano Sala and Ilia Toli. A Representation Theory Approach to AES Cryptanalysis. Work in progress.
 7. Renaud Pacalet and Ilia Toli. Arithmetic Optimization of AES. Work in progress.

Posters

1. Ilia Toli. Efficient Arithmetic for Some Finite Fields. Special Semester on Groebner Bases and Their Application, Workshop D1. May 1 – 6 2006, Linz, Austria.
2. Ilia Toli and Alberto Zanoni. Algebraic Aspects of AES-128. Coding and Cryptography. Università di Milano Bicocca, Italy. December 1, 2003. Poster session.

3. Ilia Toli and William Sit. Hidden Algebraic Structure Cryptosystems. The Asian Symposium on Computer Mathematics ASCM 2003. Beijing, October 23 – 25, 2003. Poster Session.
4. Also in East Coast Computer Algebra Day, ECCAD 2003. Clemson University, South Carolina, USA. April 5, 2003. Poster Session.

Selected Talks

1. Efficient Arithmetic for Some Finite Fields. BCRI Workshop on Coding and Cryptography. May 21 and 22, 2006. UCC, Cork, Ireland.
2. Algebraic Aspects of the Advanced Encryption Standard. Bonn-Aachen International Center for Information Technology. 31 January 2006.
3. Keyspace Redundancies of the HFE and Implications on Its Implementation. Cryptographic Architectures Embedded in Reconfigurable Devices - CryptArchi 2005. Le Bessat, Saint-Etienne, France. June 9 – 11, 2005.
4. An Algebraic Interpretation of AES-128. Fourth Conference on the Advanced Encryption Standard (AES) "AES – State of the Crypto Analysis". Hilton Hotel, Bonn, Germany. May 10 – 12, 2004.
5. On Some Hybrid System Solving Techniques and Their Applications in Cryptography. Université de Bordeaux I, France, March 11, 2004.
6. The Polynomial Solving Problem in Cryptography. Workshop *Computing in Algebra and Geometry*. Universität Kaiserslautern, Germany. June 16 – 20, 2003.
7. Hidden Polynomial Cryptosystems. BCRI Workshop on Coding and Cryptography. May 29, 2003. UCC, Cork, Ireland.
8. I Crittosistemi HFE. Università di Pisa, Italy, May 2003.