# Emmanuela Orsini

**Address**: Via Silvestri 11, 56125 Pisa, Italy
**Phone**:(+39)3292064528
**Contact information**: Dipartimento di matematica "L. Tonelli" - Progetto POSSO
Università degli Studi di Pisa
Largo Bruno Pontecorvo, 5
56127, Pisa, Italy
+390502213283
**E-mail**: orsini@posso.dm.unipi.it

## Current position

**Post-doctoral fellowship** " Grobner Bases in Coding Theory and Cryptography "
Department of Mathematics "L. Tonelli", Pisa

## Degrees

*2005–2007* **PhD in Mathematics and Statistic for the Computational Sciences**
Dipartimento di Matematica "Federigo Enriques"
Università degli Studi di Milano
Thesis discussed on January 9th, 2008
PhD thesis title:*"On the decoding and distance problems for algebraic codes"*.
Supervisors: Prof. Teo Mora, Prof. M. Sala.

*2003–2004* **Master MAMI-SAMI in Applied Mathematics** (INdAM grant)
Dipartimento di Matematica e Applicazioni
Università di Milano Bicocca.
Thesis title:*"Metodi algebrici per la costruzione di matrici di parità per LDPCC"*.
Supervisors: Prof. M. Sala, University College Cork, and Ing. D. Gatti, STMicroelectronics.

*April 2003* **M.S., Mathematics**, Dipartimento di Matematica, Università di Pisa.
Thesis title: *"Basi di Gröbner e specializzazioni"*. Supervisor: Prof. Patrizia Gianni.

## Qualifications

*3/II/2010* Maître de conférences, Mathématiques, $N^o$ de qualification 10225201349

*21/I/2010* Maître de conférences, Informatique, $N^o$ de qualification 10227201349

(Qualified for the oral examination for the position 26/25 MCF, Université de Limoges, France (20/05/2010)).

## Past academic position

*March-October 2008* **Post-doctoral fellowship** "Grobner Bases in Coding Theory "
Department of Mathematics "L. Tonelli", Pisa

*2005–2007* **PhD student** (with an Italian government scholarship) in Mathematics and Statistic for the Computational Sciences, University of Milan

*January-February 2006* **Visiting student**, Boole Center for Research in Informatic, University College Cork, Ireland.

*2005–2007* **Master student**: (with an INdAM scholarship) master in Applications of Mathematics to Industry and Services (MAMI), University of Milan Bicocca

## Research interests

• **Algebra**: computational algebra, Gröbner bases, Gröbner bases with parameters
• **Cryptography**: public-key cryptosystems, lattice-based cryptosystems, Polly-Cracker systems, cryptographic perspective of lattice problems.
• **Coding theory**: cyclic codes, affine-variety codes, decoding algorithms, nonlinear codes, MDS, codes, LDPC codes, shape of general error locator polynomial, Goppa codes

## Talks

*July 2010* Symbolic Computation and its Applications, Maribor, Slovenia. (Invited Speaker).

*June 2010* SCC 2010, 2nd International Conference on Symbolic Computation and Cryptography, "Lattice Polly Cracker Signature" $23-25$ June 2010, Royal Holloway, University of London, UK.

*July 2008* S3CM, Soria Summer School on Computational Mathematics "Algebraic Coding Theory"(part of Fitzpatrickk-Martinez course): *On the structure of the syndrome variety*. (Invited Lecture).

*October 2007* University of Trento: *On the complexity of decoding cyclic codes*.(Invited talk).

*May 2006* SPECIAL SEMESTER ON GRÖBNER BASES (Linz): *Decoding cyclic codes: The Cooper philosophy*, Workshop D1.Gröbner bases in Cryptography, Coding Theory, and Algebraic Combinatorics. (Invited talk).

*May 2006* SPECIAL SEMESTER ON GRÖBNER BASES (Linz): *Introduction to cyclic codes*, Workshop D1.Gröbner bases in Cryptography, Coding Theory, and Algebraic Combinatorics.(Invited talk) .

*December 2005* Cork, Ireland: *On the sparsity of general error locator polynomial for some binary cyclic codes*, Dept. of Electrical and Electronic Engineering, UCC Cork.

*May/June 2005* MEGA 2005 (Alghero): *General error locator polynomial for binary cyclic code with* $t \leq 2$ *and* $n < 63$, (Short Talk).

*November 2003* Cork, Ireland: *New decoding algorithm for cyclic codes*, BCRI, UCC Cork.

## Schools, Conference and Workshop

*June 2010* SCC 2010, 2nd International Conference on Symbolic Compuation and Cryptography. Royal Hoolway, University of London, UK.

*29 May 2010* Lattice Crypto Day (LCD), Saturday May 29th, 2010 at ENS, Paris, France.

*26/28 May 2010* 13th International Conference on Practice and Theory in Public Key Cryptography 2010, May $26-28$, 2010, ENS Paris, France.

*2/12 July 2008* Soria Summer School on Computational Mathematics: "Algebraic Coding Theory", Soria, Spain.

*April 2007* Versailles (France), International Workshop on Coding and Cryptography, WCC'07, INRIA.

*18/22 June 2007* Summer School in Coding Theory, Sophus Lie Conference Center, Nordfjordeid, Norway.

*May 2005* CoCoA IX International School, Alghero, Italy.

## Teaching

- 2009/2010 **Arithmetic, additional classes**
  Duration: 20h.
  Department of Mathematics, University of Pisa.

- 2009/2010 **Arithmetic, Teaching assistant**
  Duration: 20h.
  Course taught by Prof. C. Traverso at the Dept. of Mathematics, University of Pisa.

  Course schedule: Properties of the integers: induction and recursion, division and divisibility, equivalence and remainders mod $m$, greatest common divisors, factorization into primes; Groups, subgroups, cyclic groups; Morphisms; Rings, morphisms of rings; Integral domain and Fields; Polynomials, the division property of polynomials; Ideals; Quotient rings; Isomorphism Theorem for rings; Principal ideal domains, prime and maximal ideals; Elements of field theory: extension fields, analysis of simple extension fields, finite fields as algebraic extensions, uniqueness and existence of finite fields.

- 2008/2009 **Linear Algebra and Geometry, Teaching assistant**
  Duration: 40h.
  Course taught by Prof. P. Conti at the Dept. of Mechanical Engineering , University of Pisa.

  Course schedule: Vector spaces:subspaces, bases, dimension theorem of vector spaces, examples of vector spaces. Linear equations and matrices: system of linear equations, gaussian elimination, matrix theory, matrix multiplication, matrix inversion, invertible matrix, transpose. Determinats. Linear trasformations: properties, matrices of linear trasformations, change of bases, dual spaces. Inner product spaces: dot products and inner products, the lengths and angles of vectors, Gram-Schmidt orthogonalization, projections. Diagonalization: eigenvalues and eigenvectors. Quadratic form. Analytic geometry: in the plane (circle, ellipse, hyperbola, parabola, classification), in the space (quadratic surface, classification). Affine transformations. Elements of projective geometry.

- 2008 **Coding theory, Teaching assistant**
  Duration: 20h.
  Course taught by Prof. C. Traverso at the Dept. of Mathematics, University of Pisa.

  Course schedule: communication channels, Maximum likelihood decoding, Hamming distance, Nearest minimum distance decoding, distance of a code. Finite fields: structure, polynomial rings, minimal polynomials. Linear codes: generator and parity-check matrix , encoding and decoding, cosets, syndrome decoding. Bounds: Sphere Packing Bound, covering radius, and perfect codes, Plotkin Upper Bound, Singleton Upper Bound and MDS codes, Elias Upper Bound, Griesmer Upper Bound, Gilbert Lower Bound, Varshamov Lower Bound. Cyclic codes: generator polynomial, decoding cyclic codes, BCH codes, decoding BCH codes. Reed-Solomon codes. Quadratic residue codes.

- 2007 **Coding theory, Teaching assistant**
  Duration: 20h.
  Course taught by Prof. C. Traverso at the Dept. of Mathematics, University of Pisa.

  Course schedule: communication channels, Maximum likelihood decoding, Hamming distance, Nearest minimum distance decoding, distance of a code. Finite fields: structure, polynomial rings, minimal polynomials. Linear codes: generator and parity-check matrix , encoding and decoding, cosets, syndrome decoding. Bounds: Sphere Packing Bound, covering radius, and perfect codes, Plotkin Upper Bound, Singleton Upper Bound and MDS codes, Elias Upper Bound, Griesmer Upper Bound, Gilbert Lower Bound, Varshamov Lower Bound. Cyclic codes: generator polynomial, decoding cyclic codes, BCH codes, decoding BCH codes. Reed-Solomon codes. Quadratic residue codes.

- 2006 **Coding theory and cryptography**
  Duration: 20h.
  Course taught by prof. Massimiliano Sala at the Dept. of Mathematics, University of Milano Bicocca.

  Course schedule: Information security and cryptography: basic terminology and concepts. Mathematical Background: complexity theory, number theory, finite fields, the integer factorization problem, the RSA problem, the quadratic residuosity problem, computing square roots in Zn, the discrete logarithm problem. factoring polynomials over finite fields. Block Ciphers: background and general concepts, DES. Public-Key Encryption: RSA public-key encryption. Coding theory: introduction, Hamming distance, Nearest minimum distance decoding, distance of a code, linear codes, generator and parity-check matrix , encoding and decoding, cosets, syndrome decoding.

# Publications

### PhD Thesis

- E. Orsini, On the decoding and distance problems for algebraic codes, PhD thesis, 156 pages, January 2008.

## Refereed Papers

- E. Orsini, "New decoding algorithm for cyclic codes", *Proceeding of Miriam Workshop*, Industrial Days 2003-2004, Milano, Volume 2, pp. 62-65, June 2005.
- E. Orsini, M. Sala, "Correcting errors and erasures via the syndrome variety", *J. Pure Appl. Algebra*, Volume **200**, 1-2, August 2005, pp. 191-226.
- E. Orsini, M. Sala "General error locator polynomials for binary cyclic code with $t \leq 2$ and $n < 63$", *IEEE Trans. on Information Theory*, Volume 53, No 3, March 2007, pp. 1095-1107.
- D. Augot, E. Betti, E. Orsini, "An introduction to linear and cyclic codes", *Gröbner , Coding and Cryptography*, Sala, M.; Mora, T.; Perret, L.; Sakata, S.; Traverso, C. (Eds.), RISC Book Series, Springer, Heidelberg 2009, pp. 47-68.
- Mora T., Orsini E., "Decoding cyclic codes: the Cooper philosophy" *Gröbner Bases, Coding, and Cryptography*, RISC *Groebner, Coding and Cryptography*, Sala, M.; Mora, T.; Perret, L.; Sakata, S.; Traverso, C. (Eds.), RISC Book Series, Springer, Heidelberg 2009, pp. 69-91.
- E. Guerrini, E. Orsini, I. Simonetti, "An algorithm for the distance distribution of systematic nonlinear codes", *Gröbner Bases, Coding, and Cryptography*, Sala, M.; Mora, T.; Perret, L.; Sakata, S.; Traverso, C. (Eds.), RISC Book Series, Springer, Heidelberg 2009, pp. 367-372.
- E. Guerrini, E. Orsini, M. Sala, "Computing the distance of some non–linear codes", accepted for publications to *Journal of Algebra and Its Applications*, Volume 9, No. 1 (2010), 1-16 (DOI No: 10.1142/S0219498810003884).
- E. Orsini, M. Sala, "Improved decoding of affine–variety codes", accepted *J. of Pure and Applied Algebra*, (preprint at Boole Centre for Research in Informatics, Cork, Ireland, http://www.bcri.ucc.ie/BCRI_68.pdf).

## Other papers

- T. Mora, E. Orsini, Invited Talk: "Decoding Cyclic Codes", *MMICS*, 2008, pp. 126-127, http://dx.doi.org/10.1007/978-3-540-89994-5_10.

## Work in progress

- E. Orsini, C. Traverso, "The LPC signature" (extended abstract accepted at SCC 2010, 23 – 25 June 2010, Royal Holloway, University of London, UK).
- E. Orsini, "Syndrome decoding of the $(41,21,9)$ Quadratic Residue Code".
- F. Caruso, E. Orsini, M. Sala, "On the shape of the general error locator polynomial".

**Professional experience**

*May-November 2005* **Internship at STMicroelectronics**, Agrate Brianza, Milano.
The goal of the research has been the study of parity check matrices for low density parity check codes (LDPC) and the construction of an encoder/decoder for the same codes (C language and Matlab).

**Other activities**

Review activities for IEEE Communication Letters, IEEE Trans. on Information Theory, INS Information Science.

**Other skills**

**Languages**
Italian: mother tongue
English: good level, both written and spoken (*Cambridge FCE*, June 2002)

**Computer skills**
Operative system: Linux, MS Windows
Programming languages: C, C++, PHP5, HTML, XHTML, Fortran,
Computer Algebra System: Singular, CoCoA, Magma, Maple
Professional typing/publication software: LaTex, Publisher, Acrobat, MS Office

**Scientific activities**

The principal research activities lie in the general areas of Cryptography, Algebraic Coding Theory and Computational Algebra.

# 1 Cryptography

Lattice-based cryptosystems hold a great promise for post-quantum cryptography, as they enjoy very strong security proofs and relatively efficient implementations. There now exist public-key cryptosystem based on the hardness of lattice problems and moreover lattices play a crucial rôle in several attacks against various cryptographic schemes.

## 1.1 The NTWO cryptosystem and heterogeneous lattice metrics

We are currently working on the study of a new cryptosystem, called NTWO. This cryptosystem, from the public point of view, looks like NTRU, (except the non secondary detail that multivariate polynomial algebra is used, instead of univariate algebra), but is different in key creation and decryption. As a consequence, while the message attacks are shared with NTRU, the key attacks are different; it is still possible to define a lattice like the Coppersmith-Shamir lattice, and breaking the private key via a SVP (shortest vector problem) in this lattice, but the metric on this lattice is heterogeneous: in some components the distance is Euclidean, in some other components the distance is Hamming. We study the SVP in this metric, and reduce the approximate solution of this problem to the approximate solution of the same problem in a larger lattice.

## 1.2 Lattice Polly Cracker signature

Using Gröbner bases for the construction of public key cryptosystem has been often attempted, but always failed. LPC (Lattice Polly Cracker cryptosystem) ([1]) is a public key cryptosystem that uses Gröbner bases of lattices for the preparation of the public key and normal form for decryption. However its security is not relied on the difficulty of computing Gröbner bases, but the trapdoor information is a change of variables that trasforms the private lattice (a block lattice with a “fat” staircase) into the public lattice. We study the security of this scheme and we show that security considerations force the adoption of a very tight form of block lattice. In [9] we give further analysis linking normal form with respect to a suitable Gröbner basis to approximate CVP (Closest

Vector Problem). This analysis allows to give a test to estimate the security of an instance of LPC. We define moreover a signature protocol using LPC. This scheme uses a protocol similar to other lattice signature protocols, the signer being identified by her ability to solve an approximate CVP challange.

# 2 Coding theory

We apply symbolic methods to the problem of decoding linear code and of distance computing for systematic nonlinear codes. The paradigm we employ is as follows: we reformulate the initial problem in terms of system of polynomial equations over a finite field in such a way the solution(s) of such systems should yield a way to solve the initial problem. Our main tools for handling polynomials and polynomial systems is the technique of Gröbner bases.

## 2.1 Nonlinear codes

The most basic aim of codes is to correct errors on noisy communication and for this purpose linear codes have many practical advantages, but if we want to obtain a code with the largest possible number of codewords with a given distance, we must sometimes use nonlinear codes.For implementation issues, the only non-linear codes that makes sense to study are systematic.

We have succeeded in building a variety whose points are in bijections with systematic nonlinear codes having specific parameters. In this way, we provides ([4]) a Gröbner basis technique to compute the distance and the distance distribution of any systematic nonlinear code. We investigate these codes from an algebraic point a view, in particular we see codes as algebraic varieties and we examine the Gröbner bases of their vanishing ideal.
The proposed algorithm depends on some relations between the relevant Gröbner basis and the distance. We remark that to compute the distance of nonlinear codes no other method is known except for the brute force approach consisting of checking the mutual distance of any pair of codewords.

## 2.2 Decoding algorithms

The idea in polynomial system solving methods for decoding codes is to associate to the code (and to the received vector) certain polynomial system over a finite field. The solution(s) of such a system should yield the corresponding error vector(s) in more or less straighforward way.

### 2.2.1 Cyclic codes

The syndrome variety has been used by several authors to decode cyclic codes and derive information on their distance and weight distribution. The relevant algebraic computations are carried with Groebner basis techniques. However, the presence of spurious solutions make the use of the syndrome variety rather cumbersome and inefficient. Actually, one has to look through the entire reduced Gröbner bases associated to the syndrome variety, which usually is quite complicated, in order to extract elements needed for decoding. We develop a variation of the syndrome variety that allows efficient decoding using a new concept: “general error locator polynomials”. We prove the following result ([6]):

*Every cyclic code C possesses a general error locator polynomial (gelp). This means that there exists a unique polynomial $L_C$ from $F_q[X_1,\ldots,X_{n-k},Z]$ that satisfies the two properties:*

- $L_C = Z^t + a_{t-1}Z^{t-1} + \ldots + a_0$ *with* $a_j \in F_q[X_1,\ldots,X_{n-k}]$, $0 \leq j \leq t-1$
- *given a syndrome* $\mathbf{s} = (s_1,\ldots,s_{n-k}) \in F^{n-k}$ *corresponding to an error of weight* $\mu \leq t$ *and error locations* $\{k_1,\ldots,k_\mu\}$*, if we evaluate the X-variables, then the roots of* $L_C(\mathbf{s},Z)$ *are*

*exactly* $a^{k_1}, \ldots, a^{k_\mu}$ *and zero of multiplicity* $t-\mu$*, in other words*

$$L_C(\mathbf{s}, Z) = z^{t-\mu} \prod_{i=1}^{t} (z - a^{k_1}).$$

We prove similar results for the case of simultaneous correction of errors and erasures.

Such an error–locator polynomial actually is an element of the reduced Gröbner basis associated to the syndrome variety. Having this polynomial, decoding of the cyclic code $C$ reduces to univariate factorization. The main effort is finding the reduced Gröbner basis, especially for large size codes. We prove ([7]) that the our decoding algorithm may be efficiently applied to all binary cyclic codes with length less than 63 and correction capability $t \leq 2$. In all these cases we provide a sparse representation of the general error locator polynomial, suggesting that any decoding procedure for cyclic codes based on this polynomial might be efficient.
In [2] we are generalizing our structural theorems on the general error locator polynomials, starting from results by Chang and Lee ([3]).

### 2.2.2 Affine–variety codes

Affine–variety codes provide a way to represent any linear code as an evaluation code for a suitable polynomial ideal. This rather general description does not provide immediately efficient decoding algorithms.
By changing the ideal for the decoding previously suggested by Fitzgerald and Lax, we prove the existence of "multidimensional general error locator" polynomials for affine-variety codes. Multidimensional error locator polynomials are the multidimensional analogue of general error locator polynomials introduced for cyclic codes. Once the syndromes are received they permit direct computations of the error locations by simply evaluating some polynomials. We investigate some interesting cases, including Hermitian codes.

### 2.2.3 LDPC codes

Low-Density Parity-Check codes have emerged recently, due to their sub-optimal decoding performance. However, they lack an algebraic structure, making their theoretical study difficult. What is difficult is to find explicitely families which are easy to encode and whose Tanner graph has a high girth. Many such families have been proposed, but usually with a not-so-high girth.
We study algebraic properties and decoding performance of LDPC-Goppa codes. This work has been done in collaboration with STMicroelectronics.

## 3 Computational Algebra

Gröbner bases are the computational method par excellence for studying polynomial systems. In the case of parametric polynomial systems one has to determine the reduced Gröbner basis in dependence of the values of the parameters.
The work done for my master at Pisa University, under the supervision of Prof. Patrizia Gianni, was devoted on the study of the proprerties of Gröbner bases under specializzation. We have focused first on the study of comprehensive Gröbner basis and then on sufficient conditions to garantee that the leading term ideal commutes with the specialization, i.e., given an ideal $I \subseteq R[X]$ and $\phi : R \longrightarrow R$ a ring omomorphism, $(\mathrm{LT}\phi(I)) = LT\phi((I))$. We also investigated what information remains in a Gröbner basis under specialization, even if the leading term ideal is not preserved.

## References

[1] M. Caboara, F. Caruso, C. Traverso "Lattice Polly Cracker cryptosystem", to appear in J. Symb. Comp. 2010. 1.2

[2] F. Caruso, E. Orsini, M. Sala, “On the shape of the general error locator polynomial”, work in progress. 2.2.1

[3] Y. Chang; C. Lee, “Algebraic Decoding of a Class of Binary Cyclic Codes Via Lagrange Interpolation Formula”, Information Theory, IEEE Transactions on Volume: 56 , Issue: 1 , Page(s): 130 - 139, 2010. 2.2.1

[4] E. Guerrini, E. Orsini, M. Sala, “Computing the distance of some non–linear codes”, accepted for publications to Journal of Algebra and Its Applications, Volume 9, No. 1 (2010), 1-16 (DOI No: 10.1142/S0219498810003884). 2.1

[5] Mora T., Orsini E., Decoding cyclic codes: the Cooper philosophy. In *Gröbner Bases, Coding, and Cryptography*, RISC book series, Springer, Heidelberg, (2009).

[6] E. Orsini, M. Sala, Correcting errors and erasures via the syndrome variety, *J. Pure Appl. Algebra*, **200** (2005), 191–226. 2.2.1

[7] E. Orsini, M. Sala “General error locator polynomials for binary cyclic code with $t \leq 2$ and $n < 63$”, *IEEE Trans. on Information Theory*, 53, 2007, pp. 1095-1107. 2.2.1

[8] E. Orsini, M. Sala, “Improved decoding of affine–variety codes”, submitted J. of Pure and Applied Algebra.

[9] E. Orsini, C. Traverso, “The LPC signature” (extended abstract submitted to SCC 2010, 23 – 25 June 2010, Royal Holloway, University of London, UK. 1.2