IN PARTNERSHIP WITH:
CNRS

Université Pierre et Marie Curie (Paris 6)

Activity Report 2013

Project-Team POLSYS

Polynomial Systems

IN COLLABORATION WITH: Laboratoire d'informatique de Paris 6 (LIP6)

RESEARCH CENTER
Paris - Rocquencourt

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Project-Team POLSYS

Keywords: Computer Algebra, Cryptography, Algorithmic Geometry, Algorithmic Number Theory, Complexity

Creation of the Team: 2012 January 01*, updated into Project-Team:* 2013 January 01.

1. Members

Research Scientists

Jean-Charles Faugère [Team leader, Inria, Senior Researcher, HdR]
Elias Tsigaridas [Inria, Researcher]
Dongming Wang [CNRS, Senior Researcher, HdR]

Faculty Members

Jérémy Berthomieu [Univ. Paris VI, Associate Professor]
Antoine Joux [Univ. Paris VI, Chaire de Crypto de la Fondation Partenariale de l'UPMC, HdR]
Daniel Lazard [Univ. Paris VI, Professor Emeritus, HdR]
Ludovic Perret [Univ. Paris VI, Associate Professor]
Guénaël Renault [Univ. Paris VI, Associate Professor]
Mohab Safey El Din [Univ. Paris VI, Professor, HdR]

PhD Students

Aurélien Greuet [Univ. Versailles]
Louise Huot [Univ. Paris VI]
Simone Naldi [LAAS/CNRS, Toulouse, granted by ANR GEOLMI project]
Cecile Pierrot [Univ. Paris VI]
Frederic Urvoy de Portzamparc [Inria, granted by Gemalto]
Ulrick Severin [Univ. Paris VI]
Jules Svartz [Univ. Paris VI]
Thibaut Verron [Univ. Paris VI]
Alexandre Wallet [Inria, granted by ANR EXACTA project, from Oct 2013]
Rina Zeitoun [Univ. Paris VI and Oberthur]

Post-Doctoral Fellow

Christian Eder [Inria, granted by ANR EXACTA project, from Feb 2013]

Visiting Scientist

Chee Yap [Invited Professor, Jun 2013 until Jul 2013]

Administrative Assistants

Virginie Collette [Inria]
Emmanuelle Grousset [Inria]
Nelly Maloisel [Inria]

2. Overall Objectives

2.1. Introduction

The main focus of the POLSYS project is to solve systems of polynomial equations.

Our main objectives are:

- **Fundamental Algorithms and Structured Systems.** The objective is to propose fast exponential exact algorithms to solve the problem of solving polynomial equations and to identify large classes of structured polynomial systems which can be solved in polynomial time.
- **Solving Systems over the Reals and Applications.** For positive dimensional systems basic questions over the reals may be very difficult (for instance testing the existence of solutions) but also very useful in applications (e.g. global optimization problems). We plan to propose efficient algorithms and implementations to address the most important issues: computing sample points in the real solution sets, decide if two such sample points can be path-connected and, as a long term objective, perform quantifier elimination over the reals (computing a quantifier-free formula which is equivalent to a given quantified boolean formula of polynomial equations/inequalities).
- **Dedicated Algebraic Computation and Linear Algebra.** While linear algebra is a key step in the computation of Gröbner bases, the matrices generated by the algorithms F_4/F_5 have specific structures (quasi block triangular).The objective is to develop a dedicated efficient multi-core linear algebra package as the basis of a future open source library for computing Gröbner bases.
- **Solving Systems in Finite Fields, Applications in Cryptology and Algebraic Number Theory.** We propose to develop a systematic use of *structured systems* in Algebraic Cryptanalysis. We want to improve the efficiency and to predict the theoretical complexity of such attacks. We plan to demonstrate the power of algebraic techniques in new areas of cryptography such as Algebraic Number Theory (typically, in curve based cryptography).

2.2. Highlights of the Year

- Mohab Safey El Din was invited speaker in the International Symposium on Symbolic and Algebraic Computation (ISSAC), held in Boston, June 26-29, 2013.
- In [6] we investigate the security of HFE and Multi-HFE schemes. Our attacks are based on solving the MinRank problem. We prove that they are polynomial in the degree of the extension field for all possible practical settings used in HFE and Multi-HFE.
- In [11] we consider an algorithm to solve the DLP problem on Edwards curves, which are a well-known family of elliptic curves. We exploit the symmetries and the structure of twisted Edwards and twisted Jacobi intersections curves to gain an exponential factor $2^{\omega(n-1)}$ in the complexity bound where ω is the exponent of matrix multiplication.
- In [17] we give an explicit upper bound for the algebraic degree and an explicit lower bound for the absolute value of the minimum of a polynomial function on a compact connected component of a basic closed semialgebraic set when this minimum is not zero and is attained.

3. Research Program

3.1. Introduction

Polynomial system solving is a fundamental problem in Computer Algebra with many applications in cryptography, robotics, biology, error correcting codes, signal theory, ... Among all available methods for solving polynomial systems, computation of Gröbner bases remains one of the most powerful and versatile method since it can be applied in the continuous case (rational coefficients) as well as in the discrete case (finite fields). Gröbner bases is also a building blocks for higher level algorithms who compute real sample points in the solution set of polynomial systems, decide connectivity queries and quantifier elimination over the reals. The major challenge facing the designer or the user of such algorithms is the intrinsic exponential behaviour of the complexity for computing Gröbner bases. The current proposal is an attempt to tackle these issues in a number of different ways: improve the efficiency of the fundamental algorithms (even when the complexity is exponential), develop high performance implementation exploiting parallel computers, and investigate new classes of structured algebraic problems where the complexity drops to polynomial time.

3.2. Fundamental Algorithms and Structured Systems

Participants: Jean-Charles Faugère, Mohab Safey El Din, Elias Tsigaridas, Guénaël Renault, Dongming Wang, Jérémy Berthomieu, Pierre-Jean Spaenlehauer, Chenqi Mou, Jules Svartz, Louise Huot, Thibault Verron.

Efficient algorithms F_4/F_5 [1] for computing the Gröbner basis of a polynomial system rely heavily on a connection with linear algebra. Indeed, these algorithms reduce the Gröbner basis computation to a sequence of Gaussian eliminations on several submatrices of the so-called Macaulay matrix in some degree. Thus, we expect to improve the existing algorithms by
(i) developing dedicated linear algebra routines performing the Gaussian elimination steps: this is precisely the objective 2 described below;
(ii) generating smaller or simpler matrices to which we will apply Gaussian elimination.
We describe here our goals for the latter problem. First, we focus on algorithms for computing a Gröbner basis of *general polynomial systems*. Next, we present our goals on the development of dedicated algorithms for computing Gröbner bases of *structured polynomial systems* which arise in various applications.

Algorithms for general systems. Several degrees of freedom are available to the designer of a Gröbner basis algorithm to generate the matrices occurring during the computation. For instance, it would be desirable to obtain matrices which would be almost triangular or very sparse. Such a goal can be achieved by considering various interpretations of the F_5 algorithm with respect to different monomial orderings. To address this problem, the tight complexity results obtained for F_5 will be used to help in the design of such a general algorithm. To illustrate this point, consider the important problem of solving boolean polynomial systems; it might be interesting to preserve the sparsity of the original equations and, at the same time, using the fact that overdetermined systems are much easier to solve.

Algorithms dedicated to *structured* polynomial systems. A complementary approach is to exploit the structure of the input polynomials to design specific algorithms. Very often, problems coming from applications are not random but are highly structured. The specific nature of these systems may vary a lot: some polynomial systems can be sparse (when the number of terms in each equation is low), overdetermined (the number of the equations is larger than the number of variables), invariants by the action of some finite groups, multi-linear (each equation is linear w.r.t. to one block of variables) or more generally multihomogeneous. In each case, the ultimate goal is to identify large classes of problems whose theoretical/practical complexity drops and to propose in each case dedicated algorithms.

3.3. Solving Systems over the Reals and Applications.

Participants: Mohab Safey El Din, Daniel Lazard, Elias Tsigaridas, Pierre-Jean Spaenlehauer, Aurélien Greuet, Simone Naldi.

We will develop algorithms for solving polynomial systems over complex/real numbers. Again, the goal is to extend significantly the range of reachable applications using algebraic techniques based on Gröbner bases and dedicated linear algebra routines. Targeted application domains are global optimization problems, stability of dynamical systems (e.g. arising in biology or in control theory) and theorem proving in computational geometry.

The following functionalities shall be requested by the end-users:
(i) deciding the emptiness of the real solution set of systems of polynomial equations and inequalities,
(ii) quantifier elimination over the reals or complex numbers,
(iii) answering connectivity queries for such real solution sets.
We will focus on these functionalities.

[1] J.-C. Faugère. *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5).* In Proceedings of ISSAC '02, pages 75-83, New York, NY, USA, 2002. ACM.

We will develop algorithms based on the so-called critical point method to tackle systems of equations and inequalities (problem *(i)*) . These techniques are based on solving 0-dimensional polynomial systems encoding "critical points" which are defined by the vanishing of minors of jacobian matrices (with polynomial entries). Since these systems are highly structured, the expected results of Objective 1 and 2 may allow us to obtain dramatic improvements in the computation of Gröbner bases of such polynomial systems. This will be the foundation of practically fast implementations (based on singly exponential algorithms) outperforming the current ones based on the historical Cylindrical Algebraic Decomposition (CAD) algorithm (whose complexity is doubly exponential in the number of variables). We will also develop algorithms and implementations that allow us to analyze, at least locally, the topology of solution sets in some specific situations. A long-term goal is obviously to obtain an analysis of the global topology.

3.4. Low level implementation and Dedicated Algebraic Computation and Linear Algebra.

Participants: Jean-Charles Faugère, Christian Eder, Elias Tsigaridas, F. Martani.

Here, the primary objective is to focus on *dedicated* algorithms and software for the linear algebra steps in Gröbner bases computations and for problems arising in Number Theory. As explained above, linear algebra is a key step in the process of computing efficiently Gröbner bases. It is then natural to develop specific linear algebra algorithms and implementations to further strengthen the existing software. Conversely, Gröbner bases computation is often a key ingredient in higher level algorithms from Algebraic Number Theory. In theses cases, the algebraic problems are very particular and specific. Hence dedicated Gröbner bases algorithms and implementations would provide a better efficiency.

Dedicated linear algebra tools.FGB is an efficient library for Gröbner bases computations which can be used, for instance, via MAPLE. However, the library is sequential. A goal of the project is to extend its efficiency to new trend parallel architectures such as clusters of multi-processor systems in order to tackle a broader class of problems for several applications. Consequently, our first aim is to provide a durable, long term software solution, which will be the successor of the existing FGB library. To achieve this goal, we will first develop a high performance linear algebra package (under the LGPL license). This could be organized in the form of a collaborative project between the members of the team. The objective is not to develop a general library similar to the LINBOX project but to propose a dedicated linear algebra package taking into account the specific properties of the matrices generated by the Gröbner bases algorithms. Indeed these matrices are sparse (the actual sparsity depends strongly on the application), almost block triangular and not necessarily of full rank. Moreover, most of the pivots are known at the beginning of the computation. In practice, such matrices are huge (more than 10^6 columns) but taking into account their shape may allow us to speed up the computations by one or several orders of magnitude. A variant of a Gaussian elimination algorithm together with a corresponding C implementation has been presented. The main peculiarity is the order in which the operations are performed. This will be the kernel of the new linear library that will be developed.

Fast linear algebra packages would also benefit to the transformation of a Gröbner basis of a zero–dimensional ideal with respect to a given monomial ordering into a Gröbner basis with respect to another ordering. In the generic case at least, the change of ordering is equivalent to the computation of the minimal polynomial of a so-called multiplication matrix. By taking into account the sparsity of this matrix, the computation of the Gröbner basis can be done more efficiently using variant of the Wiedemann algorithm. Hence, our goal is also to obtain a dedicated high performance library for transforming (i.e. change ordering) Gröbner bases.

Dedicated algebraic tools for Algebraic Number Theory. Recent results in Algebraic Number Theory tend to show that the computation of Gröbner bases is a key step toward the resolution of difficult problems in this domain [2]. Using existing resolution methods is simply not enough to solve relevant problems. The main algorithmic lock to overcome is to adapt the Gröbner basis computation step to the specific problems. Typically, problems coming from Algebraic Number Theory usually have a lot of symmetries or the input

[2] P. Gaudry, *Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem*, Journal of Symbolic Computation 44,12 (2009) pp. 1690-1702

systems are very structured. This is the case in particular for problems coming from the algorithmic theory of Abelian varieties over finite fields [3] where the objects are represented by polynomial system and are endowed with intrinsic group actions. The main goal here is to provide dedicated algebraic resolution algorithms and implementations for solving such problems. We do not restrict our focus on problems in positive characteristic. For instance, tower of algebraic fields can be viewed as triangular sets; more generally, related problems (e.g. effective Galois theory) which can be represented by polynomial systems will receive our attention. This is motivated by the fact that, for example, computing small integer solutions of Diophantine polynomial systems in connection with Coppersmith's method would also gain in efficiency by using a dedicated Gröbner bases computations step.

3.5. Solving Systems in Finite Fields, Applications in Cryptology and Algebraic Number Theory.

Participants: Jean-Charles Faugère, Ludovic Perret, Guénaël Renault, Louise Huot, Frédéric de Portzamparc, Rina Zeitoun.

Here, we focus on solving polynomial systems over finite fields (i.e. the discrete case) and the corresponding applications (Cryptology, Error Correcting Codes, ...). Obviously this objective can be seen as an application of the results of the two previous objectives. However, we would like to emphasize that it is also the source of new theoretical problems and practical challenges. We propose to develop a systematic use of *structured systems* in *algebraic cryptanalysis*.
(i) So far, breaking a cryptosystem using algebraic techniques could be summarized as modeling the problem by algebraic equations and then computing a, usually, time consuming Gröbner basis. A new trend in this field is to require a theoretical complexity analysis. This is needed to explain the behavior of the attack but also to help the designers of new cryptosystems to propose actual secure parameters.
(ii) To assess the security of several cryptosystems in symmetric cryptography (block ciphers, hash functions, ...), a major difficulty is the size of the systems involved for this type of attack. More specifically, the bottleneck is the size of the linear algebra problems generated during a Gröbner basis computation.

We propose to develop a systematic use of *structured systems* in *algebraic cryptanalysis*.

The first objective is to build on the recent breakthrough in attacking McEliece's cryptosystem: it is the first structural weakness observed on one of the oldest public key cryptosystem. We plan to develop a well founded framework for assessing the security of public key cryptosystems based on coding theory from the algebraic cryptanalysis point of view. The answer to this issue is strongly related to the complexity of solving bihomogeneous systems (of bidegree $(1, d)$). We also plan to use the recently gained understanding on the complexity of structured systems in other areas of cryptography. For instance, the MinRank problem – which can be modeled as an overdetermined system of bilinear equations – is at the heart of the structural attack proposed by Kipnis and Shamir against HFE (one of the most well known multivariate public cryptosystem). The same family of structured systems arises in the algebraic cryptanalysis of the Discrete Logarithmic Problem (DLP) over curves (defined over some finite fields). More precisely, some bilinear systems appear in the polynomial modeling the points decomposition problem. Moreover, in this context, a natural group action can also be used during the resolution of the considered polynomial system.

Dedicated tools for linear algebra problems generated during the Gröbner basis computation will be used in algebraic cryptanalysis. The promise of considerable algebraic computing power beyond the capability of any standard computer algebra system will enable us to attack various cryptosystems or at least to propose accurate secure parameters for several important cryptosystems. Dedicated linear tools are thus needed to tackle these problems. From a theoretical perspective, we plan to further improve the theoretical complexity of the hybrid method and to investigate the problem of solving polynomial systems with noise, i.e. some equations of the system are incorrect. The hybrid method is a specific method for solving polynomial systems over finite fields. The idea is to mix exhaustive search and Gröbner basis computation to take advantage of the over-determinacy of the resulting systems.

[3] e.g. point counting, discrete logarithm, isogeny.

Polynomial system with noise is currently emerging as a problem of major interest in cryptography. This problem is a key to further develop new applications of algebraic techniques; typically in side-channel and statistical attacks. We also emphasize that recently a connection has been established between several classical lattice problems (such as the Shortest Vector Problem), polynomial system solving and polynomial systems with noise. The main issue is that there is no sound algorithmic and theoretical framework for solving polynomial systems with noise. The development of such framework is a long-term objective.

4. Application Domains

4.1. Cryptology

We propose to develop a systematic use of structured systems in Algebraic Cryptanalysis. We want to improve the efficiency and to predict the theoretical complexity of such attacks. We plan to demonstrate the power of algebraic techniques in new areas of cryptography such as Algebraic Number Theory (typically, in curve based cryptography).

4.2. Engineering sciences

Solving polynomial systems over the reals arise as a critical issue in wide range of problems coming from engineering sciences (biology, physics, control theory, etc.). We will focus on developing general enough software that may impact on these domains with a particular focus on control theory

5. Software and Platforms

5.1. FGb

Participant: Jean-Charles Faugère [contact].

FGb is a powerful software for computing Groebner bases.It includes the new generation of algorihms for computing Gröbner bases polynomial systems (mainly the F4, F5 and FGLM algorithms). It is implemented in C/C++ (approximately 250000 lines), standalone servers are available on demand. Since 2006, FGb is dynamically linked with Maple software (version 11 and higher) and is part of the official distribution of this software.
See also the web page http://www-polsys.lip6.fr/~jcf/Software/FGb/index.html.

- ACM: I.1.2 Algebraic algorithms
- Programming language: C/C++

5.2. RAGlib

Participant: Mohab Safey El Din [contact].

RAGLib is a Maple library for solving over the reals polynomial systems and computing sample points in semi-algebraic sets.

5.3. Epsilon

Participant: Dongming Wang [contact].

Epsilon is a library of functions implemented in Maple and Java for polynomial elimination and decomposition with (geometric) applications.

6. New Results

6.1. Fundamental Algorithms and Structured Systems

6.1.1. Structured polynomial systems: the quasi-homogeneous case

Let $\mathbb{K}$ be a field and $(f_1, ..., f_n) \subset \mathbb{K}[X_1, ..., X_n]$ be a sequence of quasi-homogeneous polynomials of respective weighted degrees $(d_1, ..., d_n)$ w.r.t a system of weights $(w_1, \cdots, w_n)$. Such systems are likely to arise from a lot of applications, including physics or cryptography. In [29], we design strategies for computing Gröbner bases for quasi-homogeneous systems by adapting existing algorithms for homogeneous systems to the quasi-homogeneous case. Overall, under genericity assumptions, we show that for a generic zero-dimensional quasi-homogeneous system, the complexity of the full strategy is polynomial in the weighted Bézout bound $\prod_{i=1}^{n} d_i / \prod_{i=1}^{n} w_i$. We provide some experimental results based on generic systems as well as systems arising from a cryptography problem. They show that taking advantage of the quasi-homogeneous structure of the systems allow us to solve systems that were out of reach otherwise.

6.1.2. Structured polynomial systems: the determinantal case

In [13], We study the complexity of solving the *generalized MinRank problem*, i.e. computing the set of points where the evaluation of a polynomial matrix has rank at most r. A natural algebraic representation of this problem gives rise to a *determinantal ideal*: the ideal generated by all minors of size $r + 1$ of the matrix. We give new complexity bounds for solving this problem using Gröbner bases algorithms under genericity assumptions on the input matrix. In particular, these complexity bounds allow us to identify families of generalized MinRank problems for which the arithmetic complexity of the solving process is polynomial in the number of solutions. We also provide an algorithm to compute a rational parametrization of the variety of a 0-dimensional and radical system of bi-degree $(D, 1)$. We show that its complexity can be bounded by using the complexity bounds for the generalized MinRank problem.

6.1.3. On the Complexity of the Generalized MinRank Problem

In [13] we study the complexity of solving the *generalized MinRank problem*, i.e. computing the set of points where the evaluation of a polynomial matrix has rank at most r. A natural algebraic representation of this problem gives rise to a *determinantal ideal*: the ideal generated by all minors of size $r + 1$ of the matrix. We give new complexity bounds for solving this problem using Gröbner bases algorithms under genericity assumptions on the input matrix. In particular, these complexity bounds allow us to identify families of generalized MinRank problems for which the arithmetic complexity of the solving process is polynomial in the number of solutions. We also provide an algorithm to compute a rational parametrization of the variety of a 0-dimensional and radical system of bi-degree $(D, 1)$. We show that its complexity can be bounded by using the complexity bounds for the generalized MinRank problem.

6.1.4. On the Complexity of Computing Gröbner Bases for Quasi-homogeneous Systems

Let $\mathbb{K}$ be a field and $(f_1, ..., f_n) \subset \mathbb{K}[X_1, ..., X_n]$ be a sequence of quasi-homogeneous polynomials of respective weighted degrees $(d_1, ..., d_n)$ w.r.t a system of weights $(w_1, \cdots, w_n)$. Such systems are likely to arise from a lot of applications, including physics or cryptography.

In [29], we design strategies for computing Gröbner bases for quasi-homogeneous systems by adapting existing algorithms for homogeneous systems to the quasi-homogeneous case. Overall, under genericity assumptions, we show that for a generic zero-dimensional quasi-homogeneous system, the complexity of the full strategy is polynomial in the weighted Bézout bound $\prod_{i=1}^{n} d_i / \prod_{i=1}^{n} w_i$.

We provide some experimental results based on generic systems as well as systems arising from a cryptography problem. They show that taking advantage of the quasi-homogeneous structure of the systems allow us to solve systems that were out of reach otherwise.

6.1.5. Gröbner bases of ideals invariant under a commutative group : the non-modular case

In [30], we propose efficient algorithms to compute the Gröbner basis of an ideal $I \subset k[x_1, \cdots, x_n]$ globally invariant under the action of a commutative matrix group G, in the non-modular case (where $char(k)$ doesn't divide $|G|$). The idea is to simultaneously diagonalize the matrices in G, and apply a linear change of variables on I corresponding to the base-change matrix of this diagonalization. We can now suppose that the matrices acting on I are diagonal. This action induces a grading on the ring $R = k[x_1, \cdots, x_n]$, compatible with the degree, indexed by a group related to G, that we call G-degree. The next step is the observation that this grading is maintained during a Gröbner basis computation or even a change of ordering, which allows us to split the Macaulay matrices into $|G|$ submatrices of roughly the same size. In the same way, we are able to split the canonical basis of R/I (the staircase) if I is a zero-dimensional ideal. Therefore, we derive *abelian* versions of the classical algorithms F_4, F_5 or FGLM. Moreover, this new variant of F_4/F_5 allows complete parallelization of the linear algebra steps, which has been successfully implemented. On instances coming from applications (NTRU crypto-system or the Cyclic-n problem), a speed-up of more than 400 can be obtained. For example, a Gröbner basis of the Cyclic-11 problem can be solved in less than 8 hours with this variant of F_4. Moreover, using this method, we can identify new classes of polynomial systems that can be solved in polynomial time.

6.1.6. Signature Rewriting in Gröbner Basis Computation

In [27] we introduce the RB algorithm for Gröbner basis computation, a simpler yet equivalent algorithm to F5GEN. RB contains the original unmodified F5 algorithm as a special case, so it is possible to study and understand F5 by considering the simpler RB. We present simple yet complete proofs of this fact and of F5's termination and correctness. RB is parametrized by a rewrite order and it contains many published algorithms as special cases, including SB. We prove that SB is the best possible instantiation of RB in the following sense. Let X be any instantiation of RB (such as F5). Then the S-pairs reduced by SB are always a subset of the S-pairs reduced by X and the basis computed by SB is always a subset of the basis computed by X.

6.1.7. An analysis of inhomogeneous signature-based Gröbner basis computations

In [8] we give an insight into the behaviour of signature-based Gröbner basis algorithms, like F5, G2V or SB, for inhomogeneous input. On the one hand, it seems that the restriction to sig-safe reductions puts a penalty on the performance. The lost connection between polynomial degree and signature degree can disallow lots of reductions and can lead to an overhead in the computations. On the other hand, the way critical pairs are sorted and corresponding s-polynomials are handled in signature- based algorithms is a very efficient one, strongly connected to sorting w.r.t. the well-known sugar degree of polynomials.

6.1.8. Improving incremental signature-based Gröbner basis algorithms

In [9] we describe a combination of ideas to improve incremental signature-based Gröbner basis algorithms having a big impact on their performance. Besides explaining how to combine already known optimizations to achieve more efficient algorithms, we show how to improve them even more. Although our idea has a positive affect on all kinds of incremental signature-based algorithms, the way this impact is achieved can be quite different. Based on the two best-known algorithms in this area, F5 and G2V, we explain our idea, both from a theoretical and a practical point of view.

6.1.9. A new algorithmic scheme for computing characteristic sets

Ritt-Wu's algorithm of characteristic sets is the most representative for triangularizing sets of multivariate polynomials. Pseudo-division is the main operation used in this algorithm. In [18] we present a new algorithmic scheme for computing generalized characteristic sets by introducing other admissible reductions than pseudo-division. A concrete subalgorithm is designed to triangularize polynomial sets using selected admissible reductions and several effective elimination strategies and to replace the algorithm of basic sets (used in Ritt-Wu's algorithm). The proposed algorithm has been implemented and experimental results show that it performs better than Ritt-Wu's algorithm in terms of computing time and simplicity of output for a number of non-trivial test examples

6.2. Solving Systems over the Reals and Applications

6.2.1. On the Boolean complexity of real root refinement

In [32] we assume that a real square-free polynomial A has a degree d, a maximum coefficient bitsize τ and a real root lying in an isolating interval and having no nonreal roots nearby (we quantify this assumption). Then, we combine the *Double Exponential Sieve* algorithm (also called the *Bisection of the Exponents*), the bisection, and Newton iteration to decrease the width of this inclusion interval by a factor of $t = 2^{-L}$. The algorithm has Boolean complexity $\widetilde{O}_B(d^2\tau + dL)$. Our algorithms support the same complexity bound for the refinement of r roots, for any $r \leq d$.

6.2.2. On the minimum of a polynomial function on a basic closed semialgebraic set and applications

In [17] we give an explicit upper bound for the algebraic degree and an explicit lower bound for the absolute value of the minimum of a polynomial function on a compact connected component of a basic closed semialgebraic set when this minimum is not zero. We also present extensions of these results to non-compact situations. As an application, we obtain a lower bound for the separation of two disjoint connected components of basic closed semialgebraic sets, when at least one of them is compact.

6.2.3. Rational solutions to Linear Matrix Inequalities and Sums of Squares

Consider a $(D \times D)$ symmetric matrix A whose entries are linear forms in $\mathbb{Q}[X_1, ..., X_k]$ with coefficients of bit size $\leq \tau$. In [31], we provide an algorithm which decides the existence of rational solutions to the linear matrix inequality $\mathsf{A} \succeq 0$ and outputs such a rational solution if it exists. This problem is of first importance: it can be used to compute algebraic certificates of positivity for multivariate polynomials. Our algorithm runs within $(k\tau)^{O(1)}2^{O(\min(k,D)D^2)}D^{O(D^2)}$ bit operations; the bit size of the output solution is dominated by $\tau^{O(1)}2^{O(\min(k,D)D^2)}$. These results are obtained by designing algorithmic variants of constructions introduced by Klep and Schweighofer. This leads to the best complexity bounds for deciding the existence of sums of squares with rational coefficients of a given polynomial. We have implemented the algorithm; it has been able to tackle Scheiderer's example of a multivariate polynomial that is a sum of squares over the reals but not over the rationals; providing the first computer validation of this counter-example to Sturmfels' conjecture.

6.2.4. Exact Voronoi diagram of smooth convex pseudo-circles: General predicates, and implementation for ellipses

In [10] we examine the problem of computing exactly the Voronoi diagram (via the dual Delaunay graph) of a set of, possibly intersecting, smooth convex pseudo-cirlces in the Euclidean plane, given in parametric form. Pseudo-circles are (convex) sites, every pair of which has at most two intersecting points. The Voronoi diagram is constructed incrementally. Our first contribution is to propose robust and efficient algorithms, under the exact computation paradigm, for all required predicates, thus generalizing earlier algorithms for non-intersecting ellipses. Second, we focus on INCIRCLE, which is the hardest predicate, and express it by a simple sparse 5×5 polynomial system, which allows for an efficient implementation by means of successive Sylvester resultants and a new factorization lemma. The third contribution is our CGAL-based C++ software for the case of possibly intersecting ellipses, which is the first exact implementation for the problem. Our code spends about a minute to construct the Voronoi diagram of 200 ellipses, when few degeneracies occur. It is faster than the CGAL segment Voronoi diagram, when ellipses are approximated by k-gons for $k > 15$, and a state-of-the-art implementation of the Voronoi diagram of points, when each ellipse is approximated by more than 1250 points.

6.2.5. Patience of Matrix Games

In [15], for matrix games we study how small nonzero probability must be used in optimal strategies. We show that for $n \times n$ win-lose-draw games (i.e. $(-1, 0, 1)$ matrix games) nonzero probabilities smaller than $n^{-O(n)}$ are never needed. We also construct an explicit $n \times n$ win-lose game such that the unique optimal strategy uses a nonzero probability as small as $n^{-\Omega(n)}$. This is done by constructing an explicit $(-1, 1)$ nonsingular

$n \times n$ matrix, for which the inverse has only nonnegative entries and where some of the entries are of value $n^{\Omega(n)}$.

6.2.6. A polynomial approach for extracting the extrema of a spherical function and its application in diffusion MRI

Antipodally symmetric spherical functions play a pivotal role in diffusion MRI in representing sub-voxel-resolution microstructural information of the underlying tissue. This information is described by the geometry of the spherical function. In [14] we propose a method to automatically compute all the extrema of a spherical function. We then classify the extrema as maxima, minima and saddle-points to identify the maxima. We take advantage of the fact that a spherical function can be described equivalently in the spherical harmonic (SH) basis, in the symmetric tensor (ST) basis constrained to the sphere, and in the homogeneous polynomial (HP) basis constrained to the sphere. We extract the extrema of the spherical function by computing the stationary points of its constrained HP representation. Instead of using traditional optimization approaches, which are inherently local and require exhaustive search or re-initializations to locate multiple extrema, we use a novel polynomial system solver which analytically brackets all the extrema and refines them numerically, thus missing none and achieving high precision. To illustrate our approach we consider the Orientation Distribution Function (ODF). In diffusion MRI the ODF is a spherical function which represents a state-of-the-art reconstruction algorithm whose maxima are aligned with the dominant fiber bundles. It is, therefore, vital to correctly compute these maxima to detect the fiber bundle directions. To demonstrate the potential of the proposed polynomial approach we compute the extrema of the ODF to extract all its maxima. This polynomial approach is, however, not dependent on the ODF and the framework presented in this line of work can be applied to any spherical function described in either the SH basis, ST basis or the HP basis.

6.2.7. Improving Angular Speed Uniformity by Reparameterization

In [20] we introduce the notion of angular speed uniformity as a quality measure for parameter-izations of plane curves and propose an algorithm to compute uniform reparameterizations for quadratic and cubic curves. We prove that only straight lines have uniform rational parameterizations. For any plane curve other than lines, we show how to find a rational reparameterization that has the maximum uniformity among all the rational parameterizations of the same degree. We also establish specific results for quadratic and certain cubic Bézier curves.

6.2.8. Formalization and Specification of Geometric Knowledge Objects

[7] presents our work on the identification, formalization, structuring, and specification of geometric knowledge objects for the purpose of semantic representation and knowledge management. We classify geometric knowledge according to how it has been accumulated and represented in the geometric literature, formalize geometric knowledge statements by adapting the language of first-order logic, specify knowledge objects with embedded knowledge in a retrievable and extensible data structure, and organize them by modeling the hierarchic structure of relations among them. Some examples of formal specification for geometric knowledge objects are given to illustrate our approach. The underlying idea of the approach has been used successfully for automated geometric reasoning, knowledge base creation, and electronic document generation.

6.2.9. A Framework for Improving Uniformity of Parameterizations of Curves

In [16] we define quasi-speed as a generalization of linear speed and angular speed for parameterizations of curves and use the uniformity of quasi-speed to measure the quality of the parameterizations. With such conceptual setting, a general framework is developed for studying uniformity behaviors under reparameterization via proper parameter transformation and for computing reparameterizations with improved uniformity of quasispeed by means of optimal single-piece, C^0 piecewise, and C^1 piecewise Möbius transformations. Algorithms are described for uniformity-improved reparameterization using different Möbius transformations with different optimization techniques. Examples are presented to illustrate the concepts, the framework, and the algorithms. Experimental results are provided to validate the framework and to show the efficiency of the algorithms.

6.3. Solving Systems in Finite Fields, Applications in Cryptology and Algebraic Number Theory

6.3.1. On the Complexity of Solving Quadratic Boolean Systems

A fundamental problem in computer science is to find all the common zeroes of m quadratic polynomials in n unknowns over $\mathbb{F}_2$. The cryptanalysis of several modern ciphers reduces to this problem. Up to now, the best complexity bound was reached by an exhaustive search in $4\log_2 n\, 2^n$ operations. We give an algorithm that reduces the problem to a combination of exhaustive search and sparse linear algebra. This algorithm has several variants depending on the method used for the linear algebra step. Under precise algebraic assumptions on the input system, we show in [4], that the deterministic variant of our algorithm has complexity bounded by $O(2^{0.841n})$ when $m = n$, while a probabilistic variant of the Las Vegas type has expected complexity $O(2^{0.792n})$. Experiments on random systems show that the algebraic assumptions are satisfied with probability very close to 1. We also give a rough estimate for the actual threshold between our method and exhaustive search, which is as low as 200, and thus very relevant for cryptographic applications.

6.3.2. Decomposing polynomial sets into simple sets over finite fields: The positive-dimensional case

Our work in [19] presents an algorithm for decomposing any positive-dimensional polynomial set into simple sets over an arbitrary finite field. The algorithm is based on some relationship established between simple sets and radical ideals, reducing the decomposition problem to the problem of computing the radicals of certain ideals. In addition to direct application of the algorithms of Matsumoto and Kemper, the algorithm of Fortuna and others is optimized and improved for the computation of radicals of special ideals. Preliminary experiments with an implementation of the algorithm in Maple and Singular are carried out to show the effectiveness and efficiency of the algorithm.

6.3.3. Using Symmetries in the Index Calculus for Elliptic Curves Discrete Logarithm

In 2004, an algorithm is introduced to solve the DLP for elliptic curves defined over a non prime finite field $\mathbb{F}_{q^n}$. One of the main steps of this algorithm requires decomposing points of the curve $E(\mathbb{F}_{q^n})$ with respect to a factor base, this problem is denoted PDP. In [11], we apply this algorithm to the case of Edwards curves, the well-known family of elliptic curves that allow faster arithmetic as shown by Bernstein and Lange. More precisely, we show how to take advantage of some symmetries of twisted Edwards and twisted Jacobi intersections curves to gain an exponential factor $2^{\omega(n-1)}$ to solve the corresponding PDP where ω is the exponent in the complexity of multiplying two dense matrices. Practical experiments supporting the theoretical result are also given. For instance, the complexity of solving the ECDLP for twisted Edwards curves defined over $\mathbb{F}_{q^5}$, with $q \approx 2^{64}$, is supposed to be $\sim 2^{160}$ operations in $E(\mathbb{F}_{q^5})$ using generic algorithms compared to 2^{130} operations (multiplication of two 32-bits words) with our method. For these parameters the PDP is intractable with the original algorithm. The main tool to achieve these results relies on the use of the symmetries and the quasi-homogeneous structure induced by these symmetries during the polynomial system solving step. Also, we use a recent work on a new algorithm for the change of ordering of Gröbner basis which provides a better heuristic complexity of the total solving process.

6.3.4. A Distinguisher for High Rate McEliece Cryptosystems

The Goppa Code Distinguishing (GD) problem consists in distinguishing the matrix of a Goppa code from a random matrix. The hardness of this problem is an assumption to prove the security of code-based cryptographic primitives such as McEliece's cryptosystem. Up to now, it is widely believed that the GD problem is a hard decision problem. We present in [12] the first method allowing to distinguish alternant and Goppa codes over any field. Our technique can solve the GD problem in polynomial-time provided that the codes have sufficiently large rates. The key ingredient is an algebraic characterization of the key-recovery problem. The idea is to consider the rank of a linear system which is obtained by linearizing a particular polynomial system describing a key-recovery attack. Experimentally it appears that this dimension depends on the type of code. Explicit formulas derived from extensive experimentations for the rank are provided for

"generic" random, alternant, and Goppa codes over any alphabet. Finally, we give theoretical explanations of these formulas in the case of random codes, alternant codes over any field of characteristic two and binary Goppa codes.

6.3.5. Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic

We investigate in this paper the security of HFE and Multi-HFE schemes as well as their minus and embedding variants. Multi-HFE is a generalization of the well-known HFE schemes. The idea is to use a multivariate quadratic system instead of a univariate polynomial in HFE over an extension field as a private key. According to the authors, this should make the classical direct algebraic (message-recovery) attack proposed by Faugère and Joux on HFE no longer efficient against Multi-HFE. We consider here the hardness of the key-recovery in Multi-HFE and its variants, but also in HFE (both for odd and even characteristic). We first improve and generalize the basic key recovery proposed by Kipnis and Shamir on HFE. To do so, we express this attack as matrix/vector operations. In one hand, this permits to improve the basic Kipnis-Shamir (KS) attack on HFE. On the other hand, this allows to generalize the attack on Multi-HFE. Due to its structure, we prove that a Multi-HFE scheme has much more equivalent keys than a basic HFE. This induces a structural weakness which can be exploited to adapt the KS attack against classical modifiers of multivariate schemes such as minus and embedding. Along the way, we discovered that the KS attack as initially described cannot be applied against HFE in characteristic 2. We have then strongly revised KS in characteristic 2 to make it work. In all cases, the cost of our attacks is related to the complexity of solving MinRank. Thanks to recent complexity results on this problem, we prove that our attack is polynomial in the degree of the extension field for all possible practical settings used in HFE and Multi-HFE. This makes then Multi-HFE less secure than basic HFE for equally-sized keys. As a proof of concept, we have been able to practically break the most conservative proposed parameters of multi-HFE in few days (256 bits security broken in 9 days).

6.3.6. Cryptanalysis of a Public-Key Encryption Scheme Based on New Multivariate Quadratic Assumptions

In [24], we investigate the security of a public-key encryption scheme introduced by Huang, Liu and Yang (HLY) at PKC'12. This new scheme can be provably reduced to the hardness of solving a set of quadratic equations whose coefficients of highest degree are chosen according to a discrete Gaussian distributions. The other terms being chosen uniformly at random. Such a problem is a variant of the classical problem of solving a system of non-linear equations (PoSSo), which is known to be hard for random systems. The main hypothesis of Huang, Liu and Yang is that their variant is not easier than solving PoSSo for random instances. In this paper, we disprove this hypothesis. To this end, we exploit the fact that the new problem proposed by Huang, Liu and Yang reduces to an easy instance of the Learning With Errors (LWE) problem. The main contribution of this paper is to show that security and efficiency are essentially incompatible for the HLY proposal. That is, one cannot find parameters which yield a secure and a practical scheme. For instance, we estimate that a public-key of at least 1.03 GB is required to achieve 80-bit security against known attacks. As a proof of concept, we present practical attacks against all the parameters proposed Huang, Liu and Yang. We have been able to recover the private-key in roughly one day for the first challenge (i.e. Case 1) proposed by HLY and in roughly three days for the second challenge (i.e. Case 2).

6.3.7. On the Complexity of the BKW Algorithm on LWE

In [3], we present a study of the complexity of the Blum-Kalai-Wasserman (BKW) algorithm when applied to the Learning with Errors (LWE) problem, by providing refined estimates for the data and computational effort requirements for solving concrete instances of the LWE problem. We apply this refined analysis to suggested parameters for various LWE-based cryptographic schemes from the literature and compare with alternative approaches based on lattice reduction. As a result, we provide new upper bounds for the concrete hardness of these LWE-based schemes. Rather surprisingly, it appears that BKW algorithm outperforms known estimates for lattice reduction algorithms starting in dimension $n \approx 250$ when LWE is reduced to SIS. However, this assumes access to an unbounded number of LWE samples.

6.3.8. Combined Attack on CRT-RSA. Why Public Verification Must Not Be Public?

In [25] we introduce a new Combined Attack on a CRT-RSA implementation resistant against Side-Channel Analysis and Fault Injection attacks. Such implementations prevent the attacker from obtaining the signature when a fault has been induced during the computation. Indeed, such a value would allow the attacker to recover the RSA private key by computing the gcd of the public modulus and the faulty signature. The principle of our attack is to inject a fault during the signature computation and to perform a Side-Channel Analysis targeting a sensitive value processed during the Fault Injection countermeasure execution. The resulting information is then used to factorize the public modulus, leading to the disclosure of the whole RSA private key. After presenting a detailed account of our attack, we explain how its complexity can be significantly reduced by using Coppersmith's techniques based on lattice reduction. We also provide simulations that confirm the efficiency of our attack as well as two different countermeasures having a very small impact on the performance of the algorithm. As it performs a Side-Channel Analysis during a Fault Injection countermeasure to retrieve the secret value, this article recalls the need for Fault Injection and Side-Channel Analysis countermeasures as monolithic implementations.

6.3.9. Polynomial root finding over local rings and application to error correcting codes

GURUSWAMI and SUDAN designed a polynomial-time list-decoding algorithm. Their method divides into two steps. First it computes a polynomial Q in $\mathbb{F}_q[x][y]$ such that the possible transmitted messages are roots of Q in $\mathbb{F}_q[x]$. In the second step one needs to determine all such roots of Q. Several techniques have been investigated to solve both steps of the problem.

The Guruswami and Sudan algorithm has been adapted to other families of codes such as algebraic-geometric codes and alternant codes over fields. Extensions over certain types of finite rings have further been studied for Reed-Solomon codes, for alternant codes, and for algebraic-geometric codes. In all these cases, the two main steps of the Guruswami and Sudan algorithm are roughly preserved, but to the best of our knowledge, the second step has never been studied into deep details from the complexity point of view. In [5], we investigate root-finding for polynomials over *Galois rings*, which are often used within these error correcting codes, and that are defined as non-ramified extension of $\mathbb{Z}/p^n\mathbb{Z}$. We study the cost of our algorithms, discuss their practical performances, and apply our results to the Guruswami and Sudan list decoding algorithm over Galois rings.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts and Grants with Industry

- Oberthur Technologies
  Oberthur Technologies is the World second largest provider of security and identification solutions and services based on smart card technologies for mobile, payment, transport, digital TV and convergence markets. Since 2007, SALSA co-supervised 3 internships of first year master student on cryptology in smart-cards, and one internship of a 2nd year master student. The goal of this last internship was to study the feasibility of implementing multivariate schemes in constrained environments (typically a smart card). A new jointly supervised PhD thesis (PolSys/Oberthur) has start in march 2012.
- Gemalto
  Gemalto is an international IT security company providing software applications, secure personal devices such as smart cards and token, etc.Governments, wireless operators, banks, and enterprises use Gemalto's software and personal devices to deliver mobile services, payment security, authenticated cloud access, identity and privacy protection, eHealthcare, eGovernment, transport ticketing and machine to machine (M2M) communications applications.

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- **ANR Jeunes Chercheurs CAC Computer Algebra and Cryptography (2009-2013).** The contract CAC "Computer Algebra and Cryptography started in October 2009 for a period of 4 years. This project investigates the areas of cryptography and computer algebra, and their influence on the security and integrity of digital data. In CAC, we plan to use basic tools of computer algebra to evaluate the security of cryptographic schemes. CAC will focus on three new challenging applications of algebraic techniques in cryptography; namely block ciphers, hash functions, and factorization with known bits. To this hand, we will use Gröbner bases techniques but also lattice tools. In this proposal, we will explore non-conventional approaches in the algebraic cryptanalysis of these problems (Participants: L. Perret [contact], J.-C. Faugère, G. Renault).
- **ANR Grant (international program) EXACTA (2010-2013): Exact/Certified Algorithms with Algebraic Systems.**
  The main objective of this project is to study and compute the solutions of nonlinear algebraic systems and their structures and properties with selected target applications using exact or certified computation. The project consists of one main task of basic research on the design and implementation of fundamental algorithms and four tasks of applied research on computational geometry, algebraic cryptanalysis, global optimization, and algebraic biology. It will last for three years (2010-2013) with 300 person-months of workforce. Its consortium is composed of strong research teams from France and China (KLMM, SKLOIS, and LMIB) in the area of solving algebraic systems with applications.
- **ANR Grant HPAC: High Performance Algebraic Computing (2012-2016).** The pervasive ubiquity of parallel architectures and memory hierarchy has led to a new quest for parallel mathematical algorithms and software capable of exploiting the various levels of parallelism: from hardware acceleration technologies (multi-core and multi-processor system on chip, GPGPU, FPGA) to cluster and global computing platforms. For giving a greater scope to symbolic and algebraic computing, beyond the optimization of the application itself, the effective use of a large number of resources (memory and specialized computing units) is expected to enhance the performance multi-criteria objectives: time, resource usage, reliability, even energy consumption. The design and the implementation of mathematical algorithms with provable, adaptive and sustainable performance is a major challenge. In this context, this project is devoted to fundamental and practical research specifically in exact linear algebra and system solving that are two essential "dwarfs" (or "killer kernels") in scientific and algebraic computing. The project should lead to progress in matrix algorithms and challenge solving in cryptology, and should provide new insights into high performance programming and library design problems (J.-C. Faugère [contact], L. Perret, G. Renault, M. Safey El Din).
- **ANR Grant GeoLMI: Geometry of Linear Matrix Inequalities (2011-2015).** he GeoLMI project aims at developing an algebraic and geometric study of linear matrix inequalities (LMI) for systems control theory. It is an interdisciplinary project at the border between information sciences (systems control), pure mathematics (algebraic geometry) and applied mathematics (optimisation). The project focuses on the geometry of determinantal varieties, on decision problems involving positive polynomials, on computational algorithms for algebraic geometry, on computational algorithms for semi-definite programming, and on applications of algebraic geometry techniques in systems control theory, namely for robust control of linear systems and polynomial optimal control (Participants: J.-C. Faugère, M. Safey El Din [contact], E. Tsigaridas).

8.2. European Initiatives

8.2.1. FP7 Projects

8.2.1.1. A3

Type: PEOPLE

Defi:

Instrument: Career Integration Grant

Objectif: NC

Duration: May 2013 - April 2017

Coordinator: Jean-Charles Faugère

Partner: Institut National de Recherche en Informatique et en Automatique (Inria), France

Inria contact: Elias Tsigaridas

Abstract: The project Algebraic Algorithms and Applications (A3) is an interdisciplinary and multidisciplinary project, with strong international synergy. It consists of four work packages The first (Algebraic Algorithms) focuses on fundamental problems of computational (real) algebraic geometry: effective zero bounds, that is estimations for the minimum distance of the roots of a polynomial system from zero, algorithms for solving polynomials and polynomial systems, derivation of non-asymptotic bounds for basic algorithms of real algebraic geometry and application of polynomial system solving techniques in optimization. We propose a novel approach that exploits structure and symmetry, combinatorial properties of high dimensional polytopes and tools from mathematical physics. Despite the great potential of the modern tools from algebraic algorithms, their use requires a combined effort to transfer this technology to specific problems. In the second package (Stochastic Games) we aim to derive optimal algorithms for computing the values of stochastic games, using techniques from real algebraic geometry, and to introduce a whole new arsenal of algebraic tools to computational game theory. The third work package (Non-linear Computational Geometry), we focus on exact computations with implicitly defined plane and space curves. These are challenging problems that commonly arise in geometric modeling and computer aided design, but they also have applications in polynomial optimization. The final work package (Efficient Implementations) describes our plans for complete, robust and efficient implementations of algebraic algorithms.

8.3. International Initiatives

8.3.1. Inria Associate Teams

The POLSYS Team and ARIC at ENS Lyon are part of the QOLAPS (Quantifier Elimination, Optimization, Linear Algebra and Polynomial Systems) Associate Team with the Symbolic Computation Group at North Carolina State University. Activities of this associate team are described at the following url:

http://www-polsys.lip6.fr/QOLAPS/index.html

8.3.1.1. Informal International Partners

- Crypto team at Royal Holloway, University of London, UK.
- Prof. Victor Y. Pan, Department of Mathematics and Computer Science Lehman College, City University of New York, USA.

8.3.2. Inria International Labs

The POLSYS Team is involved in the ECCA (Exact Certified Computation with Algebraic Systems) at LIAMA in China.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Prof. K. Yokoyama (Japan) visited the POLSYS team during January 2013.

Prof. C. Yap (Courant Institute, New-York, USA) was an Inria invited professor and visited the POLSYS team during June and July 2013.

Prof. B. Sturmfels (Univ. Berkeley, USA) visited the POLSYS team during July 2013.

Prof. I. Bomze (Univ. of Vienna, Austria) visited the POLSYS team during October 2013.

Prof. J. Guttierez (Univ. Santander, Spain) visited the POLSYS team during November 2013.

Prof. J. Hauenstein (North Carolina State Univ., USA) visited the POLSYS team during November 2013.

J. Rohal (North Carolina State Univ., USA) visited the POLSYS team during November 2013.

8.4.1.1. Internships

- T. Verron (Internship M2 and ENS Paris): Computation of Gröbner bases for quasi-homogeneous systems.

9. Dissemination

9.1. POLSYS seminar

Our seminar hosted over twenty invited speakers in 2013.
http://www-polsys.lip6.fr/Seminar/index.html

9.2. Scientific Animation

L. Perret was a PC member of Inscrypt'13, PKC'13 and Eurocrypt'14. L. Perret joined the editorial board of Designs, Codes and Cryptography.

L. Perret was invited speaker in the workshop "Computer algebra and polynomials" held on November 25-29, 2013 at the Research Institute for Symbolic Computation, Linz, Austria.

M. Safey El Din was invited speaker at

- the Polynomial Optimisation Program at Newton Institute in Cambridge (UK);
- the conference "Numerical Methods and Efficient Computations" in honor of J.-P. Dedieu, CIRM, France, 2013.
- the International Symposium on Symbolic and Algebraic Computation (ISSAC) [21].

C. Eder and E Tsigaridas were invited speakers in the workshop "Gröbner Bases, Resultants and Linear Algebra" held on 3-6 September 3-6, 2013 at the Research Institute for Symbolic Computation, Hagenberg, Austria.

G. Renault was invited speaker in the *Minisymposium On Coppersmith's Heuristic Algorithm for Finding Roots of Multivariate Polynomials* in the *SIAM Conference on Applied Algebraic Geometry* at Colorado State University, USA (August 1–4, 2013) (http://meetings.siam.org/sess/dsp_programsess.cfm?SESSIONCODE=16747).

M. Safey El Din co-organized (with P. Boito, G. Chèze and C. Pernet) the *Journées Nationales de Calcul Formel* in CIRM, France (May, 13-17, 2013) (http://jncf2013.imag.fr/).

M. Safey El Din co-organized (with E. Kaltofen and L. Zhi) the *Minisymposium on Exact Certificates in Nonlinear Global Optimization* in the *SIAM Conference on Applied Algebraic Geometry* at Colorado State University, USA (August 1–4, 2013) (http://meetings.siam.org/program.cfm?CONFCODE=AG13).

J.-C. Faugère was invited speaker in the *Computer algebra and polynomials* International Workshop at Linz, Austria (Dec 2013).

J.-C. Faugère was invited speaker in the *Multivariate Polynomial Workshop* at Fukuoka, Japan (Fev 2013).

J.-C. Faugère was invited speaker in the *Groebner bases, resultants and linear algebra Workshop* at Linz, Austria (Sep 2013).

M. Safey El Din and E. Tsigaridas organized the *Minisymposium Algorithms in Real Algebraic Geometry and its Applications* in the *SIAM Conference on Applied Algebraic Geometry* at Colorado State University, USA (August 1–4, 2013) (http://meetings.siam.org/program.cfm?CONFCODE=AG13).

M. Safey El Din is member of the editorial board of Journal of Symbolic Computation.

E. Tsigaridas (in collaboration with O. Devillers, M. Karavelas, M. Teillaud) organized the *Workshop on Geometric Computing, Heraklion*, in Greece, January 21 – 25 2013 (http://www.acmac.uoc.gr/GC2013/).

E. Tsigaridas participated in the *International Symposium on Symbolic and Algebraic Computation* (ISSAC) which was held in June 26-29, 2013 at Northeastern University, Boston, Massachusetts, USA and presented the paper [32].

C. Eder participated in the *International Symposium on Symbolic and Algebraic Computation* (ISSAC) which was held in June 26-29, 2013 at Northeastern University, Boston, Massachusetts, USA and presented the paper [27].

C. Eder was invited in University of Mississippi, Hattiesburg Mississippi (USA) on 25 June 2013 and gave a talk on *Improved Gröbner Basis computation with applications in cryptography*.

J.-C. Faugère has the following editorial activities:

- Associate Editor of Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences (SPRINGER).
- Guest Editor of a special issue of the Journal Of Symbolic Computation (2013) (with L. Perret).

D. Wang has the following editorial activities:

- Editor-in-Chief and Managing Editor for the journal
  Mathematics in Computer Science (published by Birkhäuser/Springer, Basel).
- Executive Associate Editor-in-Chief for the journal
  SCIENCE CHINA Information Sciences (published by Science China Press, Beijing and Springer, Berlin).
- Member of the Editorial Boards for the
  - Journal of Symbolic Computation (published by Academic Press/Elsevier, London),
  - Frontiers of Computer Science (published by Higher Education Press, Beijing and Springer, Berlin),
  - Texts and Monographs in Symbolic Computation (published by Springer, Wien New York),
  - Book Series on Mathematics Mechanization (published by Science Press, Beijing),
  - Book Series on Fundamentals of Information Science and Technology (published by Science Press, Beijing).
- Member of the International Advisory Board for the Communications of JSSAC (Japan Society for Symbolic and Algebraic Computation) (published by JSSAC).
- Editor for the Book Series in Computational Science (published by Tsinghua University Press, Beijing).

D. Wang was involved in the organization of the following conferences

- General Co-chair of the

5th International Conference on Mathematical Aspects of Computer and Information Sciences (MACIS 2013) (Nanning, China, December 11-13, 2013).

- Member of the Program Committee
  - 2nd International Workshop on Hybrid Systems and Biology (HSB 2013) (Taormina, Italy, September 2, 2013),
  - 15th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC 2013) (Timisoara, Romania, September 23-26, 2013).
- Co-organizer and Program Co-chair
  Second International Seminar on Program Verification, Automated Debugging and Symbolic Computation (PAS 2013) (Beijing, China, October 23-25, 2013).
- Member of the Steering Committee
  - International Conference on Mathematical Aspects of Computer and Information Sciences (MACIS)
  - International Symposium on Symbolic Computation in Software Science (SCSS).

9.3. Teaching - Supervision - Juries

9.3.1. Teaching

Master : J.-C. Faugère. Cours sur les systemes polynomiaux au MPRI Université Paris 7 Denis Diderot, France

Master : J. Berthomieu, Modélisation et résolutions numérique et symbolique de problèmes *via* les logiciels MAPLE et MATLAB, 35 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Master : J. Berthomieu, Algèbre linéaire et applications, 35 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Master : L. Perret, 96 heures équivalent TD, niveau M1 et M2, Université Pierre-et-Marie-Curie, France

Master : L. Perret, 96 heures équivalent TD, niveau L2 et M3, Université Pierre-et-Marie-Curie, France.

Master : G. Renault, Cryptologie Avancée, 50 heures équivalent TD, niveau M2, Université Pierre-et-Marie-Curie, France

Master : G. Renault, Algèbre linéaire et applications, 35 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Licence : G. Renault, Introduction à la Cryptologie, 50 heures équivalent TD, niveau L3, Université Pierre-et-Marie-Curie, France

Master : M. Safey El Din, Modélisation et résolutions numérique et symbolique de problèmes *via* les logiciels MAPLE et MATLAB, 35 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

9.3.2. Supervision

PhD : Aurélien Greuet, 5 Dec 2013, [1]. *Optimisation polynomiale et variétés polaires : theéorie, algorithmes et implantations.* University of Versailles Saint-Quentin and Université Pierre et Marie Curie, France. V. Cossart and M. Safey El Din.

PhD : Louise Huot, 13 Dec 2013. *Résolution de systèmes polynomiaux et cryptologie sur les courbes elliptiques.* Université Pierre et Marie Curie, France. J.-C. Faugère, P. Gaudry and G. Renault.

PhD : Jing Yang, 2013. Beihang University, China and North Carolina State University, USA. D. Wang and H. Hong.

PhD : Chenqi Mou, 2013. *Solving polynomial systems over finite fields*. Beihang University, China and Université Pierre et Marie Curie, France. J.-C. Faugère and D. Wang.

- J.-C. Faugère and M. Safey El Din supervise the PhD thesis of T. Verron.
- J.-C. Faugère and G. Renault supervise the PhD thesis of R. Zeitoun.
- J.-C. Faugère and L. Perret supervise the PhD thesis of F. Portzamparc.
- J.-C. Faugère supervises the PhD thesis of J. Svartz.
- J.-C. Faugère supervises the PhD thesis of A. Wallet (jointly with V. Vitse, UJF, Grenoble).
- M. Safey El Din supervises (jointly with D. Henrion, LAAS, Toulouse) the PhD thesis of S. Naldi.

9.3.3. Juries

M. Safey El Din was member of

- the Habilitation Thesis Committee of S. Graillat (UPMC) as an examiner (Dec. 2013) ;
- the PhD Thesis committee of A. Greuet (Univ. Versailles Saint-Quentin) as the PhD advisor (Dec. 2013) ;
- the PhD Thesis committee of L. Huot (UPMC) as an examiner (Dec. 2013) ;
- the PhD Thesis committee of C. Mou (UPMC and Beihang Univ.) as president (June 2013) ;
- the PhD Thesis committee of J. Rohal (North Carolina State Univ., USA) as an external examiner (Aug. 2013).

J.-C. Faugère was member of

- the PhD Thesis committee of L. Ducas (ENS Paris) as president (2013) ;
- the PhD Thesis committee of S. Montan (UPMC) as president (2013) ;
- the PhD Thesis committee of A. Greuet (Univ. Versailles Saint-Quentin) as examiner (Dec. 2013) ;
- the PhD Thesis committee of C. Mou (UPMC and Beihang Univ.) as PhD advisor (June 2013) ;
- the PhD Thesis committee of L. Huot (UPMC) as PhD advisor (Dec. 2013) ;

M. Safey El Din participated to the hiring committee for promotion to Associate Professor of the Academy of Mathematics and Systems Science in China.

G. Renault was member of

- the PhD Thesis committee of J.-G. Kammerer (Univ. Rennes 1) as examiner (May 2013) ;
- the PhD Thesis committee of L. Huot (UPMC) as PhD advisor (Dec. 2013).

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] A. GREUET. , *Optimisation polynomiale et variétés polaires : théorie, algorithmes, et implantations*, Université de Versailles-Saint Quentin en Yvelines, December 2013, http://hal.inria.fr/tel-00922805

[2] L. HUOT. , *Résolution de systèmes polynomiaux et cryptologie sur les courbes elliptiques*, Université Pierre et Marie Curie - Paris VI, December 2013, http://hal.inria.fr/tel-00925271

Articles in International Peer-Reviewed Journals

[3] M. ALBRECHT, C. CID, J.-C. FAUGÈRE, R. FITZPATRICK, L. PERRET. *On the Complexity of the BKW Algorithm on LWE*, in "Designs, Codes and Cryptography", July 2013 [*DOI :* 10.1007%2Fs10623-013-9864-x], http://hal.inria.fr/hal-00921517

[4] M. BARDET, J.-C. FAUGÈRE, B. SALVY, P.-J. SPAENLEHAUER. *On the Complexity of Solving Quadratic Boolean Systems*, in "Journal of Complexity", February 2013, vol. 29, n° 1, pp. 53-75 [*DOI :* 10.1016/J.JCO.2012.07.001], http://hal.inria.fr/hal-00655745

[5] J. BERTHOMIEU, G. LECERF, G. QUINTIN. *Polynomial root finding over local rings and application to error correcting codes*, in "Applicable Algebra in Engineering, Communication and Computing", December 2013, vol. 24, n° 6, pp. 413-443 [*DOI :* 10.1007/S00200-013-0200-5], http://hal.inria.fr/hal-00642075

[6] L. BETTALE, J.-C. FAUGÈRE, L. PERRET. *Cryptanalysis of HFE, Multi-HFE and Variants for Odd and Even Characteristic*, in "Designs, Codes and Cryptography", 2013, vol. 69, n° 1, pp. 1 - 52 [*DOI :* 10.1007/S10623-012-9617-2], http://hal.inria.fr/hal-00776072

[7] X. CHEN, D. WANG. *Formalization and Specification of Geometric Knowledge Objects*, in "Mathematics in Computer Science", 2013, vol. 7, n° 4 [*DOI :* 10.1007/S11786-013-0167-4], http://hal.inria.fr/hal-00913400

[8] C. EDER. *An analysis of inhomogeneous signature-based Gro¨bner basis computations*, in "Journal of Symbolic Computation", 2013, vol. 59, pp. 21–35 [*DOI :* 10.1016/J.JSC.2013.08.001], http://hal.inria.fr/hal-00930286

[9] C. EDER. *Improving incremental signature-based Gröbner basis algorithms*, in "ACM Communications in Computer Algebra", 2013, vol. 47, n° 1, pp. 1-13 [*DOI :* 10.1145/2503697.2503699], http://hal.inria.fr/hal-00930293

[10] I. EMIRIS, E. TSIGARIDAS, G. TZOUMAS. *Exact Voronoi diagram of smooth convex pseudo-circles: General predicates, and implementation for ellipses*, in "Computer Aided Geometric Design", 2013 [*DOI :* 10.1016/J.CAGD.2013.06.005], http://hal.inria.fr/hal-00843033

[11] J.-C. FAUGÈRE, P. GAUDRY, L. HUOT, G. RENAULT. *Using Symmetries in the Index Calculus for Elliptic Curves Discrete Logarithm*, in "Journal of Cryptology", May 2013, pp. 1-40, 40 pages [*DOI :* 10.1007/S00145-013-9158-5], http://hal.inria.fr/hal-00700555

[12] J.-C. FAUGÈRE, V. GAUTHIER-UMANA, A. OTMANI, L. PERRET, J.-P. TILLICH. *A Distinguisher for High Rate McEliece Cryptosystems*, in "IEEE Transactions on Information Theory", June 2013, vol. 59, n° 10, pp. 6830-6844 [*DOI :* 10.1109/TIT.2013.2272036], http://hal.inria.fr/hal-00776068

[13] J.-C. FAUGÈRE, M. SAFEY EL DIN, P.-J. SPAENLEHAUER. *On the Complexity of the Generalized MinRank Problem*, in "Journal of Symbolic Computation", March 2013, vol. 55, pp. 30-58 [*DOI :* 10.1016/J.JSC.2013.03.004], http://hal.inria.fr/hal-00654094

[14] A. GHOSH, E. TSIGARIDAS, B. MOURRAIN, R. DERICHE. *A polynomial approach for extracting the extrema of a spherical function and its application in diffusion MRI*, in "Medical Image Analysis", July 2013, vol. 17, n° 5, pp. 503-514 [*DOI :* 10.1016/J.MEDIA.2013.03.004], http://hal.inria.fr/hal-00815120

[15] K. A. HANSEN, R. IBSEN-JENSEN, V. V. PODOLSKII, E. TSIGARIDAS. *Patience of Matrix Games*, in "Discrete Applied Mathematics", 2013 [*DOI :* 10.1016/J.DAM.2013.05.008], http://hal.inria.fr/hal-00843052

[16] H. HONG, D. WANG, J. YANG. *A Framework for Improving Uniformity of Parameterizations of Curves*, in "Science China Information Sciences", 2013, vol. 56, n^{o} 10 [*DOI :* 10.1007/s11432-013-4924-4], http://hal.inria.fr/hal-00913394

[17] G. JERONIMO, D. PERRUCCI, E. TSIGARIDAS. *On the minimum of a polynomial function on a basic closed semialgebraic set and applications*, in "SIAM Journal on Optimization", 2013, vol. 23, n^{o} 1, pp. 241–255, http://hal.inria.fr/hal-00776280

[18] M. JIN, X. LI, D. WANG. *A new algorithmic scheme for computing characteristic sets*, in "Journal of Symbolic Computation", 2013, vol. 50, pp. 431-449 [*DOI :* 10.1016/J.JSC.2012.04.004], http://hal.inria.fr/hal-00793120

[19] C. MOU, D. WANG, X. LI. *Decomposing polynomial sets into simple sets over finite fields: The positive-dimensional case*, in "Theoretical Computer Science", January 2013, vol. 468, pp. 102-113 [*DOI :* 10.1016/J.TCS.2012.11.009], http://hal.inria.fr/hal-00765840

[20] J. YANG, D. WANG, H. HONG. *Improving Angular Speed Uniformity by Reparameterization*, in "Computer Aided Geometric Design", 2013, vol. 30, n^{o} 7, pp. 636-652 [*DOI :* 10.1016/J.CAGD.2013.04.001], http://hal.inria.fr/hal-00913378

Invited Conferences

[21] M. SAFEY EL DIN. *Critical Point Methods and Effective Real Algebraic Geometry: New Results and Trends*, in "ISSAC 2013 - 38th International Symposium on Symbolic and Algebraic Computation", Boston, United States, M. KAUERS (editor), 2013, pp. 5-6 [*DOI :* 10.1145/2465506.2465928], http://hal.inria.fr/hal-00922718

[22] D. WANG. *Automation of Geometry - Theorem Proving, Diagram Generation, and Knowledge Management*, in "ADG 2012 - 9th International Workshop Automated Deduction in Geometry", Edinburgh, United Kingdom, T. IDA, J. FLEURIOT (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 7993, pp. 31-32 [*DOI :* 10.1007/978-3-642-40672-0_2], http://hal.inria.fr/hal-00913433

International Conferences with Proceedings

[23] M. ALBRECHT, J.-C. FAUGÈRE, R. FITZPATRICK, L. PERRET. *Lazy Modulus Switching for the BKW Algorithm on LWE*, in "Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography", Buenos Aires, Argentina, Springer, March 2014, http://hal.inria.fr/hal-00925187

[24] M. ALBRECHT, J.-C. FAUGÈRE, R. FITZPATRICK, L. PERRET, Y. TODO, K. XAGAWA. *Practical Cryptanalysis of a Public-Key Encryption Scheme Based on New Multivariate Quadratic Assumptions*, in "PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography", Buenos Aires, Argentina, Springer, March 2014, http://hal.inria.fr/hal-00932382

[25] G. BARBU, A. BATTISTELLLO, G. DABOSVILLE, C. GIRAUD, G. RENAULT, S. RENNER, R. ZEITOUN. *Combined Attack on CRT-RSA. Why Public Verification Must Not Be Public?*, in "PKC 2013 - Public-Key Cryptography", Nara, Japan, K. KUROSAWA, G. HANAOKA (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 7778, pp. 1-17 [*DOI :* 10.1007/978-3-642-36362-7_13], http://hal.inria.fr/hal-00777788

[26] J. BI, J.-S. CORON, J.-C. FAUGÈRE, P. Q. NGUYEN, G. RENAULT, R. ZEITOUN. *Rounding and Chaining LLL: Finding Faster Small Roots of Univariate Polynomial Congruences*, in "PKC 2014 - 17th IACR International Conference on Practice and Theory of Public-Key Cryptography", Buenos Aires, Argentina, Springer, 2014, http://hal.inria.fr/hal-00926902

[27] C. EDER, B. H. ROUNE. *Signature Rewriting in Gro¨bner Basis Computation*, in "ISSAC 2013 - International Symposium on Symbolic and Algebraic Computation", Boston, United States, M. KAUERS (editor), ACM, 2013, pp. 331-338 [*DOI :* 10.1145/2465506.2465522], http://hal.inria.fr/hal-00930273

[28] J.-C. FAUGÈRE, L. HUOT, A. JOUX, G. RENAULT, V. VITSE. *Symmetrized summation polynomials: using small order torsion points to speed up elliptic curve index calculus*, in "EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques", Copenhagen, Denmark, 2014, http://hal.inria.fr/hal-00935050

[29] J.-C. FAUGÈRE, M. SAFEY EL DIN, T. VERRON. *On the Complexity of Computing Gröbner Bases for Quasi-homogeneous Systems*, in "Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation", Boston, United States, ACM, 2013, pp. 189–196 [*DOI :* 10.1145/2465506.2465943], http://hal.inria.fr/hal-00780388

[30] J.-C. FAUGÈRE, J. SVARTZ. *Gröbner Bases of Ideals Invariant under a Commutative Group: the Non-Modular Case*, in "IProceedings of the 38th International Symposium on Symbolic and Algebraic Computation", Boston, United States, ACM, 2013, pp. 347-354 [*DOI :* 10.1145/2465506.2465944], http://hal.inria.fr/hal-00819337

[31] Q. GUO, M. SAFEY EL DIN, L. ZHI. *Computing rational solutions of linear matrix inequalities*, in "ISSAC 2013 - International Symposium on Symbolic and Algebraic Computation", Boston, United States, 2013, http://hal.inria.fr/hal-00815174

[32] V. PAN, E. TSIGARIDAS. *On the Boolean complexity of real root refinement*, in "ISSAC 2013 - International Symposium on Symbolic and Algebraic Computation", Boston, United States, M. KAUERS (editor), ACM, April 2013 [*DOI :* 10.1145/2465506.2465938], http://hal.inria.fr/hal-00816214

[33] J. YANG, D. WANG, H. HONG. *Improving Angular Speed Uniformity by C^1 Piecewise Reparameterization*, in "ADG 2012 - 9th International Workshop Automated Deduction in Geometry", Edinburgh, United Kingdom, T. IDA, J. FLEURIOT (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 7993, pp. 33-47 [*DOI :* 10.1007/978-3-642-40672-0_3], http://hal.inria.fr/hal-00913415

Other Publications

[34] M. ALBRECHT, J.-C. FAUGÈRE, R. FITZPATRICK, L. PERRET. , *Practical Cryptanalysis of a Public-Key Encryption Scheme Based on New Multivariate Quadratic Assumptions*, January 2014, http://hal.inria.fr/hal-00918314

[35] B. BANK, M. GIUSTI, J. HEINTZ, M. SAFEY EL DIN. , *Intrinsic complexity estimates in polynomial optimization*, April 2013, http://hal.inria.fr/hal-00815123

[36] M. BARDET, J.-C. FAUGÈRE, B. SALVY. , *On the Complexity of the F5 Gröbner basis Algorithm*, December 2013, 20 pages, http://hal.inria.fr/hal-00915522

[37] J. BERTHOMIEU. , *Decomposition of multihomogeneous polynomials: minimal number of variables*, January 2013, http://hal.inria.fr/hal-00778659

[38] J. BERTHOMIEU, J.-C. FAUGÈRE, L. PERRET. , *Polynomial-Time Algorithms for Quadratic Isomorphism of Polynomials*, 2013, http://hal.inria.fr/hal-00846041

[39] X. CHEN, D. WANG, X. ZHANG. , *Mathematics, Data and Knowledge*, 2013, Special focus of Mathematics in Computer Science, Birkhäuser/Springer, Basel, http://hal.inria.fr/hal-00913449

[40] J.-C. FAUGÈRE, P. GAUDRY, L. HUOT, G. RENAULT. , *Polynomial Systems Solving by Fast Linear Algebra*, 2013, 27 pages, http://hal.inria.fr/hal-00816724

[41] J.-C. FAUGÈRE, C. MOU. , *Sparse FGLM algorithms*, April 2013, http://hal.inria.fr/hal-00807540

[42] A. GREUET, M. SAFEY EL DIN. , *Probabilistic Algorithm for Polynomial Optimization over a Real Algebraic Set*, 2013, http://hal.inria.fr/hal-00849523

[43] M. SAFEY EL DIN, E. SCHOST. , *A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets*, July 2013, http://hal.inria.fr/hal-00849057

[44] M. SAFEY EL DIN, E. TSIGARIDAS. , *A probabilistic algorithm to compute the real dimension of a semi-algebraic set*, 2014, Several typos fixed in Sections 4 and 5. There is an error in Section 5 and thus the complexity result stated does not hold, http://hal.inria.fr/hal-00808708