IN PARTNERSHIP WITH:
CNRS

Université Pierre et Marie Curie (Paris 6)

Activity Report 2011

Project-Team SALSA

Solvers for Algebraic Systems and Applications

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

RESEARCH CENTER
Paris - Rocquencourt

THEME
Algorithms, Certification, and Cryptography

Table of contents

Project-Team SALSA

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

1. Members

Research Scientists

Jean-Charles Faugère [Team Leader, Senior Researcher, INRIA, HdR]
Dongming Wang [Senior Researcher, CNRS, HdR]

Faculty Members

Daniel Lazard [Emeritus Professor, HdR]
Ludovic Perret [Assistant Professor - Univ. Pierre et Marie Curie]
Guénaël Renault [Assistant Professor - Univ. Pierre et Marie Curie]
Mohab Safey El Din [Assistant Professor - Univ. Pierre et Marie Curie, HdR]

PhD Students

Ye Liang [China Scholarship Council - defense in 2011 - J.-C. Faugère/D. Wang]
Wei Niu [China Scholarship Council - defense in 2011 - D. Wang]
Chenqi Mou [China Scholarship Council - defense in 2012 - J.-C. Faugère/D. Wang]
Luk Bettale [DGA - defense in 2011 - J.-C. Faugère/L. Perret]
Pierre-Jean Spaenlehauer [AMX - defense in 2013 - J.-C. Faugère/M. Safey El Din]
Christopher Goyet [CIFRE - defense in 2013 - J.-C. Faugère/G. Renault]
Louise Huot [EDITE - defense in 2014 - J.-C. Faugère/G. Renault]
Aurelien Greuet [Versailles - defense in 2014 - M. Safey El Din]
Frédéric de Portzamparc [CIFRE - defense in 2015 - J.-C. Faugère/L. Perret]
Rina Zeitoun [CIFRE - defense in 2015 - J.-C. Faugère/G. Renault]
Jules Svartz [AMN - defense in 2015 - J.-C. Faugère]

Post-Doctoral Fellows

Martin Albrecht [Dec 2010 - Nov 2012]
Cristophe Petit [Dec 2010 - May 2011]
Adrien Poteaux [Sep 2010 - August 2011]
Elias Tsigaridas [Jan 2012 - Jan 2013]

Administrative Assistant

Laurence Bourcier [Secretary (SAR) Inria]

2. Overall Objectives

2.1. Introduction

The main objective of the SALSA project is to solve systems of polynomial equations and inequations. We emphasize on algebraic methods which are more robust and frequently more efficient than purely numerical tools.

Polynomial systems have many applications in various scientific - academic as well as industrial - domains. However much work is yet needed in order to define specifications for the output of the algorithms which are well adapted to the problems.

The variety of these applications implies that our software needs to be robust. In fact, almost all problems we are dealing with are highly numerically unstable, and therefore, the correctness of the result needs to be guaranteed.

Thus, a key target is to provide software which are competitive in terms of efficiency but preserve certified outputs. Therefore, we restrict ourselves to algorithms which verify the assumptions made on the input, check the correctness of possible random choices done during a computation without sacrificing the efficiency. Theoretical complexity for our algorithms is only a preliminary step of our work which culminates with efficient implementations which are designed to solve significant applications.
A consequence of our way of working is that many of our contributions are related to applicative topics such as cryptography, error correcting codes, robotics and signal theory. We have to emphasize that these applied contributions rely on a long-term and global management of the project with clear and constant objectives leading to theoretical and deep advances.

2.2. Highlights

- **Computer Algebra**. Best Poster Award STOC 2011 (San Jose, USA) – PWE : Polynomial with Errors.
- **ANR Grants** Two new projects (HPAC and GEOLMI) were accepted (4 years projetcs).
- **Maple**. Maple 15 release : the contract with Maple was renewed until Dec. 2011.

3. Scientific Foundations

3.1. Introduction

For polynomial system solving, the mathematical specification of the result of a computation, in particular when the number of solutions is infinite, is itself a difficult problem [1], [58], [57]. Sorting the most frequently asked questions appearing in the applications, one distinguishes several classes of problems which are different either by their mathematical structure or by the significance that one can give to the word "solving".

Some of the following questions have a different meaning in the real case or in the complex case, others are posed only in the real case :

- zero-dimensional systems (with a finite number of complex solutions - which include the particular case of univariate polynomials); The questions in general are well defined (numerical approximation, number of solutions, etc) and the handled mathematical objects are relatively simple and well-known;
- parametric systems: They are generally zero-dimensional for almost all the parameters' values. The goal is to characterize the solutions of the system (number of real solutions, existence of a parameterization, etc.) with respect to parameters' values.
- positive dimensional systems: For a direct application, the first question is the existence of zeros of a particular type (for example real, real positive, in a finite field). The resolution of such systems can be considered as a black box for the study of more general problems (semi-algebraic sets for example) and information to be extracted is generally the computation of a point per connected component in the real case.
- constructible and semi-algebraic sets: As opposed to what occurs numerically, the addition of constraints or inequalities complicates the problem. Even if semi-algebraic sets represent the basic object of the real geometry, their automatic "and effective study" remains a major challenge. To date, the state of the art is poor since only two classes of methods are existing :
  - the Cylindrical Algebraic Decomposition which basically computes a partition of the ambient space in cells where the signs of a given set of polynomials are constant;
  - deformations based methods that turn the problem into solving algebraic varieties.

The first solution is limited in terms of performances (maximum 3 or 4 variables) because of a recursive treatment variable by variable, the second also because of the use of a sophisticated arithmetic (formal infinitesimals).

- quantified formulas; deciding efficiently if a first order formula is valid or not is certainly one of the greatest challenges in "effective" real algebraic geometry. However this problem is relatively well encircled since it can always be rewritten as the conjunction of (supposed to be) simpler problems like the computation of a point per connected component of a semi-algebraic set.

As explained in some parts of this document, the iniquity of the studied mathematical objects does not imply the uncut of the related algorithms. The priorities we put on our algorithmic work are generally dictated by the applications. Thus, above items naturally structure the algorithmic part of our research topics.

For each of these goals, our work is to design the most efficient possible algorithms: there is thus a strong correlation between implementations and applications, but a significant part of the work is dedicated to the identification of black-box allowing a modular approach of the problems. For example, the resolution of the zero-dimensional systems is a prerequisite for the algorithms treating of parametric or positive dimensional systems.

An essential class of black-box developed in the project does not appear directly in the absolute objectives counted above : the "algebraic or complex" resolutions. They are mostly reformulations, more algorithmically usable, of the studied systems. One distinguishes two categories of complementary objects :

- ideals representations: From a computational point of view these are the structures which are used in the first steps;
- varieties representations: The algebraic variety, or more generally the constructible or semi-algebraic set is the studied object.

To give a simple example, in $\mathbb{C}^2$ the variety $\{(0,0)\}$ can be seen like the zeros set of more or less complicated ideals (for example, ideal(X,Y), ideal(X^2,Y), ideal(X^2,X,Y,Y^3), etc). The entry which is given to us is a system of equations, i.e. an ideal. It is essential, in many cases, to understand the structure of this object to be able to correctly treat the degenerated cases. A striking example is certainly the study of the singularities. To take again the preceding example, the variety is not singular, but this cannot be detected by the blind application of the Jacobian criterion (one could wrongfully think that all the points are singular, contradicting, for example, Sard's lemma).

The basic tools that we develop and use to understand in an automatic way the algebraic and geometrical structures are on the one hand Gröbner bases (the most known object used to represent an ideal without loss of information) and on the other hand triangular sets (effective way to represent the varieties).

3.2. Gröbner basis and triangular sets

Participants: J.C. Faugère, G. Renault, M. Safey El Din, P.J. Spaenlehauer, D. Wang, C. Mou, J. Svartz.

Let us denote by $K[X_1,...,X_n]$ the ring of polynomials with coefficients in a field K and indeterminates $X_1,...,X_n$ and $S=\{P_1,...,P_s\}$ any subset of $K[X_1,...,X_n]$. A point $x \in \mathbb{C}^n$ is a zero of S if $P_i(x)=0 \quad i \in [1...s]$.

The ideal $\mathcal{I}=\langle P_1,...,P_s\rangle$ generated by $P_1,...,P_s$ is the set of polynomials in $K[X_1,...,X_n]$ constituted by all the combinations $\sum\limits_{k=1}^{R} P_k U_k$ with $U_k \in \mathbb{Q}[X_1,...,X_n]$. Since every element of $\mathcal{I}$ vanishes at each zero of S, we denote by $V_C(S)=V_C(I)=\{x \in C^n \mid p(x)=0 \ \forall p \in \mathcal{I}\}$ (resp. $V_R(S)=V_R(I)=V_{\mathbb{C}}(I)\bigcap\mathbb{R}^n$), the set of complex (resp. real) zeros of S, where R is a real closed field containing K and C its algebraic closure.

One Gröbner basis' main property is to provide an algorithmic method for deciding if a polynomial belongs or not to an ideal through a reduction function denoted "Reduce" from now.

If G is a Gröbner basis of an ideal $\mathcal{I} \subset \mathbb{Q}[X_1, ..., X_n]$ for any monomial ordering $<$.

(i) a polynomial $p \in \mathbb{Q}[X_1, ..., X_n]$ belongs to $\mathcal{I}$ if and only if Reduce$(p, G, <) = 0$,

(ii) Reduce(p,G,$<$) does not depend on the order of the polynomials in the list G, thus, this is a canonical reduced expression modulus $\mathcal{I}$, and the Reduce function can be used as a *simplification* function.

Gröbner bases are computable objects. The most popular method for computing them is Buchberger's algorithm ([47], [46]). It has several variants and it is implemented in most of general computer algebra systems like Maple or Mathematica. The computation of Gröbner bases using Buchberger's original strategies has to face to two kind of problems :

- (A) arbitrary choices : the order in which are done the computations has a dramatic influence on the computation time;
- (B) useless computations : the original algorithm spends most of its time in computing 0.

For problem (A), J.C. Faugère proposed ([4] - algorithm F_4) a new generation of powerful algorithms ([4]) based on the intensive use of linear algebra technics. In short, the arbitrary choices are left to computational strategies related to classical linear algebra problems (matrix inversions, linear systems, etc.).

For problem (B), J.C. Faugère proposed ([3]) a new criterion for detecting useless computations. Under some regularity conditions on the system, it is now proved that the algorithm do never perform useless computations.

A new algorithm named F_5 was built using these two key results. Even if it still computes a Gröbner basis, the gap with existing other strategies is consequent. In particular, due to the range of examples that become computable, Gröbner basis can be considered as a reasonable computable object in large applications.

We pay a particular attention to Gröbner bases computed for elimination orderings since they provide a way of "simplifying" the system (equivalent system with a structured shape). A well known property is that the zeros of the first non null polynomial define the Zariski closure (classical closure in the case of complex coefficients) of the projection on the coordinate's space associated with the smallest variables.

Such kinds of systems are algorithmically easy to use, for computing numerical approximations of the solutions in the zero-dimensional case or for the study of the singularities of the associated variety (triangular minors in the Jacobian matrices).

Triangular sets have a simplier structure, but, except if they are linear, algebraic systems cannot, in general, be rewritten as a single triangular set, one speaks then of decomposition of the systems in several triangular sets.

Lexicographic Gröbner bases	Triangular sets
$\begin{cases} f(X_1) = 0 \\ f_2(X_1, X_2) = 0 \\ \vdots \\ f_{k_2}(X_1, X_2) = 0 \\ f_{k_2+1}(X_1, X_2, X_3) = 0 \\ \vdots \\ f_{k_{n-1}+1}(X_1, ..., X_n) = 0 \\ \vdots \\ f_{k_n}(X_1, ..., X_n) = 0 \end{cases}$	$\begin{cases} t_1(X_1) = 0 \\ t_2(X_1, X_2) = 0 \\ \vdots \\ t_n(X_1, ..., X_n) = 0 \end{cases}$

Triangular sets appear under various names in the field of algebraic systems. J.F. Ritt ([64]) introduced them as characteristic sets for prime ideals in differential algebra. His constructive algebraic tools were adapted by W.T. Wu in the late seventies for geometric applications. The concept of regular chain (see [56] and [74]) is adapted for recursive computations in a univariate way.

It provides a membership test and a zero-divisor test for the strongly unmixed dimensional ideal it defines. Kalkbrenner defined regular triangular sets and showed how to decompose algebraic varieties as a union of Zariski closures of zeros of regular triangular sets. Gallo showed that the principal component of a triangular decomposition can be computed in $O(d^{O(n^2)})$ (n= number of variables, d=degree in the variables). During the 90s, implementations of various strategies of decompositions multiply, but they drain relatively heterogeneous specifications.

D. Lazard contributed to the homogenization of the work completed in this field by proposing a series of specifications and definitions gathering the whole of former work [1]. Two essential concepts for the use of these sets (regularity, separability) at the same time allow from now on to establish a simple link with the studied varieties and to specify the computed objects precisely.

A remarkable and fundamental property in the use we have of the triangular sets is that the ideals induced by regular and separable triangular sets, are radical and equidimensional. These properties are essential for some of our algorithms. For example, having radical and equidimensional ideals allows us to compute straightforwardly the singular locus of a variety by canceling minors of good dimension in the Jacobian matrix of the system. This is naturally a basic tool for some algorithms in real algebraic geometry [2], [7], [67].

In 1993, Wang [70] proposed a method for decomposing any polynomial system into *fine* triangular systems which have additional properties such as the projection property that may be used for solving parametric systems (see Section 3.4.2).

Triangular sets based techniques are efficient for specific problems, but the implementations of direct decompositions into triangular sets do not currently reach the level of efficiency of Gröbner bases in terms of computable classes of examples. Anyway, our team benefits from the progress carried out in this last field since we currently perform decompositions into regular and separable triangular sets through lexicographical Gröbner bases computations.

3.3. Zero–dimensional systems

Participants: L. Bettale, J.C. Faugère, D. Lazard, C. Mou, J. Svartz, P.J. Spaenlehauer.

A system is zero-dimensional if the set of the solutions in an algebraically closed field is finite. In this case, the set of solutions does not depend on the chosen algebraically closed field.

Such a situation can easily be detected on a Gröbner basis for any admissible monomial ordering.

These systems are mathematically particular since one can systematically bring them back to linear algebra problems. More precisely, the algebra $K[X_1, ..., X_n]/I$ is in fact a K-vector space of dimension equal to the number of complex roots of the system (counted with multiplicities). We chose to exploit this structure. Accordingly, computing a base of $K[X_1, ..., X_n]/I$ is essential. A Gröbner basis gives a canonical projection from $K[X_1, ..., X_n]$ to $K[X_1, ..., X_n]/I$, and thus provides a base of the quotient algebra and many other informations more or less straightforwardly (number of complex roots for example).

The use of this vector-space structure is well known and at the origin of the one of the most known algorithms of the field ([49]) : it allows to deduce, starting from a Gröbner basis for any ordering, a Gröbner base for any other ordering (in practice, a lexicographic basis, which are very difficult to compute directly). It is also common to certain semi-numerical methods since it allows to obtain quite simply (by a computation of eigenvalues for example) the numerical approximation of the solutions (this type of algorithms is developed, for example, in the INRIA Galaad project).

Contrary to what is written in a certain literature, the computation of Gröbner bases is not "doubly exponential" for all the classes of problems. In the case of the zero-dimensional systems, it is even shown that it is simply exponential in the number of variables, for a degree ordering and for the systems without zeros at infinity. Thus, an effective strategy consists in computing a Gröbner basis for a favorable ordering and then to deduce, by linear algebra technics, a Gröbner base for a lexicographic ordering [49].

The case of the zero-dimensional systems is also specific for triangular sets. Indeed, in this particular case, we have designed algorithms that allow to compute them efficiently [59] starting from a lexicographic Gröbner basis. Note that, in the case of zero-dimensional systems, regular triangular sets are Gröbner bases for a lexicographical order.

Many teams work on Gröbner bases and some use triangular sets in the case of the zero-dimensional systems, but up to our knowledge, very few continue the work until a numerical resolution and even less tackle the specific problem of computing the real roots. It is illusory, in practice, to hope to obtain numerically and in a reliable way a numerical approximation of the solutions straightforwardly from a lexicographical basis and even from a triangular set. This is mainly due to the size of the coefficients in the result (rational number).

The use of innovative algorithms for Gröbner bases computations [4], [3], Rational Univariate representations ([49] and [38] for the "shape position" case, allows to use zero-dimensional solving as sub-task in other algorithms.

3.4. Positive-dimensional and parametric systems

Participants: J.C. Faugère, D. Lazard, M. Safey El Din, D. Wang.

When a system is **positive dimensional** (with an infinite number of complex roots), it is no more possible to enumerate the solutions. Therefore, the solving process reduces to decomposing the set of the solutions into subsets which have a well-defined geometry. One may perform such a decomposition from an algebraic point of view or from a geometrical one, the latter meaning not taking the multiplicities into account (structure of primary components of the ideal is lost).

Although there exist algorithms for both approaches, the algebraic point of view is presently out of the possibilities of practical computations, and we restrict ourselves to geometrical decompositions.

When one studies the solutions in an algebraically closed field, the decompositions which are useful are the equidimensional decomposition (which consists in considering separately the isolated solutions, the curves, the surfaces, ...) and the prime decomposition (decomposes the variety into irreducible components). In practice, our team works on algorithms for decomposing the system into *regular separable triangular sets*, which corresponds to a decomposition into equidimensional but not necessarily irreducible components. These irreducible components may be obtained eventually by using polynomial factorization.

However, in many situations one is looking only for real solutions satisfying some inequalities ($P_i > 0$ or $P_i \geq 0$)[1]. In this case, there are various kinds of decompositions besides the above ones: connected components, cellular or simplicial decompositions, ...

There are general algorithms for such tasks, which rely on Tarski's quantifier elimination. Unfortunately, these problems have a very high complexity, usually doubly exponential in the number of variables or the number of blocks of quantifiers, and these general algorithms are intractable. It follows that the output of a solver should be restricted to a partial description of the topology or of the geometry of the set of solutions, and our research consists in looking for more specific problems, which are interesting for the applications, and which may be solved with a reasonable complexity.

We focus on 2 main problems:
1. computing one point on each connected components of a semi-algebraic set;
2. solving systems of equalities and inequalities depending on parameters.

[1] In the zero-dimensional case, inequations and inequalities are usually taken into account only at the end of the computation, to eliminate irrelevant solutions.

3.4.1. Critical point methods

The most widespread algorithm computing sampling points in a semi-algebraic set is the Cylindrical Algebraic Decomposition Algorithm due to Collins [48]. With slight modifications, this algorithm also solves the problem of Quantifier Elimination. It is based on the recursive elimination of variables one after an other ensuring nice properties between the components of the studied semi-algebraic set and the components of semi-algebraic sets defined by polynomial families obtained by the elimination of variables. It is doubly exponential in the number of variables and its best implementations are limited to problems in 3 or 4 variables. Since the end of the eighties, alternative strategies (see [55], [45] and references therein) with a single exponential complexity in the number of variables have been developed. They are based on the progressive construction of the following subroutines:
(a) solving zero-dimensional systems: this can be performed by computing a lexicographical Grobner basis;
(b) computing sampling points in a real hypersurface: after some infinitesimal deformations, this is reduced to problem (a) by computing the critical locus of a polynomial mapping reaching its extrema on each connected component of the real hypersurface;
(c) computing sampling points in a real algebraic variety defined by a polynomial system: this is reduced to problem (b) by considering the sum of squares of the polynomials;
(d) computing sampling points in a semi-algebraic set: this is reduced to problem (c) by applying an infinitesimal deformation.

On the one hand, the relevance of this approach is based on the fact that its complexity is asymptotically optimal. On the other hand, some important algorithmic developments have been necessary to obtain efficient implementations of subroutines (b) and (c).

During the last years, we focused on providing efficient algorithms solving the problems (b) and (c). The used method rely on finding a polynomial mapping reaching its extrema on each connected component of the studied variety such that its critical locus is zero-dimensional. For example, in the case of a smooth hypersurface whose real counterpart is compact choosing a projection on a line is sufficient. This method is called in the sequel the critical point method. We started by studying problem (b) [65]. Even if we showed that our solution may solve new classes of problems ([66]), we have chosen to skip the reduction to problem (b), which is now considered as a particular case of problem (c), in order to avoid an artificial growth of degree and the introduction of singularities and infinitesimals.
Putting the critical point method into practice in the general case requires to drop some hypotheses. First, the compactness assumption, which is in fact intimately related to an implicit properness assumption, has to be dropped. Second, algebraic characterizations of critical loci are based on assumptions of non-degeneracy on the rank of the Jacobian matrix associated to the studied polynomial system. These hypotheses are not satisfied as soon as this system defines a non-radical ideal and/or a non equidimensional variety, and/or a non-smooth variety. Our contributions consist in overcoming efficiently these obstacles and several strategies have been developed [2], [7].
The properness assumption can be dropped by considering the square of a distance function to a generic point instead of a projection function: indeed each connected component contains at least a point minimizing locally this function. Performing a radical and equidimensional decomposition of the ideal generated by the studied polynomial system allows to avoid some degeneracies of its associated Jacobian matrix. At last, the recursive study of overlapped singular loci allows to deal with the case of non-smooth varieties. These algorithmic issues allow to obtain a first algorithm [2] with reasonable practical performances.
Since projection functions are linear while the distance function is quadratic, computing their critical points is easier. Thus, we have also investigated their use. A first approach [7] consists in studying recursively the critical locus of projection functions on overlapped affine subspaces containing coordinate axes combined with the study of their set of non-properness. A more efficient one [67], avoiding the study of sets of non-properness is obtained by considering iteratively projections on *generic* affine subspaces restricted to the studied variety and fibers on arbitrary points of these subspaces intersected with the critical locus of the corresponding projection. The underlying algorithm is the most efficient we obtained.

In terms of complexity, we have proved in [68] that when the studied polynomial system generates a radical ideal and defines a smooth algebraic variety, the output of our algorithms is smaller than what could be expected by applying the classical Bèzout bound and than the output of the previous algorithms. This has also given new upper bounds on the number of connected components of a smooth real algebraic variety which improve the classical Thom-Milnor bound. The technique we used, also allows to prove that the degree of the critical locus of a projection function is inferior or equal to the degree of the critical locus of a distance function. Finally, it shows how to drop the assumption of equidimensionality required in the aforementioned algorithms.

3.4.2. Parametric systems

Most of the applications we recently solved (celestial mechanics, cuspidal robots, statistics, etc.) require the study of semi-algebraic systems depending on parameters. Although we covered these subjects in an independent way, some general algorithms for the resolution of this type of systems can be proposed from these experiments.

The general philosophy consists in studying the generic solutions independently from algebraic subvarieties (which we call from now on discriminant varieties) of dimension lower than the semi-algebraic set considered. The study of the varieties thus excluded can be done separately to obtain a complete answer to the problem, or is simply neglected if one is interested only in the generic solutions, which is the case in some applications.

We recently proposed a new framework for studying basic constructible (resp. semi-algebraic) sets defined as systems of equations and inequations (resp. inequalities) depending on parameters. Let's consider the basic semi-algebraic set

$$\mathcal{S} = \{x \in \mathbb{R}^n \ , \ p_1(x) = 0, ..., p_s(x) = 0, f_1(x) > 0, ...f_s(x) > 0\}$$

and the basic constructible set

$$\mathcal{C} = \{x \in \mathbb{C}^n \ , \ p_1(x) = 0, ..., p_s(x) = 0, f_1(x) \neq 0, ...f_s(x) \neq 0\}$$

where p_i, f_j are polynomials with rational coefficients.

- $[U, X] = [U_1, ...U_d, X_{d+1}, ...X_n]$ is the set of *indeterminates* or variables, $U = [U_1, ...U_d]$ is the set of *parameters* and $X = [X_{d+1}, ...X_n]$ the set of *unknowns*;
- $\mathcal{E} = \{p_1, ...p_s\}$ is the set of polynomials defining the equations;
- $\mathcal{F} = \{f_1, ...f_l\}$ is the set of polynomials defining the inequations in the complex case (resp. the inequalities in the real case);
- For any $u \in C^d$ let ϕ_u be the specialization $U \longrightarrow u$;
- $\Pi_U : \mathbb{C}^n \longrightarrow \mathbb{C}^d$ denotes the canonical projection on the parameter's space $(u_1, \cdots, u_d, x_{d+1}, ..., x_n) \longrightarrow (u_1, \cdots, u_d)$;
- Given any ideal I we denote by $\mathbf{V}(I) \subset \mathbb{C}^n$ the associated (algebraic) variety. If a variety is defined as the zero set of polynomials with coefficients in $\mathbb{Q}$ we call it a $\mathbb{Q}$-algebraic variety; we extend naturally this notation in order to talk about $\mathbb{Q}$-irreducible components, $\mathbb{Q}$-Zariski closure, etc.
- for any set $\mathcal{V} \subset \mathbb{C}^n$, $\overline{\mathcal{V}}$ will denote its $\mathbb{C}$-Zariski closure in $\mathbb{C}^n$.

In most applications, $\mathbf{V}(< \phi_u(\mathcal{E}) >)$) as well as $\phi_u(\mathcal{C}) = \Pi_U^{-1}(u) \bigcap \mathcal{C}$ are finite and not empty for almost all parameter's u. Most algorithms that study $\mathcal{C}$ or $\mathcal{S}$ (number of real roots w.r.t. the parameters, parameterizations of the solutions, etc.) compute in any case a $\mathbb{Q}$-Zariski closed set $W \subset C^d$ such that for any $u \in \mathbb{C}^d \setminus W$, there exists a neighborhood $\mathcal{U}$ of u with the following properties :

- $(\Pi_U^{-1}(\mathcal{U}) \bigcap \mathcal{C}, \Pi_U)$ is an analytic covering of $\mathcal{U}$; this implies that the elements of $\mathcal{F}$ do not vanish (and so have constant sign in the real case) on the connected components of $\Pi_U^{-1}(\mathcal{U}) \bigcap \mathcal{C}$;

We recently [6] show that the parameters' set such that there doesn't exist any neighborhood $\mathcal{U}$ with the above analytic covering property is a $\mathbb{Q}$-Zariski closed set which can exactly be computed. We name it the *minimal discriminant variety of* $\mathcal{C}$ *with respect to* Π_U and propose also a definition in the case of non generically zero-dimensional systems.

Being able to compute the minimal discriminant variety allows to simplify the problem depending on n variables to a similar problem depending on d variables (the parameters) : it is sufficient to describe its complementary in the parameters' space (or in the closure of the projection of the variety in the general case) to get the full information about the generic solutions (here generic means for parameters' values outside the discriminant variety).

Then being able to describe the connected components of the complementary of the discriminant variety in $\mathbb{R}^d$ becomes a main challenge which is strongly linked to the work done on positive dimensional systems. Moreover, rewriting the systems involved and solving zero-dimensional systems are major components of the algorithms we plan to build up.

We currently propose several computational strategies. An a priori decomposition into equidimensional components as zeros of radical ideals simplifies the computation and the use of the discriminant varieties. This preliminary computation is however sometimes expensive, so we are developing adaptive solutions where such decompositions are called by need. The main progress is that the resulting methods are fast on easy problems (generic) and slower on the problems with strong geometrical contents.

The existing implementations of algorithms able to "solve" (to get some information about the roots) parametric systems do all compute (directly or indirectly) discriminant varieties but none computes optimal objects (strict discriminant variety). This is the case, for example of the Cylindrical Algebraic Decomposition adapted to $\mathcal{E} \bigcup \mathcal{F}$ [48], of algorithms based on "Comprehensive Gröbner bases" [72], [73], [71] or of methods that compute parameterizations of the solutions (see [69] for example). The consequence is that the output (case distinctions w.r.t. parameters' values) are huge compared with the results we can provide.

3.5. Cryptography

Participants: J.-C. Faugère, L. Perret, G. Renault, L. Bettale.

A fundamental problem in cryptography is to evaluate the security of cryptosystems against the most powerful techniques. To this end, several *general* methods have been proposed: linear cryptanalysis, differential cryptanalysis, *etc* ... *Algebraic cryptanalysis* is another general method which permits to study the security of the main public-key and secret-key cryptosystems.

Algebraic cryptanalysis can be described as a general framework that permits to asses the security of a wide range of cryptographic schemes. In fact the recent proposal and development of algebraic cryptanalysis is now widely considered as an important breakthrough in the analysis of cryptographic primitives. It is a powerful technique that applies potentially to a large range of cryptosystems. The basic principle of such cryptanalysis is to model a cryptographic primitive by a set of algebraic equations. The system of equations is constructed in such a way as to have a correspondence between the solutions of this system, and a secret information of the cryptographic primitive (for instance, the secret key of an encryption scheme).

Although the principle of algebraic attacks can probably be traced back to the work of Shannon, algebraic cryptanalysis has only recently been investigated as a cryptanalytic tool. To summarize algebraic attack is divided into two steps :

1. Modeling, i.e. representing the cryptosystem as a polynomial system of equations
2. Solving, i.e. finding the solutions of the polynomial system constructed in Step 1.

Typically, the first step leads usually to rather “big” algebraic systems (at least several hundreds of variables for modern block ciphers). Thus, solving such systems is always a challenge. To make the computation efficient, we usually have to study the structural properties of the systems (using symmetries for instance). In addition, one also has to verify the consistency of the solutions of the algebraic system with respect to the desired solutions of the natural problem. Of course, all these steps must be constantly checked against the natural problem, which in many cases can guide the researcher to an efficient method for solving the algebraic system.

Multivariate cryptography comprises any cryptographic scheme that uses multivariate polynomial systems. The use of such polynomial systems in cryptography dates back to the mid eighties [62], and was motivated by the need for alternatives to number theoretic-based schemes. Indeed, multivariate systems enjoy low computational requirements and can yield short signatures; moreover, schemes based on the hard problem of solving multivariate equations over a finite field are not concerned with the quantum computer threat, whereas as it is well known that number theoretic-based schemes like RSA, DH, or ECDH are. Multivariate cryptosystems represent a target of choice for algebraic cryptanalysis due to their intrinsic multivariate repesentation.

The most famous multivariate public key scheme is probably the Hidden Field Equation (HFE) cryptosystem proposed by Patarin [63]. The basic idea of HFE is simple: build the secret key as a univariate polynomial $S(x)$ over some (big) finite field (often GF(2^n)). Clearly, such a polynomial can be easily evaluated; moreover, under reasonable hypotheses, it can also be “inverted” quite efficiently. By inverting, we mean finding any solution to the equation $S(x) = y$, when such a solution exists. The secret transformations (decryption and/or signature) are based on this efficient inversion. Of course, in order to build a cryptosystem, the polynomial S must be presented as a public transformation which hides the original structure and prevents inversion. This is done by viewing the finite field GF(2^n) as a vector space over GF(2) and by choosing two linear transformations of this vector space L_1 and L_2. Then the public transformation is the composition of L_1, S and L_2. Moreover, if all the terms in the polynomial $S(x)$ have Hamming weight 2, then it is obvious that all the (multivariate) polynomials of the public key are of degree two.

By using fast algorithms for computing Gröbner bases, it was possible to break the first HFE challenge [5] (real cryptographic size 80 bits and a symbolic prize of 500 US$) in only two days of CPU time. More precisely we have used the $F_5/2$ version of the fast F_5 algorithm for computing Gröbner bases (implemented in C). The algorithms available up to now (Buchberger) were extremely slow and could not have been used to break the code (they should have needed at least a few centuries of computation). The new algorithm is thousands of times faster than previous algorithms. Several matrices have to be reduced (Echelon Form) during the computation: the biggest one has no less than 1.6 million columns, and requires 8 gigabytes of memory. Implementing the algorithm thus required significant programming work and especially efficient memory management.

The weakness of the systems of equations coming from HFE instances can be *explained* by the algebraic properties of the secret key (work presented at Crypto 2003 in collaboration with A. Joux). From this study, it is possible to predict the maximal degree occurring in the Gröbner basis computation. This permits to establish precisely the complexity of the Gröbner attack and compare it with the theoretical bounds. The same kind of technique has since been used for successfully attacking other types of multivariate cryptosystems : IP [51], 2R [53], ℓ-IC [54], and MinRank [50].

On the one hand algebraic techniques have been successfully applied against a number of multivariate schemes and in stream cipher cryptanalysis. On the other hand, the feasibility of algebraic cryptanalysis remains the source of speculation for block ciphers, and an almost unexplored approach for hash functions. The scientific lock is that the size of the corresponding algebraic systems are so huge (thousands of variables and equations) that nobody is able to predict correctly the complexity of solving such polynomial systems. Hence one goal of the team is ultimately to design and implement a new generation of efficient algebraic cryptanalysis toolkits to be used against block ciphers and hash functions. To achieve this goal, we will investigate *non-conventional* approaches for modeling these problems.

4. Application Domains

4.1. Panorama

Applications are fundamental for our research for several reasons.

The first one is that they are the only source of fair tests for the algorithms. In fact, the complexity of the solving process depends very irregularly of the problem itself. Therefore, random tests do not give a right idea of the practical behavior of a program, and the complexity analysis, when possible, does not necessarily provide realistic information.

A second reason is that, as quoted above, we need real world problems to determine which specifications of algorithms are really useful. Conversely, it is frequently by solving specific problems through ad hoc methods that we found new algorithms with general impact.

Finally, obtaining successes with problems which are intractable by the other known approaches is the best proof for the quality of our work.

On the other hand, there is a specific difficulty. The problems which may be solved with our methods may be formulated in many different ways, and their usual formulation is rarely well suited for polynomial system solving or for exact computations. Frequently, it is not even clear that the problem is purely algebraic, because researchers and engineers are used to formulate them in a differential way or to linearize them.

Therefore, our software may not be used as black boxes, and we have to understand the origin of the problem in order to translate it in a form which is well suited for our solvers.

It follows that many of our results, published or in preparation, are classified in scientific domains which are different from ours, like cryptography, error correcting codes, robotics, signal processing, statistics or biophysics.

4.2. Robotic

The (parallel) manipulators we study are general parallel robots: the hexapods are complex mechanisms made up of six (often identical) kinematic chains, of a base (fixed rigid body including six joints or articulations) and of a platform (mobile rigid body containing six other joints). The design and the study of parallel robots require the resolution of direct geometrical models (computation of the absolute coordinates of the joints of the platform knowing the position and the geometry of the base, the geometry of the platform as well as the distances between the joints of the kinematic chains at the base and the platform) and inverse geometrical models (distances between the joints of the kinematic chains at the base and the platform knowing the absolute positions of the base and the platform).

Since the inverse geometrical models can be easily solved, we focus on the resolution of the direct geometrical models. The study of the direct geometrical model is a recurrent activity for several members of the project. One can say that the progress carried out in this field illustrates perfectly the evolution of the methods for the resolution of algebraic systems. The interest carried on this subject is old. The first work in which the members of the project took part in primarily concerned the study of the number of (complex) solutions of the problem [61], [60]. The results were often illustrated by Gröbner bases done with Gb software.

One of the remarkable points of this study is certainly the classification suggested in [52].

5. Software

5.1. FGb

Participant: J.C. Faugère [contact].

FGb/Gb is a powerful software for computing Gröbner bases; it is written in C/C++ (approximately 250000 lines counting the old *Gb* software).

5.2. FGb

Participant: Jean-Charles Faugere [correspondant].

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-salsa.lip6.fr/~jcf/Software/FGb/index.html.

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

5.3. RAGlib

Participant: M. Safey El Din [contact].

RAGLib is a Maple library for computing sampling points in semi-algebraic sets.

5.4. Epsilon

Participant: D. 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. Real Solving Polynomial Systems

In [20], we describe an algorithm (VQE) for a variant of the real quantifier elimination problem (QE). The variant problem requires the input to satisfy a certain extra condition, and allows the output to be almost equivalent to the input. The motivation/rationale for studying such a variant QE problem is that many quantified formulas arising in applications do satisfy the extra conditions. Furthermore, in most applications, it is sufficient that the output formula is almost equivalent to the input formula. The main idea underlying the algorithm is to substitute the repeated projection step of CAD by a single projection without carrying out a parametric existential decision over the reals. We find that the algorithm can tackle important and challenging problems, such as numerical stability analysis of the widely-used MacCormack's scheme. The problem has been practically out of reach for standard QE algorithms in spite of many attempts to tackle it. However the current implementation of VQE can solve it in about 12 hours. This paper extends the results reported at the conference ISSAC 2009.

We also focused on the interaction of real solving polynomial system with global optimization. Let $f \in \mathbb{Q}[X_1, ..., X_n]$ of degree D. Algorithms for solving the unconstrained global optimization problem $f^{\star} = \inf_{\mathbf{x} \in \mathbb{R}^n} f(\mathbf{x})$ are of first importance since this problem appears frequently in numerous applications in engineering sciences. This can be tackled by either designing appropriate quantifier elimination algorithms or by certifying lower bounds on $f^{\star}$ by means of sums of squares decompositions but there is no efficient algorithm for deciding if $f^{\star}$ is a minimum. The paper [41] is dedicated to this important problem. We design an algorithm that decides if $f^{\star}$ is reached over $\mathbb{R}^n$ and computes a point $\mathbf{x}^{\star} \in \mathbb{R}^n$ such that $f(\mathbf{x}^{\star}) = f^{\star}$ if such a point exists. If L is the length of a straight-line program evaluating f, a *probabilistic* version of the algorithm runs in time $\widetilde{O}(n^2(L+n^2)(D(D-1)^{n-1})^2)$. Experiments show its practical efficiency.

Global optimization problems can also be tackled by computing algebraic certificates of positivity through sums of squares decompositions. Let $f_1, \cdots, f_p$ and f be polynomials in $\mathbb{Q}[X_1, \cdots, X_n]$ and let $V = V(f_1, \cdots, f_p) \subset \mathbb{C}^n$ be the algebraic variety defined by $f_1 = \cdots = f_p = 0$ whose dimension is denoted by d. Assume in the sequel that the ideal $\langle f_1, ..., f_p \rangle$ is radical and equidimensional and that V is smooth. In [18], up to a generic linear change of variables, we construct families of polynomials $\mathsf{M}_0, ..., \mathsf{M}_d$ in $\mathbb{Q}[X_1, ..., X_n]$ such that $f(x) \geq 0$ for all $x \in V \cap \mathbb{R}^n$ if and only if f can written as a sum of squares of polynomials in $\mathbb{R}[X_1, ..., X_n]$ modulo $\langle \mathsf{M}_i \rangle$ for $0 \leq i \leq d$. Such an algebraic certificate of positivity is simpler than the more general Positivstellensatz in Real Algebra. It can be used to certify lower bounds on $f^{\star} = \inf_{x \in V \cap \mathbb{R}^n} f(x)$. Also, computing a numerical approximation of such certificates of positivity can be reformulated as a semidefinite program which can be solved efficiently. We provide numerical experiments showing the effectiveness of our approach.

In [25], we consider the problem of constructing roadmaps of real algebraic sets. This problem was introduced by Canny to answer connectivity questions and solve motion planning problems. Given s polynomial equations with rational coefficients, of degree D in n variables, Canny's algorithm has a Monte Carlo cost of $s^n \log(s) D^{O(n^2)}$ operations in $\mathbb{Q}$; a deterministic version runs in time $s^n \log(s) D^{O(n^4)}$. A subsequent improvement was due to Basu, Pollack and Roy, with an algorithm of deterministic cost $s^{d+1} D^{O(n^2)}$ for the more general problem of computing roadmaps of a semi-algebraic set ($d \leq n$ is the dimension of an associated object). We give a probabilistic algorithm of complexity $(nD)^{O(n^{1.5})}$ for the problem of computing a roadmap of a closed and bounded hypersurface V of degree D in n variables, with a finite number of singular points. Even under these extra assumptions, no previous algorithm featured a cost better than $D^{O(n^2)}$.

6.2. Zero dimensional Solve

Let $I \subset \mathbb{K}[x_1, ..., x_n]$ be a 0-dimensional ideal of degree D where $\mathbb{K}$ is a field. It is well-known that obtaining efficient algorithms for change of ordering of Gröbner bases of I is crucial in polynomial system solving. Through the algorithm *FGLM*, this task is classically tackled by linear algebra operations in $\mathbb{K}[x_1, ..., x_n]/I$. With recent progress on Gröbner bases computations, this step turns out to be the bottleneck of the whole solving process.

In [38], we present an efficient algorithm that takes advantage of the sparsity structure of multiplication matrices appearing during the change of ordering. This sparsity structure arises even when the input polynomial system defining I is dense. As a by-product, we obtain an implementation which is able to manipulate 0-dimensional ideals over a prime field of degree greater than 30000. It outperforms the *Magma/Singular/FGb* implementations of *FGLM*.

In [38], we investigate the particular but important shape position case. The obtained algorithm performs the change of ordering within a complexity $O(D(N_1 + n \log(D)))$, where N_1 is the number of nonzero entries of a multiplication matrix (the density of the matrix). This almost matches the complexity of computing the minimal polynomial of *one* multiplication matrix. Then, we address the general case and give corresponding complexity results. Our algorithm is dynamic in the sense that it selects automatically which strategy to use depending on the input. Its key ingredients are the Wiedemann algorithm to handle 1-dimensional linear recurrence (for the shape position case), and the Berlekamp–Massey–Sakata algorithm from Coding Theory to handle multi-dimensional linearly recurring sequences in the general case.

6.3. Solving structured systems

Solving multihomogeneous systems, as a wide range of *structured algebraic systems* occurring frequently in practical problems, is of first importance. Experimentally, solving these systems with Gröbner bases algorithms seems to be easier than solving homogeneous systems of the same degree. Nevertheless, the reasons of this behaviour are not clear. In [16], we focus on bilinear systems (i.e. bihomogeneous systems where all equations have bidegree $(1, 1)$). Our goal is to provide a theoretical explanation of the aforementioned experimental behaviour and to propose new techniques to speed up the Gröbner basis computations by using the multihomogeneous structure of those systems. The contributions are theoretical and practical.

First, we adapt the classical F_5 criterion to avoid reductions to zero which occur when the input is a set of bilinear polynomials. We also prove an explicit form of the Hilbert series of bihomogeneous ideals generated by generic bilinear polynomials and give a new upper bound on the degree of regularity of generic affine bilinear systems. This leads to new complexity bounds for solving bilinear systems. We propose also a variant of the F_5 Algorithm dedicated to multihomogeneous systems which exploits a structural property of the Macaulay matrix which occurs on such inputs. Experimental results show that this variant requires less time and memory than the classical homogeneous F_5 Algorithm. Lastly, we investigate the complexity of computing a Gröbner basis for the grevlex ordering of a generic 0-dimensional affine bilinear system over $k[x_1,...,x_{n_x},y_1,...,y_{n_y}]$. In particular, we show that this complexity is upper bounded by $O\left(\binom{n_x+n_y+\min(n_x+1,n_y+1)}{\min(n_x+1,n_y+1)}^{\omega}\right)$, which is polynomial in n_x+n_y (i.e. the number of unknowns) when $\min(n_x,n_y)$ is constant.

6.4. Structured Systems and Applications to Cryptanalysis

The Goppa Code Distinguishing (GCD) problem consists in distinguishing the matrix of a Goppa code from a random matrix. Up to now, it is widely believed that the GCD problem is a hard decisional problem. In [36], we present the first technique allowing to distinguish alternant and Goppa codes over any field. Our technique can solve the GCD problem in polynomial-time provided that the codes have rates sufficiently large. The key ingredient is an algebraic characterization of the key-recovery problem which reduces to the solving of a system of bi-homogeneous polynomial equations. The idea is to consider the dimension of the solution space of a linearized system deduced from the algebraic system describing the key-recovery. It turns out that experimentally this dimension depends on the type of code. Explicit formulas derived from extensive experimentations for the value of the dimension are provided for "generic" random, alternant, and Goppa code over any alphabet. Finally, we give explanations of these formulas in the case of random codes, alternant codes over any field and binary Goppa codes.

6.5. Algebraic Cryptanalysis

The Isomorphism of Polynomials (IP) is one of the most fundamental problems in multivariate public key cryptography (MPKC). In In [23], we introduce a new framework to study the counting problem associated to IP. Namely, we present tools of finite geometry allowing to investigate the counting problem associated to IP. Precisely, we focus on enumerating or estimating the number of isomorphism equivalence classes of homogeneous quadratic polynomial systems. These problems are equivalent to finding the scale of the key space of a multivariate cryptosystem and the total number of different multivariate cryptographic schemes respectively, which might impact the security and the potential capability of MPKC. We also consider their applications in the analysis of a specific multivariate public key cryptosystem. Our results not only answer how many cryptographic schemes can be derived from monomials and how big the key space is for a fixed scheme, but also show that quite many HFE cryptosystems are equivalent to a Matsumoto-Imai scheme.

In [34], we present a practical cryptanalysis of the Identification Scheme proposed by Patarin at Crypto 1996. This scheme relies on the hardness of the Isomorphism of Polynomial with One Secret (IP1S), and enjoys shorter key than many other schemes based on the hardness of a combinatorial problem (as opposed to number theoretic problems). We present two new deterministic algorithms to attack the IP1S problem, and we rigorously analyze their complexity and success probability. We show that they can solve a constant fraction of all the instances of degree two in polynomial time.

In [33], we investigate the security of a generalization of HFE (multivariate and odd-characteristic variants). We propose an improved version of the basic Kipnis-Shamir key recovery attack against HFE. We then generalize the Kipnis-Shamir attack to Multi-HFE. The attack reduces to solve a MinRank problem directly on the public key. This leads to an improvement of a factor corresponding to the square of the degree of the extension field. We used recent results on MinRank to show that our attack is polynomial in the degree of the extension field. It appears that multi-HFE is less secure than original HFE for equal-sized keys. Finally, adaptations of our attack overcome several variants (i.e. minus modifier and embedding). As a proof of concept, we have practically broken the most conservative parameters given by Chen, Chen, Ding,Werner and Yang in 9 days for 256 bits security. All in all, our results give a more precise picture on the (in)security of several variants of HFE proposed these last years.

In [31], we initiate the formal treatment of cryptographic constructions ("Polly Cracker") based on the hardness of computing remainders modulo an ideal. We start by formalising and studying the relation between the ideal remainder problem and the problem of computing a Gröbner basis. We show both positive and negative results. On the negative side, we define a symmetric Polly Cracker encryption scheme and prove that this scheme only achieves bounded CPA security under the hardness of the IR problem. Furthermore, we show that a large class of algebraic transformations cannot convert this scheme to a fully secure Polly Cracker-style scheme. On the positive side, we formalise noisy variants of the ideal related problems. These problems can be seen as natural generalisations of the LWE problem and the approximate GCD problem over polynomial rings. After formalising and justifying the hardness of the noisy assumptions we show that noisy encoding of messages results in a fully IND-CPA secure somewhat homomorphic encryption scheme. Together with a standard symmetric-to-asymmetric transformation for additively homomorphic schemes, we provide a positive answer to the long standing open problem of constructing a secure Polly Cracker-style cryptosystem reducible to the hardness of solving a random system of equations. Indeed, our results go beyond that by also providing a new family of somewhat homomorphic encryption schemes based on new, but natural, hard problems. Our results also imply that Regev's LWE-based public-key encryption scheme is (somewhat) multiplicatively homomorphic for appropriate choices of parameters.

6.6. Computer Algebra and Algorithmic Number Theory

The Elliptic Curve Discrete Logarithm Problem (ECDLP) has become the most attractive alternative to factoring for public key cryptography. Whereas subexponential factoring algorithms exist, solving the ECDLP in general can only be done in exponential time. Provided that a certain heuristic assumption holds, we present in [39] an index calculus algorithm solving ECDLP over any binary field $\mathbb{F}_q$ in time $O(2^{c\,n^{2/3}\log n})$, where c is a small constant. Our algorithm follows the index calculus method that was first introduced by Semaev and later developed by Gaudry and Diem. In particular, the main step consists in decomposing points of the curve with respect to an appropriately chosen factor basis. This part can be nicely reformulated as a purely algebraic problem consisting in finding solutions to a multivariate polynomial $\mathbf{f}(\mathbf{x_1},...,\mathbf{x_m}) = \mathbf{0}$ such that all the variables $\mathbf{x_i}$ belong to some vector subspace of $\mathbb{F}_q/\mathbb{F}_p$. We solve this problem by means of Gröbner basis techniques and analyse its complexity using the multihomogeneous structure of the equations. Even, if this paper is essentially theoretical and is not aiming for practical attacks, the new ideas developed here could be used to have practical attacks in the future. This of course represents a challenging open problem.

7. Contracts and Grants with Industry

7.1. Contract with Thalès

Participants: J.-C. Faugère [contact], G. Renault, C. Goyet.

The goal of this contract (including a CIFRE PhD grant) is to mix side chanel attacks (DPA) and algebraic cryptanalysis.

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR Jeunes Chercheurs "CAC"

Participants: L. Perret [contact], J.-C. Faugère, G. Renault.

The new contract CAC " Computer Algebra and Cryptography" begins in October 2009 for a period of 4 years. This project will investigate 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.

8.2. ANR "HPAC"

Participants: J.-C. Faugère [contact], L. Perret, G. Renault, M. Safey El Din.

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[2] 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.

8.3. ANR "GeoLMI"

Participants: J.-C. Faugère, M. Safey El Din [contact].

The GeoLMI project[3] 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.

8.3.1. European Initiatives

8.3.1.1. ECRYPT II - European Network of Excellence for Cryptology

Participants: J.C. Faugère [contact], L. Perret, G. Renault, L. Bettale.

ECRYPT II - European Network of Excellence for Cryptology II is a 4-year network of excellence funded within the Information & Communication Technologies (ICT) Programme of the European Commission's Seventh Framework Programme (FP7) under contract number ICT-2007-216676. It falls under the action line Secure, dependable and trusted infrastructures. ECRYPT II started on 1 August 2008. Its objective is to continue intensifying the collaboration of European researchers in information security. The ECRYPT II research roadmap is motivated by the changing environment and threat models in which cryptology is deployed, by the gradual erosion of the computational difficulty of the mathematical problems on which cryptology is based, and by the requirements of new applications and cryptographic implementations. Its main objective is to ensure a durable integration of European research in both academia and industry and to maintain and strengthen the European excellence in these areas. In order to reach this goal, 11 leading players have integrated their research capabilities within three virtual labs focusing on symmetric key algorithms (SymLab), public key

[2] http://hpac.gforge.inria.fr/
[3] http://homepages.laas.fr/henrion/geolmi/

algorithms and protocols (MAYA), and hardware and software implementations associate (VAMPIRE). They are joined by more than 20 adjoint members to the network who will closely collaborate with the core partners. The team joins the European Network of Excellence for Cryptology ECRYPT II this academic year as associate member.

8.3.2. International Initiatives

8.3.2.1. Royal Society Project

Participants: J.C. Faugère [contact], L. Perret, L. Bettale.

Royal Society Project with the Crypto team Royal Holloway, University of London, UK.

8.3.2.2. Joint LIAMA Project ECCA

ECCA (Exact/Certified Computation with Algebraic systems) is a LIAMA project (Reliable Software Theme) focusing on polynomial system solving. The partners are INRIA, CNRS, and CAS (Chinese Academy of Sciences). The general objectives of this project are mainly the same as those of *SALSA*.

8.3.2.3. ANR International Grant "EXACTA"

Participants: D. Wang [contact], J.-C. Faugère, D. Lazard, L. Perret, G. Renault, M. Safey El Din.

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 (2010–2012) 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.

8.3.3. Scientific Animation

8.3.3.1. Journals – Associate Editors and Program Committees

J.-C. Faugère is member of the editorial board of Journal "Mathematics in Computer Science" (Birkhäuser) and Journal "Cryptography and Communications – Discrete Structures, Boolean Functions and Sequences" (Springer); guest editor for special issues in Journal of Symbolic Computation (Elsevier) and Journal "Mathematics in Computer Science" (Birkhäuser).

M. Safey el Din is member of the editorial board of Journal of Symbolic Computation (Elsevier).

J.-C. Faugère is PC co-chair of the third SCC conference (Santander, 2012).

D. Wang is member of the editorial board of:

- 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 in China (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).
- Editor for the Book Series in Computational Science (published by Tsinghua University Press, Beijing).

M. Safey El Din was member of the program committees of the 36-th International Symposium on Symbolic and Algebraic Computation (San Jose, USA, June 8–11 2011) and the 13-th International Workshop on Computer Algebra in Scientific Computing (Kassel, Germany, September 5 - 9, 2011) and is member of the program committee of the 13-th International Workshop on Computer Algebra in Scientific Computing (Maribor, Slovenia, September 3 - 6, 2012).

D.Wang was member of the program committee of:

- Technical Session at ICCSA 2011 on Symbolic Computing for Dynamic Geometry (Santander, Spain, June 20–23, 2011),

8.3.3.2. Scientific visits and international seminar

M. Safey El Din was invited 2 weeks in July 2011 by L. Zhi at the Key Laboratory of Mechnanization and Mathematics (Chinese Academy of Sciences, Beijing China), 1 week at the department of Computer Science at Aarhus University (Denmark), 2 weeks in October 2011 by E. Schost at the Department of Computer Science at The University of Western Ontario (London, Canada). He is a co-organizer of the next National Days of Computer Algebra in 2012.

L. Perret was invited 2 weeks in 2011 (in July and December) by D. Lin at the SKLOIS (Chinese Academy of Sciences, Beijing China), 1 week (April, 2011) at the Stevens Institute (New-York, USA) by A. Miasnikov.

J.-C. Faugère was invited 1 week in July 2011 by D. Lin at the SKLOIS (Chinese Academy of Sciences, Beijing China).

8.3.3.3. Conferences (organization) and invited talks

J.-C. Faugère was plenary invited speaker at ECC 2011, the 15th workshop on Elliptic Curve Cryptography.

J.-C. Faugère, is member of the MEGA Advisory Board.

M. Safey El Din is co-organizer (with L. Zhi) of the First International Workshop on Certified and Reliable Computing, held in July 2011 at Nanning, China, co-organizer of the mini-symposia on Algebraic Complexity (with E. Schost) and Algorithms in Real Algebraic Geometry (with H. Hong) which have been held on the occasion of the SIAM conference on Applications of Algebraic Geometry (Raleigh, Oct. 2011).

M. Safey El Din was invited speaker at the mini-symposium on Algebraic Geometry and Optimization (SIAM conference on Optimization), the MaGIX conference (LIX, Palaiseau) and gave several talks in the mini-symposia organized during the SIAM Conference on Applications of Algebraic Geometry. He was also invited to give a talk at the joint Mathematics-Computer Science seminar at the University of Western Ontario and gave a talk at the first workshop of the GeoLMI project (Rennes, Nov. 2011).

J.-C. Faugère was invited speaker at the MaGIX conference (LIX, Palaiseau) and in the mini-symposium on Linear Algebra organized during the SIAM Conference on Applications of Algebraic Geometry (Raleigh, USA). He was also invited to give a talk at the joint Mathematics-Computer Science seminar at the University of Aarhus (Danmark).

8.3.3.4. Committees

J.-C. Faugère was a member of the evaluation committee (AERES) of the institut de mathématiques de Toulon et du Var.

M. Safey El Din is a designated member of the French National Council of the Universities (CNU).

J.-C. Faugère is member of the hiring committee in computer science at the <<Université Pierre et Marie Curie>>, <<Université de Toulon>> and <<Université Joseph Fourier>>.

8.3.4. Teaching

J.C. Faugère, L. Perret give a course on Polynomial System Solving, Computer Algebra and Applications at the “Master Parisien de Recherche en Informatique” (MPRI).

G. Renault gives a course on Computational Number Theory and Cryptology at the <<Master d’Informatique de l’Université Paris 6>>.

9. Bibliography

Major publications by the team in recent years

[1] P. Aubry, D. Lazard, M. Moreno-Maza. *On the theories of triangular sets*, in "Journal of Symbilic Computation", 1999, vol. 28, p. 105-124.

[2] P. Aubry, F. Rouillier, M. Safey El Din. *Real Solving for Positive Dimensional Systems*, in "Journal of Symbolic Computation", 2002, vol. 34, n^{o} 6, p. 543–560.

[3] J.-C. Faugère. *A new efficient algorithm for computing Gröbner bases without reduction to zero F_5*, in "International Symposium on Symbolic and Algebraic Computation Symposium - ISSAC 2002", Villeneuve d'Ascq, France, Jul 2002.

[4] J.-C. Faugère. *A New Efficient Algorithm for Computing Gröbner bases (F_4)*, in "Journal of Pure and Applied Algebra", June 1999, vol. 139, n^{o} 1-3, p. 61-88.

[5] J.-C. Faugère, A. Joux. *Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases*, in "CRYPTO 2003", 2003, p. 44-60.

[6] D. Lazard, F. Rouillier. *Solving parametric polynomial systems*, in "Journal of Symbolic Computation", 2007, vol. 42, p. 636-667.

[7] M. Safey El Din, E. Schost. *Polar varieties and computation of one point in each connected component of a smooth real algebraic set*, in "International Symposium on Symbolic and Algebraic Computation 2003 - ISSAC'2003", Philadelphie, USA, J. Sendra (editor), ACM Press, aug 2003, p. 224-231.

[8] D. Wang. *Elimination Methods*, Springer-Verlag, Wien New York, 2001.

Publications of the year

Doctoral Dissertations and Habilitation Theses

[9] L. Bettale. *Cryptanalyse algébrique : outils et applications*, Université Paris 6, 2011.

[10] Y. Liang. *Approximate Gröbner Bases*, Université Paris 6 and Beihang University, 2011.

[11] W. Niu. *Analyse Qualitative des Systèmes Biologiques par des Méthodes Algébriques*, Université Paris 6, 2011.

Articles in International Peer-Reviewed Journal

[12] X. Chen, D. Wang. *Management of Geometric Knowledge in Textbooks*, in "Data and Knowledge Engineering", 2011, p. 1–15, In press, http://dx.doi.org/10.1016/j.datak.2011.10.004.

[13] J.-C. Faugère, Y. Liang. *Artificial discontinuities of single-parametric Gröbner bases*, in "Journal of Symbolic Computation", 2011, vol. 46, n^{o} 4, p. 459 – 466 [*DOI :* 10.1016/j.jsc.2010.11.001], http://www-salsa.lip6.fr/~jcf/Papers/JSC_LP10.pdf.

[14] J.-C. FAUGÈRE, Y. LIANG. *Pivoting in Extended Rings for Computing Approximate Gröbner Bases*, in "Mathematics in Computer Science", 2011, vol. 5, p. 179-194 [*DOI :* 10.1007/S11786-011-0089-Y], http://www-salsa.lip6.fr/~jcf/Papers/MCS2011.pdf.

[15] J.-C. FAUGÈRE, D. LUBICZ, D. ROBERT. *Computing modular correspondences for abelian varieties*, in "Journal Of Algebra", 2011, vol. 343, n^{o} 1, p. 248 - 277 [*DOI :* 10.1016/J.JALGEBRA.2011.06.031], http://www-salsa.lip6.fr/~jcf/Papers/JAlgebra2011.pdf.

[16] J.-C. FAUGÈRE, M. SAFEY EL DIN, P.-J. SPAENLEHAUER. *Gröbner Bases of Bihomogeneous Ideals Generated by Polynomials of Bidegree (1,1): Algorithms and Complexity*, in "Journal of Symbolic Computation", 2011, vol. 46, n^{o} 4, p. 406–437, Available online 4 November 2010 [*DOI :* 10.1016/J.JSC.2010.10.014], http://www-salsa.lip6.fr/~jcf/Papers/JSC_FSS10.pdf.

[17] A. GALLIGO, A. POTEAUX. *Computing monodromy via continuation methods on random Riemann surfaces*, in "Theoretical Computer Science", 2011, vol. 412, n^{o} 16, p. 1492–1507, Symbolic and Numerical Algorithms [*DOI :* 10.1016/J.TCS.2010.11.047], http://www.sciencedirect.com/science/article/B6V1G-51MDSJP-5/2/798a2d9fedcde3f52382391e770e1a5a.

[18] A. GREUET, G. GUO, M. SAFEY EL DIN, L. ZHI. *Global optimization of polynomials restricted to a smooth variety using sums of squares*, in "Journal of Symbolic Computation", 2011, p. 1–19, to appear, http://www-salsa.lip6.fr/~safey/Articles/sos_vcg_final.pdf.

[19] A. HASHEMI, D. LAZARD. *Sharper complexity bounds for zero-dimensional Gröbner bases and polynomial system solving*, in "International Journal of Algebra and Computation (IJAC)", 2011, vol. 21, p. 703–713, http://dx.doi.org/10.1142/S0218196711006364.

[20] H. HONG, M. SAFEY EL DIN. *Variant Quantifier Elimination*, in "Journal of Symbolic Computation", 2011, p. 1–24, to appear, http://www-salsa.lip6.fr/~safey/Articles/vqe_jsc_final.pdf.

[21] Y. HUANG, D. WANG. *Computing Intersection and Self-intersection Loci of Parametrized Surfaces Using Regular Systems and Gröbner Bases*, in "Computer Aided Geometric Design", 2011, vol. 28, n^{o} 9, p. 566–581, http://dx.doi.org/10.1016/j.cagd.2011.09.002.

[22] X. LI, C. MOU, W. NIU, D. WANG. *Stability Analysis for Discrete Biological Models Using Algebraic Methods*, in "Mathematics in Computer Science", 2011, vol. 5, n^{o} 3, p. 247–262, http://dx.doi.org/10.1007/s11786-011-0096-z.

[23] D. LIN, J.-C. FAUGÈRE, L. PERRET, T. WANG. *On enumeration of polynomial equivalence classes and their application to MPKC*, in "Finite Fields and Their Applications", 2011, p. 1–20 [*DOI :* DOI:10.1016/J.FFA.2011.09.001], http://www-salsa.lip6.fr/~jcf/Papers/FFA2011.pdf.

[24] A. POTEAUX, M. RYBOWICZ. *Complexity bounds for the rational Newton-Puiseux algorithm over finite fields*, in "Applicable Algebra in Engineering, Communication and Computing", 2011, vol. 22, p. 187–217, http://dx.doi.org/10.1007/s00200-011-0144-6.

[25] M. SAFEY EL DIN, E. SCHOST. *A Baby Steps/Giant Steps Probabilistic Algorithm for Computing Roadmaps in Smooth Bounded Real Hypersurface*, in "Discrete and Computational Geometry", 2011, vol. 45, n^{o} 1, p. 181–220 [*DOI :* 10.1007/S00454-009-9239-2], http://www-salsa.lip6.fr/~safey/Articles/SaSc09.pdf.

[26] D. WANG. *Algebraic Analysis of Stability and Bifurcation for Nonlinear Flight Dynamics*, in "The Aeronautical Journal", 2011, vol. 115, n^{o} 1168, p. 345–349.

[27] T. ZHAO, D. WANG, H. HONG. *Solution Formulas for Cubic Equations Without or With Constraints*, in "Journal of Symbolic Computation", 2011, vol. 46, n^{o} 8, p. 904–918, http://dx.doi.org/10.1016/j.jsc.2011.02.001.

Articles in National Peer-Reviewed Journal

[28] X. LI, D. WANG. *Simple Decomposition of Polynomial Sets over Finite Fields (in Chinese)*, in "Journal of Systems Science and Mathematical Sciences", 2011, p. 1–13, In press.

International Conferences with Proceedings

[29] M. ALBRECHT, C. CID, T. DULIEN, J.-C. FAUGÈRE, L. PERRET. *Algebraic Precomputations in Differential Cryptanalysis*, in "Information Security and Cryptology: 6th International Conference, Inscrypt 2010, Revised Selected Papers", X. LAI, M. YUNG, D. LIN (editors), Springer Berlin / Heidelberg, October 2011, vol. 6584, p. 387-403 [*DOI :* 10.1007/978-3-642-21518-627], http://www-salsa.lip6.fr/~jcf/Papers/INSCRYPT2010.pdf.

[30] M. ALBRECHT, P. FARSHIM, K. PATERSON, G. WATSON. *On Cipher-Dependent Related-Key Attacks in the Ideal Cipher Model*, in "Fast Software Encryption 2011, FSE", Lecture Notes in Computer Science, Springer, 2011, p. 1–20.

[31] M. ALBRECHT, J.-C. FAUGÈRE, P. FARSHIM, L. PERRET. *Polly Cracker, Revisited*, in "Advances in Cryptology Asiacrypt 2011", D. LEE, X. WANG (editors), Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 2011, vol. 7073, p. 179–196 [*DOI :* 10.1007/978-3-642-25385-010], http://www-salsa.lip6.fr/~jcf/Papers/Asia2011.pdf.

[32] F. ARMKNECHT, D. AUGOT, L. PERRET, A. SADEGHI. *On Constructing Homomorphic Encryption Schemes from Coding Theory*, in "IMA Int. Conf.", 2011, p. 23-40, http://dx.doi.org/10.1007/978-3-642-25516-8_3.

[33] L. BETTALE, J.-C. FAUGÈRE, L. PERRET. *Cryptanalysis of Multivariate and Odd-Characteristic HFE Variants*, in "Public Key Cryptography - PKC 2011", D. CATALANO, N. FAZIO, R. GENNARO, A. NICOLOSI (editors), Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 2011, vol. 6571, p. 441–458 [*DOI :* 10.1007/978-3-642-19379-827], http://www-salsa.lip6.fr/~jcf/Papers/pkc2011a.pdf.

[34] C. BOUILLAGUET, J.-C. FAUGÈRE, P.-A. FOUQUE, L. PERRET. *Practical Cryptanalysis of the Identification Scheme Based on the Isomorphism of Polynomial with One Secret Problem*, in "Public Key Cryptography - PKC 2011", D. CATALANO, N. FAZIO, R. GENNARO, A. NICOLOSI (editors), Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 2011, vol. 6571, p. 473-493 [*DOI :* 10.1007/978-3-642-19379-829], http://www-salsa.lip6.fr/~jcf/Papers/BFFP11.pdf.

[35] X. CHEN, Y. HUANG, D. WANG. *On the Design and Implementation of a Geometric Knowledge Base*, in "Automated Deduction in Geometry", Berlin Heidelberg, T. STURM, C. ZENGLER (editors), Lecture Notes in Artificial Intelligence, Springer-Verlag, 2011, vol. 6301, p. 22–41, http://dx.doi.org/10.1007/978-3-642-21046-4_2.

[36] J.-C. FAUGÈRE, A. GAUTHIER-UMAÑA, L. PERRET, J.-P. TILLICH. *A Distinguisher for High Rate McEliece Cryptosystems*, in "Information Theory Workshop (ITW), 2011 IEEE", oct. 2011, p. 282 -286 [*DOI :* 10.1109/ITW.2011.6089437], http://www-salsa.lip6.fr/~jcf/Papers/ITW2011.pdf.

[37] J.-C. FAUGÈRE, D. GLIGOROSKI, E. JENSEN, R. ODEGARD, L. PERRET, S. JOHAN KNAPSKOG, S. MARKOVSKI. *An Ultra-fast and Provably CMA Resistant Digital Signature Scheme*, in "The Third International Conference on Trusted Systems - INTRUST 2011", Y. MOTI, C. LIQUN, Z. LIEHUANG (editors), Lecture Notes in Computer Science, Springer Verlag, 2011, p. 1–10.

[38] J.-C. FAUGÈRE, C. MOU. *Fast Algorithm for Change of Ordering of Zero-dimensional Gröbner Bases with Sparse Multiplication Matrices*, in "Proceedings of the 36th international symposium on Symbolic and algebraic computation", New York, NY, USA, ISSAC '11, ACM, 2011, p. 115–122 [*DOI :* 10.1145/1993886.1993908], http://www-salsa.lip6.fr/~jcf/Papers/FM11.pdf.

[39] J.-C. FAUGÈRE, L. PERRET, C. PETIT, G. RENAULT. *Improving the Complexity of Index Calculus Algorithms in Elliptic Curves over Binary Field*, in "Proceedings of Eurocrypt 2012", Lecture Notes in Computer Science, Springer Verlag, 2012, p. 1–15.

[40] C. GOYET, J.-C. FAUGÈRE, G. RENAULT. *Algebraic Side Channel Analysis*, in "COSADE'11: The 2nd International Workshop on Constructive Side-Channel Analysis and Secure Design", Fraunhofer SIT, 2011, p. 1–6.

[41] A. GREUET, M. SAFEY EL DIN. *Deciding reachability of the infimum of a multivariate polynomial*, in "ISSAC '11: Proceedings of the 2011 international symposium on Symbolic and algebraic computation", New York, NY, USA, ISSAC '11, ACM, 2011, p. 131–138, http://doi.acm.org/10.1145/1993886.1993910.

[42] T. ZHAO, D. WANG, H. HONG, P. AUBRY. *Real Solution Formulas of Cubic and Quartic Equations Applied to Generate Dynamic Diagrams with Inequality Constraints*, in "SAC 2012: Proceedings of the 27th ACM Symposium on Applied Computing", Riva del Garda/Trento, Italy, ACM Press, March 2012, p. 1–8, In press.

Scientific Books (or Scientific Book chapters)

[43] *Proceedings of the 13th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC 2011)*, IEEE Computer Society, Timisoara, Romania, September 2011, p. 1–400.

[44] D. WANG, C. MOU, X. LI, J. YANG, M. JIN, Y. HUANG. *Polynomial Algebra (in Chinese)*, Higher Education Press, 2011, isbn: 9787040316988.

References in notes

[45] S. BASU, R. POLLACK, M.-F. ROY. *A new algorithm to find a point in every cell defined by a family of polynomials*, in "Quantifier elimination and cylindrical algebraic decomposition", Springer-Verlag, 1998.

[46] B. BUCHBERGER. *"Groebner bases : an algorithmic method in polynomial ideal theory"*, Recent trends in multidimensional systems theory, Reider ed. Bose, 1985.

[47] B. BUCHBERGER, G.-E. COLLINS, R. LOOS. *Computer Algebra Symbolic and Algebraic Computation*, second edition, Springer-Verlag, 1982.

[48] G.-E. COLLINS. *Quantifier elimination for real closed fields by cylindrical algebraic decomposition*, in "Springer Lecture Notes in Computer Science 33", 1975, vol. 33, p. 515-532.

[49] J.-C. FAUGÈRE, P. GIANNI, D. LAZARD, T. MORA. *Efficient Computation of Zero-Dimensional Gröbner Basis by Change of Ordering*, in "Journal of Symbolic Computation", Oct. 1993, vol. 16, n^{O} 4, p. 329–344.

[50] J.-C. FAUGÈRE, F. LEVY-DIT-VEHEL, L. PERRET. *Cryptanalysis of Minrank*, in "Advances in Cryptology CRYPTO 2008", Santa-Barbara, USA, D. WAGNER (editor), Lecture Notes in Computer Science, Springer-Verlag, 2008, vol. 5157, p. 280–296.

[51] J.-C. FAUGÈRE, L. PERRET. *Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects*, in "Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques", Lecture Notes in Computer Science, Springer, 2007, vol. 4004, p. 30-47.

[52] J.-C. FAUGÈRE, D. LAZARD. *The Combinatorial Classes of Parallel Manipulators*, in "Mechanism and Machine Theory", 1995, vol. 30, p. 765–776.

[53] J.-C. FAUGÈRE, L. PERRET. *Cryptanalysis of $2R^{-}$ Schemes*, in "Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference", Lecture Notes in Computer Science, Springer, 2007, vol. 4117, p. 357-372.

[54] P.-A. FOUQUE, G. MACARIORAT, L. PERRET, J. STERN. *On the Security of the ℓ-IC Signature Scheme*, in "Public Key Cryptography, 4th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2008", Lecture Notes in Computer Science, Springer, 2008, vol. 4939, p. 1–17.

[55] D. GRIGOR'EV, N. VOROBJOV. *Solving Systems of Polynomial Inequalities in Subexponential Time*, in "J. Symbolic Comput.", 1988, vol. 5, p. 37–64.

[56] M. KALKBRENNER. *Three contributions to elimination theory*, Johannes Kepler University, Linz, 1991.

[57] D. LAZARD. *Resolution of polynomial systems*, in "4th Asian Symposium on Computer Mathematics - ASCM 2000", Chiang Mai, Thailand, Lecture Notes Series on Computing, World Scientific, Dec 2000, vol. 8, p. 1 - 8.

[58] D. LAZARD. *On the specification for solvers of polynomial systems*, in "5th Asian Symposium on Computers Mathematics -ASCM 2001", Lecture Notes Series in Computing, World Scientific, 2001, vol. 9, p. 66-75.

[59] D. LAZARD. *Solving Zero - dimensional algebraic systems*, in "Journal of Symbolic Computation", 1992, vol. 13, p. 117-132.

[60] D. LAZARD. *Stewart platforms and Gröbner basis*, in "Proceedings of Advances in Robotics Kinematics", Sep 1992, p. 136-142.

[61] D. LAZARD, J.-P. MERLET. *The (true) Stewart platform has 12 configurations*, in "Proc. of IEEE Conference on Robotics and Vision", San Diego, 1994.

[62] T. MATSUMOTO, H. IMAI. *Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption*, in "Advances in Cryptology: EUROCRYPT 1988", Lecture Notes in Computer Science, Springer-Verlag, 1988, vol. 330, p. 497–506.

[63] J. PATARIN. *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of Asymmetric Algorithms*, in "Advances in Cryptology: EUROCRYPT 1996", Lecture Notes in Computer Science, Springer-Verlag, 1996, vol. 1070, p. 33-48.

[64] J.-F. RITT. *Differential equations from an algebraic standpoint*, in "American Mathematical Society Colloquium Publications", 1932, vol. 14.

[65] F. ROUILLIER, M.-F. ROY, M. SAFEY EL DIN. *Finding at least one point in each connected component of a real algebraic set defined by a single equation*, in "Journal of Complexity", 2000, vol. 16, p. 716–750.

[66] F. ROUILLIER, M. SAFEY EL DIN, E. SCHOST. *Solving the Birkhoff Interpolation Problem via the Critical Point Method: An Experimental Study*, in "Automated Deduction in Geometry - Third International Workshop ADG 2000, Zurich Switzerland, September 2000, Revised Papers", J. RICHTER-GEBERT, D. WANG (editors), Lecture Notes in Artificial Intelligence, Springer, 2001, n^o 2061, p. 26–40.

[67] M. SAFEY EL DIN, E. SCHOST. *Properness defects of projection functions and computation of at least one point in each connected component of a real algebraic set*, in "Journal of Discrete and Computational Geometry", sep 2004.

[68] M. SAFEY EL DIN, P. TRÉBUCHET. *Strong bihomogeneous Bézout theorem and degree bounds for algebraic optimization*, INRIA, 2004, n^o 5071, submitted to Journal of Pure and Applied Algebra, http://hal.inria.fr/inria-00071512.

[69] E. SCHOST. *Computing Parametric Geometric Resolutions*, in "Applicable Algebra in Engineering, Communication and Computing", 2003, vol. 13, n^o 5, p. 349 - 393.

[70] D. WANG. *An Elimination Method for Polynomial Systems*, in "Journal of Symbolic Computation", 1993, vol. 16, p. 83–114.

[71] V. WEISPFENNING. *Canonical comprehensive Gröbner bases*, in "Proceedings of the 2002 international symposium on Symbolic and algebraic computation", ACM Press, 2002, p. 270–276, http://doi.acm.org/10.1145/780506.780541.

[72] V. WEISPFENNING. *Comprehensive Gröbner bases*, in "Journal of Symbolic Computation", 1992, vol. 14, p. 1–29.

[73] V. WEISPFENNING. *Solving parametric polynomial equations and inequalities by symbolic algorithms*, World Scientific, 1995.

[74] L. YANG, J. ZHANG. *Searching dependency between algebraic equations: an algorithm applied to automated reasoning*, in "Artificial intelligence in mathematics", J. JOHNSON, S. MCKEE, A. VELLA (editors), Oxford University Press, 1994, p. 147–156.