INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team salsa

Solvers for Algebraic Systems and Applications

Paris - Rocquencourt

Theme : Algorithms, Certification, and Cryptography

Activity Report

2010

Table of contents

1. Team

Research Scientists

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

Faculty Members

Pierre-Vincent Koseleff [On leave from Univ. Pierre et Marie Curie]
Daniel Lazard [Emeritus Professor, HdR]
Ludovic Perret [Assistant Professor - Univ. Pierre et Marie Curie]
Guénael Renault [Assistant Professor - Univ. Pierre et Marie Curie]
Mohab Safey El Din [On leave from Univ. Pierre et Marie Curie, HdR]

PhD Students

Ye Liang [China Scholarship Council - defense in 2010 - J.-C. Faugère/D. Wang]
Wei Niu [China Scholarship Council - defense in 2010 - D. Wang]
Chenqi Mou [China Scholarship Council - defense in 2012 - J.-C. Faugère/D. Wang]
Luk Bettale [DGA - defense in 2012 - 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]

Post-Doctoral Fellows

Mate Soos [Sep 2009 - Nov 2010]
Martin Albrecht [Dec 2010 - Nov 2011]
Petit Cristophe [Dec 2010 - Nov 2011]
Adrien Poteaux [Sep 2010 - August 2011]

Visiting Scientist

Rune Ødegård [visiting PhD student]

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 Student Paper award at Issac 2010.
- **Computer Algebra**. New record of complexity for the roadmap.
- **Maple**. Maple 14 release : inclusion of the Raglib package.
- **Chinese-SALSA** : Joint LIAMA Project ECCA (Reliable Software Theme) INRIA/CNRS/UPMC/CAS.

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], [83], [82]. 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, F. Rouillier, M. Safey El Din, P.J. Spaenlehauer, D. Wang, R. Xiao.

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 $\sum_{k=1}^{R} P_k U_k$ 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 ([71], [70]). 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 ([89]) 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 [81] and [100]) 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], [9], [93].

In 1993, Wang [96] 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, F. Rouillier, 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 ([74]) : 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 [74].

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 [84] 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).

Our specificity is to carry out the computations until their term thanks to two types of results :

- the computation of the Rational Univariate Representation [7] : we proved that any zero-dimensional system, depending on variables $X_1, ...X_n$, can systematically be rewritten, without loss of information (multiplicities, real roots), in the form $f(T) = 0, X_i = g_i(T)/g(T), i = 1...n$ where the polynomials $f, g, g_1, ...g_n$ have coefficients in the same ground field as those of the system and where T is a new variable (independent from $X_1, ...X_n$).
- efficient algorithms for isolating and counting the real roots of univariate polynomials [8].

Thus, the use of innovative algorithms for Gröbner bases computations [4], [3], Rational Univariate representations ([74] for the "shape position" case and [7] for the general 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, G. Moroz, W. Niu, F. Rouillier, M. Safey El Din, D. Wang, R. Xiao, T. Zhao.

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 [72]. 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 [80], [69] 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 Rational Univariate Representation (see [7]);
(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) [91]. Even if we showed that our solution may solve new classes of problems ([92]), 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], [9].
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 [9] 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 [93], 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 [94] 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 $\mathcal{E} \bigcup \mathcal{F}$ [72], of algorithms based on "Comprehensive Gröbner bases" [98], [99], [97] or of methods that compute parameterizations of the solutions (see [95] 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 [87], 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 [88]. 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 [76], 2R [78], ℓ-IC [79], and MinRank [75].

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 [86], [85]. 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 [77]. The next efforts were related to the real roots and the effective computation of the solutions [90]. The studies then continued following the various algorithmic progresses, until the developed tools made possible to solve non-academic problems. In 1999, the various efforts were concretized by an industrial contract with the SME CMW (*Constructions Mécaniques des Vosges-Marioni*) for studying a robot dedicated to machine tools. Since 2002, we are interested in the study of singularities of manipulators (serial or parallel). The first results we obtained (characterization of all the cuspidal serial robots with 3 D.O.F.) have been computed using a very primary variant of the Discriminant Variety [73]. Since 2007, we are working on the singularities of parallel planar robots (ANR grand *SIROPA*).

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. RS

Participant: F. Rouillier [contact].

RS is a software entirely developed in C (150000 lines approximately) dedicated to the study of real roots of algebraic systems.

5.3. RAGlib

Participant: M. Safey El Din [contact].

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

5.4. DV

Participants: G. Moroz [contact], F. Rouillier [contact].

DV stands for *Discriminant Varieties* and is a software developped in Maple language, contains algorithms for computing Discriminant varieties, but also some variants of cylindrical algebraic decompositions (CAD).

5.5. 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

Discriminant varities are basic objects to compute for solving parametric systems of polynomial equations and inequalities. In [27], we show how to reduce this computation to the computation of the set of non-properness of a projection and we provide degree bounds on the minimal discriminant variety of a 0-dimensional parametric system under some assumptions.

Let $f \in \mathbb{Q}[X_1, ..., X_n]$. In [57], we prove that if $f \geq 0$ over the reals, up to a generic linear change of variables, it can be written as a sum of squares modulo the ideal generated by $n-1$ partial derivatives. This new kind of algebraic certificates of positivity is used to certify lower bounds on infima for unconstrained global optimization problems.

In [30], we provide an algorithm which, given a polynomial system of s n-variate polynomials of degree bounded by D and coefficients of bit-length dominated by τ defining a *convex* semi-algebraic set S, computes rational points in S. The bit complexity is $\tau^{O(1)}s^nD^{O(n^3)}$ and, in case of non-emptiness, the outputted points have bit length bounded by $\tau D^{O(n^3)}$. This result is used to prove upper bounds on the bit length of coefficients in sums of squares decompositions since such decompositions are obtained by computing rational points in convex semi-algebraic sets.

Let $V \subset \mathbb{R}^n$ be a smooth bounded real hypersurface whose set of singular points has dimension at most 0, defined by a polynomial of degree D. In [29], we provide an algorithm computing a *roadmap* of V, i.e. an algebraic curve having a non-empty and connected intersection with each connected component of V. The complexity of this algorithm is $(nD)^{O(n^{1.5})}$. Even under the considered assumptions, this result improves the best previous bound $D^{O(n^2)}$ obtained 20 years ago by J. Canny.

The above result is achieved by exploiting properties on polar varieties which are defined by the vanishing of some minors of truncated jacobian matrices. Sufficient conditions to ensure the smoothness (and other properties such as equidimensionality, etc.) of polar varieties are proved in [12].

6.2. Solving structured systems

Solving multihomogeneous systems, as a wide range of *structured algebraic systems* occurring frequently in practical problems, is of first importance. In [16], we focus on bilinear systems (i.e. bihomogeneous systems where all equations have bidegree $(1, 1)$). We 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. 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 $O\left(\begin{pmatrix} n_x + n_y + \min(n_x + 1, n_y + 1) \\ \min(n_x + 1, n_y + 1) \end{pmatrix}^{\omega}\right)$, which is polynomial in $n_x + n_y$ (i.e. the number of unknowns) when $\min(n_x, n_y)$ is constant.

Computing loci of rank defects of linear matrices (also called the MinRank problem) is a fundamental NP-hard problem of linear algebra which has applications in Cryptology, in Error Correcting Codes and in Geometry. Given a square linear matrix (i.e. a matrix whose entries are k-variate linear forms) of size n and an integer r, the problem is to find points such that the evaluation of the matrix has rank less than $r + 1$. In [54] we obtain the most efficient algorithm to solve this problem. To this end, we give the theoretical and practical complexity of computing Gröbner bases of two algebraic formulations of the MinRank problem. Both modelings lead to *structured algebraic systems*.

In [17], we settle conjectures, which are experimentally supported, on the monodromy generated by specific loops in the complex plane. Assuming them enables us to develop tools for getting fast probabilistic algorithms for absolute multivariate polynomial factorization, under the hypothesis that the factors behave like random polynomials whose coefficients follow uniform distributions.

6.3. Structured systems and applications to Cryptanalysis

In [49], [50], [51], we propose a new approach to investigate the security of the McEliece cryptosystem (based on error-correcting codes). Since its invention thirty years ago, no efficient attack had been devised that managed to recover the private key. We prove that the private key of the cryptosystem satisfies a system of bi-homogeneous polynomial equations. We have used these highly structured algebraic equations to mount an efficient key-recovery attack against two recent variants of the McEliece cryptosystems that aim at reducing public key sizes.

6.4. Algebraic Cryptanalysis

MQQ is a multivariate public key cryptosystem (MPKC) based on multivariate quadratic quasigroups and a special transform called "*Dobbertin transformation*" The security of MQQ, as well as any MPKC, reduces to the difficulty of solving a non-linear system of equations easily derived from the public key. It has been already observed that that the algebraic systems obtained are much easier to solve that random non-linear systems of the same size. In [47], [46], we go one step further in the analysis of MQQ. We explain why systems arising in MQQ are so easy to solve in practice.

In [42], we present an efficient cryptanalysis of the so-called HM cryptosystem which was published at Asiacrypt'1999, and one perturbed version of HM. Until now, this scheme was exempt from cryptanalysis. We first present a distinguisher which uses a differential property of the public key. This distinguisher permits to break one perturbed version of HM. After that, we describe a practical message-recovery attack against HM using Gröbner bases. The attack can be mounted in few hundreds seconds for recommended parameters. It turns out that algebraic systems arising in HM are easier to solve than random systems of the same size.

Even if Algebraic cryptanalysis have been successfully applied against a number of multivariate schemes and stream ciphers. Yet, their feasibility against block ciphers remains the source of much speculation. At FSE 2009 Albrecht and Cid proposed to combine differential cryptanalysis with algebraic attacks against block ciphers. The proposed attacks required Gröbner basis computations during the online phase of the attack. In [36], [37] we take a different approach and only perform Gröbner basis computations in a pre-computation (or offline) phase. In other words, we study how we can improve "classical" differential cryptanalysis using algebraic tools. We apply our techniques against the block ciphers PRESENT and KTANTAN.

In [38], we present an extended version of the hybrid approach [13], suitable for polynomials of higher degree. To easily access our tools, we provide a MAGMA package available at http://www-salsa.lip6.fr/~bettale/hybrid.html that provide all the necessary material to use our hybrid approach and to compute the complexities.

In [53], we fully break the Algebraic Surface Cryptosystem (ASC for short) proposed at PKC'2009. This result is rather surprising since the algebraic attack is often more efficient than the legal decryption algorithm.

6.5. Decomposition of Generic Multivariate Polynomials

In [55], we consider the composition $f = g \circ h$ of two systems $g = (g_0, ..., g_t)$ and $h = (h_0, ..., h_s)$ of homogeneous multivariate polynomials over a field $\mathbb{K}$, where each $g_j \in \mathbb{K}[y_0, ..., y_s]$ has degree ℓ, each $h_k \in \mathbb{K}[x_0, ..., x_r]$ has degree m, and $f_i = g_i(h_0, ..., h_s) \in \mathbb{K}[x_0, ..., x_r]$ has degree $n = \ell \cdot m$, for $0 \leq i \leq t$. The motivation of this paper is to investigate the behavior of the decomposition algorithm **MultiComPoly** proposed at ISSAC'09. We prove that the algorithm works correctly for generic decomposable instances – in the special cases where ℓ is 2 or 3, and m is 2 – and investigate the issue of uniqueness of a *generic* decomposable instance. The uniqueness is defined w.r.t. the "normal form" of a multivariate decomposition, a new notion introduced in this paper, which is of independent interest.

6.6. Triangular Sets - Decomposition

D. Wang [31] has applied algebraic methods to derive exact conditions for certain nonlinear flight dynamical systems to exhibit stability and bifurcation. The roll-coupling flight model has been taken as an example to show the feasibility of algebraic analysis. Some of the previous stability and bifurcation results obtained using numerical analysis for this model have been confirmed.

In [25], D. Wang and others have proposed algorithms for decomposing any zero-dimensional polynomial set into simple sets over an arbitrary finite field, with an associated ideal or zero decomposition. They have generalized the squarefree decomposition approach for univariate polynomials over a finite field to that over the field product determined by a simple set, based on a new technique to extract the pth root of any element in the field product. Experiments with a preliminary implementation show the effectiveness of their algorithms.

D. Wang and his co-authors [41] have designed a geometric knowledge base that stores standardized, formalized, and structured geometric knowledge data. They have adopted a key strategy that works by encapsulating certain interrelated knowledge data into knowledge objects and then organizing the knowledge objects according to the hierarchic structure of their relations. A geometric knowledge base system has been implemented, providing functionalities for creating, rendering, and managing knowledge data with basic query services.

6.7. Computer Algebra and Algorithmic Number Theory

In [44] we propose a new attack using an implicit hint on the famous number theory based cryptosystem RSA. In this work, we develop a new interaction between techniques coming from lattice reduction (e.g. LLL algorithm) and the elimination theory (e.g. Gröbner basis computation) in order to solve problems coming from cryptography.

The work [59] propose a constructive use of computer algebra in Algorithmic Number Theory wit application in Cryptography. More explicitly, techniques coming from univariate polynomial solving by radical (Algorithmic Galois Theory) is used for the construction of encoding in the set of points of elliptic and hyperelliptic curves defined over a finite field. Fixing a prime p verifing some antural assumptions, the general method proposed in [59] is the first one which provides deterministic polynomial time encoding into the rational points of all the elliptic curves and half of the genus 2 hyperelliptic curves defined over p. These two types of curves are the main objects for cryptography based on algebraic curves.

6.8. Efficient Implementations - High Performance Linear Algebra

FGb: a library for computing Gröbner bases has been presented at ICMS[32] in Japan. A key component of the efficiency of FGb is a dedicated linear algebra package: in [43], we present a new linear algebra package written in C which contains specific algorithms to compute Gaussian elimination as well as specific internal representation of matrices.

The Goppa Code Distinguishing (GD) problem consists in distinguishing the matrix of Goppa code from a random matrix. Up to now, it was widely believed that this problem is computationally hard. The hardness of this problem was a mandatory assumption to prove the security of code-based cryptographic primitives like McEliece's cryptosystem. In [48], we present a polynomial time distinguisher for alternant and Goppa codes of high rate over any field. The key ingredient is an algebraic technique already used to asses the security McEliece's cryptosystem.

6.9. Applications in computational geometry and robotics

In [60], [26], we investigate the existence conditions of cusp points in the design parameter space of the RPR-2PRR parallel manipulators. Cusp points make possible non-singular assemblymode changing motion, which can possibly increase the size of the aspect, i.e. the maximum singularity free workspace.

In [28], we revisit the problem of computing the topology and geometry of a real algebraic plane curve. The topology is of prime interest but geometric information, such as the position of singular and critical points, is also relevant. A challenge is to compute efficiently this information for the given coordinate system even if the curve is not in generic position. Previous methods based on the cylindrical algebraic decomposition (CAD) use sub-resultant sequences and computations with polynomials with algebraic coefficients. A novelty of our approach is to replace these tools by Gröbner basis computations and isolation with rational univariate representations. This has the advantage of avoiding computations with polynomials with algebraic coefficients, even in non-generic positions. Our algorithm isolates critical points in boxes and computes a decomposition of the plane by rectangular boxes. This decomposition also induces a new approach for computing an arrangement of polylines isotopic to the input curve. We also present an analysis of the complexity of our algorithm. An implementation of our algorithm demonstrates its efficiency, in particular on high-degree non-generic curves.

In [61], this work is kept on by providing an algorithm for isolating the real roots of bivariate polynomial systems which mixed different points of view depending on the geometric properties that are detected during the computations.

6.10. Polynomial Knots

Since Vassiliev (1990), we know that any knot admits a polynomial parametrization. A natural question is to give explicit and minimal parametrizations.

In [20] we show that every knot is a Chebyshev knot, that is to say, admits a polynomial parametrization $C(a,b,c,\phi) : x = T_a(t),\ y = T_b(t),\ z = T_c(t+\phi)$. Here T_n is the Chebyshev polynomial of degree n and ϕ is a real constant. We give explicit parametrizations of the torus knots $K_{2,2n+1}$: $x = T_3(t),\ y = T_{3n+2}(t),\ z = T_{3n+1}(t)$. This is the first known infinite family of polynomial knots.

In citeKPR10, we give (with D. Pecker and F. Rouillier) an exhaustive list of minimal parametrizations for two-bridge knots with 10 crossings or fewer. This result has been obtained by considering a zero-dimensional variety for which we need to isolate the elements. Its degree is $\frac{1}{2}(a-1)(b-1)(c-1)$ that may be quite high. This results have been presented at the Mega 09 Conference and published in [22]. We give a new algorithm based on a new geometric description of implicit Chebyshev curves and the computation of the real roots of polynomials in $Q(\cos\frac{\pi}{a}, \cos\frac{\pi}{b}\cos\frac{\pi}{c})[t])$.

We proposed an algorithm to obtain the minimal polynomial of $\cos\frac{\pi}{n}$. This question is related to the diophantine trigonometric equation.

$$\sum_{i=1}^{k} n_i \cos r_i \pi = 0,$$

where n_i and r_i are rational numbers.

Chebyshev knots are polynomial analogues of Lissajous knots. They have been studied by many authors (Jones, Przytycki, Lamm, Hoste). In [19], we give explicit minimal parametrizations for infinite families f rational knots. In [21], we show that Fibonacci knots are not generally not Lissajous.

In [19], [20] we give a complete classification of harmonic knots $H(a,b,c)$, $a \le 4$.

7. Contracts and Grants with Industry

7.1. WMI (Maple)

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

A contract as been signed with the Canadian company *Waterloo Maple Inc* in 2005. The objective is to integrate *SALSA* software into one of the most well known general computer algebra system (*Maple*). The basic term of the contract is of four years (renewable).

7.2. 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. Other Grants and Activities

8.1. National Initiatives

8.1.1. ANR Grant "SIROPA"

Participants: F. Rouillier [contact], J.-C. Faugère, M. Safey El Din, G. Moroz.

In collaboration with COPRIN project-team (Sophia - Antipolis), IRCcYN and LINA (University / CNRS - Nantes), IRMAR (CNRS/University of Rennes I). The goal of this project is to study the singularities of parallel robots from theoretical aspects (classifications) to the practical ones (behavior).

8.1.2. ANR Grant "MAC"

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

In collaboration with France Telecom and ENSTA. This project is to be replaced in the more general context of information protection. Its research areas are cryptography and symbolic computation. We are here essentially – but not exclusively – concerned with public key cryptography. One of the main issues in public key cryptography is to identify hard problems, and propose new schemes that are not based on number theory. Following this line of research, *multivariate schemes* have been introduced in the mid eighties [Diffie and Fell 85, Matsumoto and Imai 85].

In order to evaluate the security of new proposed schemes, strong and efficient cryptanalytic methods have to be developped. The main theme we shall address in this project is the evaluation of the security of cryptographic primitives by means of algebraic methods. The idea is to model a cryptographic primitive as a system of algebraic equations. The system is constructed in such a way as to have a correspondence between the solutions of this system, and a secret information of the considered primitive. Once this modeling is done, the problem is then to solve an algebraic system. Up to now, Gröbner bases appear to yield the best algorithms to do so.

8.1.3. ANR Jeunes Chercheurs "CAC"

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

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. This proposal is a follow-up of the ANR MAC described below. In CAC, we plan to follow the methodology proposed in MAC, namely using basic tools of computer algebra to evaluate the security of cryptographic schemes. However, whilst ANR MAC was mainly interested develop new algebraic tools for studying the security of multivariate public key cryptosystems, 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. European Initiatives

8.2.1. 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 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. International Initiatives

8.3.1. 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. INRIA Associate Team "Chinese SALSA"

Chinese Salsa is an associate team created in January 2006. It brings together most of the members of SALSA and researchers from Beihang university, Beijing (university and academy of science). The general objectives of *Chinese-Salsa* are mainly the same as those of *SALSA*.

8.3.3. Joint LIAMA Project ECCA

ECCA (Exact/Certified Computation with Algebraic systems) is a LIAMA project (Reliable Software Theme). The partners are INRIA, CNRS, and CAS.

8.3.4. 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.

9. Dissemination

9.1. Scientific Animation

9.1.1. 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).

F. Rouillier is member of the editorial board of Journal of Symbolic Computation (Elsevier) and was guest editor for special issues in Journal "Mathematics in Computer Science" (Birkhäuser).

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).

J.-C. Faugère is member of the program committee for the 35th International Symposium on Symbolic and Algebraic Computation Issac'10 (Munich, Germany, July 25–28 2010), program committee of 6th China International Conference on Information Security and Cryptology (Beijing, China, October 2010) program co-chair of the 2nd International Conference on Symbolic Computation and Cryptography (Royal Holloway, University of London, June 2010), scientific and program committee of Yet Another Conference on Cryptography (October 4 – October 8, 2010, Porquerolles Island, France), member of the program committee of the PASCO (Parallel and Symbolic Computation) 2010 in Grenoble.

L. Perret was member of the program committee of the Workshop on Tools for Cryptanalysis 2010 (Royal Holloway, University of London, June 22-23 2010), program committee of the 2nd International Conference on Symbolic Computation and Cryptography (Royal Holloway, University of London, June 23-25 2010), program committee of 6th China International Conference on Information Security and Cryptology (Beijing, China, October 2010), program committee of Yet Another Conference on Cryptography (October 4 – October 8, 2010, Porquerolles Island, France).

G. Renault was member of the program committee of the Joint Conference of ASCM 2009 and MACIS 2009 (Fukuoka, Japan, December 14–17, 2009).

F. Rouillier was member of the program committees of the Joint Conference of ASCM 2009 and MACIS 2009 (Fukuoka, Japan, December 14–17, 2009).

M. Safey El Din was member of the program committee of the 12th International Workshop on Computer Algebra in Scientific Computing (Tsakhkadzor, Armenia, September 6–12, 2010) and is 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).

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),
- International Conference on Algebraic and Numeric Biology (Hagenberg, Austria, July 31 – August 2, 2010),
- 8th International Workshop on Automated Deduction in Geometry (Munich, Germany, July 22–24, 2010),
- 9th International Conference on Mathematical Knowledge Management (Paris, France, July 8–10, 2010),
- 10th International Conference on Artificial Intelligence and Symbolic Computation (Paris, France, July 5–6, 2010),
- Conference on Symbolic Computation and Its Applications (Maribor, Slovenia, June 30 – July 2, 2010),
- 7th Asian Workshop on Foundations of Software (Beijing, China, May 14–16, 2010).
- Member of the Advisory Program Committee for the 3rd International Congress of Mathematical Software (Kobe, Japan, September 13–17, 2010).
- Co-chair of the Track on Symbolic Computation at the 12th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (Timisoara, Romania, September 23–26, 2010).

9.1.2. Scientific visits and international seminar

G. Renault was invited 2 weeks in December 2010 by K. Yokoyama at the Mathematical Laboratory (Rykkyo University, Tokyo, Japan).

M. Safey El Din was invited 2 weeks in April 2010 by L. Zhi at the Key Laboratory of Mechnanization and Mathematics (Chinese Academy of Sciences, Beijing China) and 2 weeks in February 2020 by E. Schost at the Department of Computer Science at The University of Western Ontario (London, Canada).

J.-C. Faugère was invited 1 week in January 2010 to visit the DSO National Labs in Singapore.

9.1.3. Conferences (organization) and invited talks

J.-C. Faugère, L. Perret, G. Renault organized the second SCC conference in London.

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

F. Rouillier is member of the MACIS Steering Committee.

M. Safey El Din is co-organizer (with L. Zhi) of the First International Workshop on Certified and Reliable Computing, to be held in July 2011 at Nanning, China.

J.-C. Faugère [32] was invited speaker at Mathematical Software - ICMS 2010 in Japan [32], ESC 2010 (Early Symmetric Crypto) Remich (Luxembourg) and to give a series of talk [33] in Singapore (DSO National Labs).

M. Safey El Din was invited speaker at

1. *Minisymposium on Algebraic Geometry and Optimization*, SIAM Conference on Optimization, Darmstadt, Germany, 2011.
2. *SIAM/MSRI Workshop on Hybrid Methodologies for Symbolic-Numeric Computation*, Berkeley, USA, 2010 [64].
3. *SIAM Workshop on Parallel Processing, Special session on Symbolic Computation*, Seattle, USA, 2010 [35].
4. *SMAI MODE 2010*, Minisymposium on Computer Algebra and Optimization, March 2010, Limoges.
5. *Journées Nationales du GDR Info-Math*, France, 2010.

D Wang has organized the following conferences:

- General Co-chair of the 4th International Conference on Mathematical Aspects of Computer and Information Sciences (Beijing, China, October 19–21, 2011).
- Chair of the Program Committee for the International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (Timisoara, Romania, September 26–29, 2011).

D Wang was invited speaker at

- 4th International Symposium on Multiagent Systems, Robotics and Cybernetics: Theory and Practice (Baden-Baden, Germany, August 4–5, 2010).
- Research Institute for Symbolic Computation, Johannes Kepler University, Linz, Austria (July 13, 2010).

9.1.4. Committees

J.-C. Faugère was a member of the EQUIPEX jury (ANR).

J.-C. Faugère was a member of the evaluation committee (AERES) of the Jean Kuntzmann lab (Grenoble) and of the institut de mathématiques de Toulon et du Var. J.-C. Faugère was a member of the visiting committee of University of Limoges (JJ Aubert chairman).

F. Rouillier and J.-C. Faugère are member of the hiring committee in computer science at the <<Université Pierre et Marie Curie>>.

JC Faugère and M. Safey El Din are members of the hiring committee in Mathematics at the “Université de Limoges”

L. Perret was in the Ph.D committee of Gilles Macariot-Rat (Ph.D defended at ENS-ULM)

9.2. 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>>.

10. 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] F. Rouillier. *Solving zero-dimensional systems through the rational univariate representation*, in "Journal of Applicable Algebra in Engineering, Communication and Computing", 1999, vol. 9, n^o 5, p. 433–461.

[8] F. Rouillier, P. Zimmermann. *Efficient Isolation of Polynomial Real Roots*, in "Journal of Computational and Applied Mathematics", 2003, vol. 162, n^o 1, p. 33-50.

[9] 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.

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

Publications of the year

Doctoral Dissertations and Habilitation Theses

[11] M. Safey El Din. *Polynomial System Solving over the Reals: Algorithms, Complexity, Implementations and Applications*, University Pierre and Marie Curie, 2010, Habilitation Thesis, Ph. D. Thesis.

Articles in International Peer-Reviewed Journal

[12] B. BANK, M. GIUSTI, J. HEINTZ, M. SAFEY EL DIN, E. SCHOST. *On the geometry of polar varieties*, in "Applicable Algebra in Engineering, Communication and Computing", 2010, vol. 21, n^{o} 1, p. 33-83 [*DOI :* 10.1007/S00200-009-0117-1], http://www-salsa.lip6.fr/~safey/Articles/BaGiHeSaSc09.pdf.

[13] L. BETTALE, J.-C. FAUGÈRE, L. PERRET. *Hybrid approach for solving multivariate systems over finite fields*, in "Journal of Mathematical Cryptology", 2010, vol. 3, n^{o} 3, p. 177-197 [*DOI :* 10.1515/JMC.2009.009], http://www-salsa.lip6.fr/~jcf/Papers/JMC2.pdf.

[14] G. BOURGEOIS, J.-C. FAUGÈRE. *Algebraic Attack on NTRU using Witt Vectors and Gröbner bases*, in "Journal of Mathematical Cryptology", 2010, vol. 3, n^{o} 3, p. 205-214 [*DOI :* 10.1515/JMC.2009.011], http://www-salsa.lip6.fr/~jcf/Papers/JMC1.pdf.

[15] J.-C. FAUGÈRE, Y. LIANG. *Artificial discontinuities of single-parametric Gröbner bases*, in "Journal of Symbolic Computation", 2010, vol. In Press, Corrected Proof, p. 1–17 [*DOI :* 10.1016/J.JSC.2010.11.001], http://www-salsa.lip6.fr/~jcf/Papers/JSC_LP10.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", 2010, vol. In Press, Corrected Proof, p. 1–39, 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", 2010, vol. In Press, Corrected Proof, p. 1–16, to appear, http://dx.doi.org/10.1016/j.tcs.2010.11.047.

[18] A. HASHEMI, D. LAZARD. *Sharper complexity bounds for zero-dimensional Gröbner bases and polynomial system solving*, in "International Journal of Algebra and Computation (IJAC)", 2010, p. 1–8, Accepted on November 15, 2010.

[19] P.-V. KOSELEFF, D. PECKER. *Chebyshev diagrams for two-bridge knots*, in "Geometricae Dedicata", 2010, p. 1–1, http://dx.doi.org/10.1007/s10711-010-9514-7.

[20] P.-V. KOSELEFF, D. PECKER. *Chebyshev Knots*, in "Journal of Knot Theory and Ramifications", 2010, p. 1–1, accepted.

[21] P.-V. KOSELEFF, D. PECKER. *On Fibonacci knots*, in "Fibonacci Quarterly", 2010, vol. 48, n^{o} 2, p. 137–143.

[22] P.-V. KOSELEFF, D. PECKER, F. ROUILLIER. *The first rational Chebyshev knots*, in "Journal of Symbolic Computation", 2010, vol. 45, p. 1341–1358, http://dx.doi.org/10.1016/j.jsc.2010.06.014.

[23] D. LAZARD. *CAD and topology of semi-algebraic sets*, in "Mathematics in Computer Science", 2010, vol. 4, p. 93–112, Special issue Computational Geometry and Computer-aided Geometric Design.

[24] F. LEVY-DIT-VEHEL, L. PERRET. *Security analysis of word problem-based cryptosystems*, in "Des. Codes Cryptography", 2010, vol. 54, n^{o} 1, p. 29-41, http://dx.doi.org/10.1007/s10623-009-9307-x.

[25] X. Li, C. Mou, D. Wang. *Decomposing Polynomial Sets into Simple Sets over Finite Fields: The Zero-dimensional Case*, in "Computers and Mathematics with Applications", 2010, vol. 60, n$^{\text{o}}$ 11, p. 2983–2997.

[26] G. Moroz, D. Chablat, P. Wenger, F. Rouillier. *On the determination of cusp points of 3-RPR parallel manipulators*, in "Journal of Mechanism and Machine Theory", 2010, vol. 45, n$^{\text{o}}$ 11, p. 1555 - 1567, under revision [*DOI :* 10.1016/j.mechmachtheory.2010.06.016], http://www.sciencedirect.com/science/article/B6V46-50M0TFS-8/2/3d5de523d3205004c6e770c5ef5b7511.

[27] G. Moroz. *Properness Defects of Projection and Minimal Discriminant Variety*, in "Journal of Symbolic Computation", 2010, p. 1–24.

[28] M. Pouget, S. Lazard, E. Tsigaridas, F. Rouillier, L. Penarnda, J. Cheng. *On the topology of planar algebraic curves*, in "Mathematics in Computer Science", 2010, p. 1–1.

[29] 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", 2010, p. 1–43 [*DOI :* 10.1007/s00454-009-9239-2], http://www-salsa.lip6.fr/~safey/Articles/SaSc09.pdf.

[30] M. Safey El Din, L. Zhi. *Computing rational points in convex semi-algebraic sets and Sums of Squares decompositions*, in "SIAM Journal on Optimization", 2010, vol. 20, n$^{\text{o}}$ 6, p. 2876-2889 [*DOI :* 10.1137/090772459], http://www-salsa.lip6.fr/~safey/Articles/convex_sas.pdf.

[31] D. Wang. *Algebraic Analysis of Stability and Bifurcation for Nonlinear Flight Dynamics*, in "The Aeronautical Journal", 2011, p. 1–1, To appear.

Invited Conferences

[32] J.-C. Faugère. *FGb: A Library for Computing Gröbner Bases*, in "Mathematical Software - ICMS 2010", Berlin, Heidelberg, K. Fukuda, J. Hoeven, M. Joswig, N. Takayama (editors), Lecture Notes in Computer Science, Springer Berlin / Heidelberg, September 2010, vol. 6327, p. 84-87 [*DOI :* 10.1007/978-3-642-15582-617], http://www-salsa.lip6.fr/~jcf/Papers/ICMS.pdf.

[33] J.-C. Faugère. *Structured Polynomial Systems and Algebraic Cryptanalysis of McEliece Variants with Compact Keys.*, in "DSO National Labs", January 2010, p. 1–1.

[34] M. Safey El Din. *Fast Algorithms for Real Solving Polynomial Systems of Inequalities/inequations*, in "SIAM Conference on Parallel Processing and Scientific Computing – High Performance Symbolic Computing", SIAM, 2010, p. 1–1.

[35] M. Safey El Din. *Fast Algorithms for Real Solving Polynomial Systems of Inequalities/inequations*, in "SIAM Conference on Parallel Processing and Scientific Computing – High Performance Symbolic Computing", SIAM, 2010, p. 1–1.

International Peer-Reviewed Conference/Proceedings

[36] 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", M. Yung, X. Lai (editors), Springer-Verlag, October 2010, p. 1–18, http://www-salsa.lip6.fr/~jcf/Papers/INSCRYPT2010.pdf.

[37] M. Albrecht, C. Cid, T. Dulien, J.-C. Faugère, L. Perret. *Algebraic Precomputations in Differential Cryptanalysis*, in "Tools'10: Proceedings of the Workshop on Tools for Cryptanalysis 2010", RHUL, Ecrypt II, June 2010, p. 1–14, http://www-salsa.lip6.fr/~jcf/Papers/Tools2010a.pdf.

[38] L. Bettale, J.-C. Faugère, L. Perret. *Hybrid Approach : a Tool for Multivariate Cryptography*, in "Tools'10: Proceedings of the Workshop on Tools for Cryptanalysis 2010", RHUL, Ecrypt II, June 2010, p. 1–2, http://www-salsa.lip6.fr/~jcf/Papers/Tools2010b.pdf.

[39] L. Bettale, J.-C. Faugère, L. Perret. *Cryptanalysis of Multivariate and Odd-Characteristic HFE Variants*, in "Public Key Cryptography - PKC 2011", D. Catalano, et al. (editors), Lecture Notes in Computer Science, Springer-Verlag, 2011, vol. 6571, p. 441–458, http://www-salsa.lip6.fr/~jcf/Papers/pkc2011a.pdf.

[40] 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", Lecture Notes in Computer Science, Springer-Verlag, 2011, vol. 6571, p. 1–12, eds. D. Catalano et al., http://www-salsa.lip6.fr/~jcf/Papers/BFFP11.pdf.

[41] 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 (editor), Lecture Notes in Artificial Intelligence, Springer-Verlag, 2010.

[42] J.-C. Faugère, A. Joux, L. Perret, J. Treger. *Cryptanalysis of the Hidden Matrix Cryptosystem*, in "Progress in Cryptology - LATINCRYPT 2010", M. Abdalla, P. Barreto (editors), Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 2010, vol. 6212, p. 241-254 [*DOI :* 10.1007/978-3-642-14712-815], http://www-salsa.lip6.fr/~jcf/Papers/LATIN2010.pdf.

[43] J.-C. Faugère, S. Lachartre. *Parallel Gaussian Elimination for Gröbner bases computations in finite fields*, in "Proceedings of the 4th International Workshop on Parallel and Symbolic Computation", New York, NY, USA, M. Moreno-Maza, J. Roch (editors), PASCO '10, ACM, July 2010, p. 89–97 [*DOI :* 10.1145/1837210.1837225], http://www-salsa.lip6.fr/~jcf/Papers/PASCO2010.pdf.

[44] J.-C. Faugère, R. Marinier, G. Renault. *Implicit Factoring with Shared Most Significant and Middle Bits*, in "in 13th International Conference on Practice and Theory in Public Key Cryptography – PKC 2010", P. Nguyen, D. Poincheval (editors), Lecture Notes in Computer Science, Springer-Verlag, 2010, vol. 6056, p. 70-87 [*DOI :* 10.1007/978-3-642-13013-75], http://www-salsa.lip6.fr/~jcf/Papers/pkc2010b.pdf.

[45] J.-C. Faugère, R. Marinier, G. Renault. *Implicit Factoring with Shared Most Significant and Middle Bits*, in "SCC '10: Proceedings of the 2nd International Conference on Symbolic Computation and Cryptography", RHUL, 2010, p. 197–201, http://www-salsa.lip6.fr/~jcf/Papers/SCC2010c.pdf.

[46] J.-C. Faugère, R. Odegard, L. Perret, D. Gligoroski. *Analysis of the MQQ Public Key Cryptosystem*, in "SCC'10: Proceedings of the 2nd International Conference on Symbolic Computation and Cryptography", RHUL, June 2010, p. 101–116, http://www-salsa.lip6.fr/~jcf/Papers/SCC2010b.pdf.

[47] J.-C. Faugère, R. Odegard, L. Perret, D. Gligoroski. *Analysis of the MQQ Public Key Cryptosystem*, in "Ninth International Conference on Cryptology And Network Security (CANS 2010)", S.-H. Heng, R. N. Wright, B.-M. Goi (editors), Subseries: Security and Cryptology, Springer-Verlag, December 2010, vol. 6467, p. 1–14, http://www-salsa.lip6.fr/~jcf/Papers/CANS2010.pdf.

[48] J.-C. FAUGÈRE, A. OTMANI, L. PERRET, J.-P. TILLICH. *A Distinguisher for High Rate McEliece Cryptosystem – Extended Abstract*, in "Yet Another Conference on Cryptography, YACC 2010", Toulon, P. VÉRON (editor), 2010, p. 1–4, http://www-salsa.lip6.fr/~jcf/Papers/ARTICLE_YACC2.pdf.

[49] J.-C. FAUGÈRE, A. OTMANI, L. PERRET, J.-P. TILLICH. *Algebraic Cryptanalysis of McEliece Variants with Compact Keys*, in "Proceedings of Eurocrypt 2010", Lecture Notes in Computer Science, Springer Verlag, 2010, vol. 6110, p. 279-298 [*DOI :* 10.1007/978-3-642-13190-514], http://www-salsa.lip6.fr/~jcf/Papers/Eurocrypt2010.pdf.

[50] J.-C. FAUGÈRE, A. OTMANI, L. PERRET, J.-P. TILLICH. *Algebraic Cryptanalysis of McEliece Variants with Compact Keys – Toward a Complexity Analysis*, in "SCC '10: Proceedings of the 2nd International Conference on Symbolic Computation and Cryptography", RHUL, June 2010, p. 45–55, http://www-salsa.lip6.fr/~jcf/Papers/SCC2010a.pdf.

[51] J.-C. FAUGÈRE, A. OTMANI, L. PERRET, J.-P. TILLICH. *Algebraic Cryptanalysis of McEliece Variants with Compact Keys – Toward a Complexity Analysis*, in "Yet Another Conference on Cryptography, YACC 2010", Toulon, P. VÉRON (editor), 2010, p. 1–4, http://www-salsa.lip6.fr/~jcf/Papers/ARTICLE_YACC1.pdf.

[52] J.-C. FAUGÈRE, L. PERRET. *Algebraic Cryptanalysis of Curry and Flurry using Correlated Messages*, in "Information Security and Cryptology: 5th International Conference, Inscrypt 2009", Beijing, China, M. YUNG, F. BAO (editors), Springer-Verlag, December 2009, vol. 6151, p. 266–277, Revised Selected Papers [*DOI :* 10.1007/978-3-642-16342-519], http://www-salsa.lip6.fr/~jcf/Papers/INSCRYPT2009.pdf.

[53] J.-C. FAUGÈRE, P.-J. SPAENLEHAUER. *Algebraic Cryptanalysis of the PKC'09 Algebraic Surface Cryptosystem*, in "Public Key Cryptography PKC 2010", P. NGUYEN, D. POINCHEVAL (editors), Lecture Notes in Computer Science, Springer-Verlag, 2010, vol. 6056, p. 35–52 [*DOI :* 10.1007/978-3-642-13013-73], http://www-salsa.lip6.fr/~jcf/Papers/pkc2010a.pdf.

[54] J.-C. FAUGÈRE, M. SAFEY EL DIN, P.-J. SPAENLEHAUER. *Computing Loci of Rank Defects of Linear Matrices using Grobner Bases and Applications to Cryptology*, in "ISSAC '10: Proceedings of the 2010 international symposium on Symbolic and algebraic computation", New York, NY, USA, ISSAC '10, ACM, 2010, p. 257–264, Best Student Paper Award [*DOI :* 10.1145/1837934.1837984], http://www-salsa.lip6.fr/~jcf/Papers/FSS10.pdf.

[55] J.-C. FAUGÈRE, J. VON ZUR GATHEN, L. PERRET. *Decomposition of Generic Multivariate Polynomials*, in "ISSAC '10: Proceedings of the 2010 international symposium on Symbolic and algebraic computation", New York, NY, USA, ISSAC '10, ACM, 2010, p. 131–137, isbn: 0747-7171 (updated version) [*DOI :* 10.1145/1837934.1837963], http://www-salsa.lip6.fr/~jcf/Papers/ISSAC_FGP_2010.pdf.

[56] 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.

[57] F. GUO, M. SAFEY EL DIN, L. ZHI. *Global Optimization of Polynomials Using Generalized Critical Values and Sums of Squares*, in "ISSAC '10: Proceedings of the 2010 international symposium on Symbolic and algebraic computation", New York, NY, USA, ACM, 2010, p. 107–114 [*DOI :* 10.1145/1837934.1837960], http://www-salsa.lip6.fr/~safey/Articles/gcv_sos.pdf.

[58] Y. HUANG, D. WANG. *Computing Self-intersection Loci of Parametrized Surfaces Using Regular Systems and Gröbner Bases*, in "SYNASC 2009: Proceedings of the 11th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing", Los Alamitos, CA, IEEE Computer Society, September 2010, p. 28–36.

[59] J.-G. KAMMERER, R. LERCIER, G. RENAULT. *Encoding Points on Hyperelliptic Curves over Finite Fields in Deterministic Polynomial Time*, in "PAIRING-BASED CRYPTOGRAPHY - PAIRING 2010", M. JOYE, A. MIYAJI, A. OTSUKA (editors), Lecture Notes in Computer Science, Springer-Verlag, 2010, vol. 6487, p. 278–297 [*DOI :* 10.1007/978-3-642-17455-118], http://arxiv.org/abs/1005.1454.

[60] G. MOROZ, D. CHABLAT, P. WENGER, F. ROUILLIER. *Cusp points in the parameter space of RPR-2PRR parallel manipulators*, in "EuroComs'2010 - 3-rd European Conference on Mechanism Science", D. PISLA (editor), New Trends in Mechanism Science: Analysis and Design, Springer, 2010, p. 29–27.

[61] F. ROUILLIER. *Solving Algebraic Systems and applications to geometric computations*, in "International Congress on Mathematical Software", Springer, 2010, p. 1–1.

[62] M. SOOS. *Grain of Salt — an Automated Way to Test Stream Ciphers through SAT Solvers*, in "Tools'10: Proceedings of the Workshop on Tools for Cryptanalysis 2010", RHUL, 2010, p. 1–2.

National Peer-Reviewed Conference/Proceedings

[63] D. WANG, X.-S. GAO, Z. LIU, Z. LI. *A Review of the Development of Mathematics Mechanization (in Chinese)*, in "Wen-tsün Wu and Chinese Mathematics", B. JIANG, B. LI, X.-S. GAO, W. LI (editors), Global Publishing, Singapore, 2010, p. 221–233.

Workshops without Proceedings

[64] M. SAFEY EL DIN. *Stability Analysis of Numerical Schemes with a Variant Quantifier Elimination Algorithm over the Reals*, in "Hybrid Methodologies for Symbolic-Numeric Computation", Mathematical Sciences Research Institute, 2010, p. 1–1.

[65] M. SOOS. *Enhanced Gaussian Elimination in DPLL-based SAT Solvers*, in "Pragmatics of SAT", Edinburgh, Scotland, UK, July 2010.

Scientific Books (or Scientific Book chapters)

[66] J.-C. FAUGÈRE, L. PERRET. *Symbolic Computation and Cryptography*, Birkhäuser and Springer, Mathematics in Computer Science, 2010, vol. 3, n^{o} 2, isbn: 1661-8270 [*DOI :* 10.1007/s11786-009-0017-6], http://www-salsa.lip6.fr/~jcf/Papers/MCSforeword.pdf.

[67] D. WANG, C. MOU, X. LI, J. YANG, M. JIN, Y. HUANG. *Polynomial Algebra (in Chinese)*, Higher Education Press, Beijing, 2011, In press.

Books or Proceedings Editing

[68] J.-C. FAUGÈRE, C. CID (editors). *Proceedings of the 2nd International Conference on Symbolic Computation and Cryptography (SCC 2010), Royal Holloway, University of London, Egham, June, 2010*, Royal Holloway, University of London, 2010, p. 1–253, isbn: 0000-0000, http://www-salsa.lip6.fr/~jcf/Papers/scc2010-proceedings.pdf.

References in notes

[69] 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.

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

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

[72] 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.

[73] S. CORVEZ, F. ROUILLIER. *Using computer algebra tools to classify serial manipulators*, in "Automated Deduction in Geometry", Lecture Notes in Artificial Intelligence, Springer, 2003, vol. 2930, p. 31–43.

[74] 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.

[75] 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.

[76] 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.

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

[78] 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.

[79] 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.

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

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

[82] 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.

[83] 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.

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

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

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

[87] 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.

[88] 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.

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

[90] F. ROUILLIER. *Real Root Counting For some Robotics problems*, in "Solid Mechanics and its Applications, Kluwer Academic Publishers", 1995, vol. 40, p. 73-82.

[91] 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.

[92] 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.

[93] 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.

[94] 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.

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

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

[97] 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.

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

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

[100] 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.