Activity Report 2012

Project-Team POLSYS

Polynomial Systems

RESEARCH CENTER
Paris - Rocquencourt

THEME
Algorithms, Certification, and Cryptography

Table of contents

Project-Team POLSYS

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

The PolSys is a common team betwen Inria, UPMC (LIP6 - Paris 6) and CNRS.

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

1. Members

Research Scientists

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

Faculty Members

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

PhD Students

Chenqi Mou [China Scholarship Council - defense in 2013 - J.-C. Faugère/D. Wang]
Luk Bettale [DGA - defense in 2011 - J.-C. Faugère/L. Perret]
Pierre-Jean Spaenlehauer [AMX - defense in 2012 - J.-C. Faugère/M. Safey El Din]
Christopher Goyet [CIFRE - defense in 2012 - J.-C. Faugère/G. Renault]
Louise Huot [EDITE - defense in 2014 - J.-C. Faugère/G. Renault]
Aurelien Greuet [Versailles - defense in 2014 - M. Safey El Din]
Frédéric de Portzamparc [CIFRE - defense in 2015 - J.-C. Faugère/L. Perret]
Rina Zeitoun [CIFRE - defense in 2015 - J.-C. Faugère/G. Renault]
Jules Svartz [AMN - defense in 2015 - J.-C. Faugère]
Thibaut Verron [ENS - defense in 2017 - J.-C. Faugère/M. Safey El Din]
Simone Naldi [Toulouse - defense in 2016 - M. Safey El Din]

Post-Doctoral Fellows

Chritian Eder [Fev 2013 - Jan 2014]
Martin Albrecht [Dec 2010 - Nov 2012]

Administrative Assistant

Virginie Collette [Secretary (SAR) Inria]

2. Overall Objectives

2.1. Introduction

The main objective of the POLSYS project is to solve systems of polynomial equations. Our main objectives are:

- **Fundamental Algorithms and Structured Systems.** The objective is to propose fast exponential exact algorithms to solve the problem of solving polynomial equations and to identify large classes of structured polynomial systems which can be solved in polynomial time.

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

2.2. Highlights of the Year

- In [4], we obtain an algorithm to solve Boolean systems with an expected complexity of $O(2^{0.792\,n})$ breaking the 2^n barrier.
- In [10], we propose an algorithm to solve a variant of the Quantififer Elimination Problem for which the output formula is *almost equivalent* to the input formula. The complexity of this algorithm is much better than other algorithms and can solve previously untractable problems.
- In [25], we improve the complexity of Index Calculus Algorithms in Elliptic Curves by means of Gröbner basis techniques and we analyze the complexity of this new approach by using the multi-homogeneous structure of the equations.

3. Scientific Foundations

3.1. Introduction

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

3.2. Fundamental Algorithms and Structured Systems

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

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

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

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

3.3. Solving Systems over the Reals and Applications.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Application Domains

4.1. Cryptology

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

4.2. Engineering sciences

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

5. Software

5.1. FGb

Participant: Jean-Charles Faugère [contact].

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

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

5.2. RAGlib

Participant: Mohab Safey El Din [contact].

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

5.3. Epsilon

Participant: Dongming Wang [contact].

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

6. New Results

6.1. The complexity of solving quadratic boolean systems is better than exhaustive search

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

6.2. Improving the Complexity of Index Calculus Algorithms in Elliptic Curves over Binary Fields

In [25], we study the index calculus method that was first introduced by Semaev for solving the ECDLP and later developed by Gaudry and Diem. In particular, we focus on the step which consists in decomposing points of the curve with respect to an appropriately chosen factor basis. This part can be nicely reformulated as a purely algebraic problem consisting in finding solutions to a multivariate polynomial. Our main contribution is the identification of particular structures inherent to such polynomial systems and a dedicated method for tackling this problem. We solve it by means of Gröbner basis techniques and analyze its complexity using the multi-homogeneous structure of the equations. We emphasize that the complexity obtained in the paper is very conservative in comparison to experimental results. We hope the new ideas provided here may lead to efficient index calculus based methods for solving ECDLP in theory and practice.

6.3. On the relation between the MXL family of algorithms and Gröbner basis algorithms

The computation of Gröbner bases remains one of the most powerful methods for tackling the Polynomial System Solving (PoSSo) problem. The most efficient known algorithms reduce the Gröbner basis computation to Gaussian eliminations on several matrices. However, several degrees of freedom are available to generate these matrices. It is well known that the particular strategies used can drastically affect the efficiency of the computations. In this work, we investigate a recently-proposed strategy, the so-called "Mutant strategy", on which a new family of algorithms is based (MXL, MXL2 and MXL3). By studying and describing the algorithms based on Gröbner basis concepts, we demonstrate in [3] that the Mutant strategy can be understood to be equivalent to the classical Normal Selection Strategy currently used in Gröbner basis algorithms. Furthermore, we show that the "partial enlargement" technique can be understood as a strategy for restricting the number of S-polynomials considered in an iteration of the F4 Gröbner basis algorithm, while the new termination criterion used in MXL3 does not lead to termination at a lower degree than the classical Gebauer–Möller installation of Buchberger's criteria. We claim that our results map all novel concepts from the MXL family of algorithms to their well-known Gröbner basis equivalents. Using previous results that had shown the relation between the original XL algorithm and F4, we conclude that the MXL family of algorithms can be fundamentally reduced to redundant variants of F4.

6.4. On the Complexity of the BKW Algorithm on LWE

In [35], we present a study of the complexity of the Blum-Kalai-Wasserman (BKW) algorithm when applied to the Learning with Errors (LWE) problem, by providing refined estimates for the data and computational effort requirements for solving concrete instances of the LWE problem. We apply this refined analysis to suggested parameters for various LWE-based cryptographic schemes from the literature and, as a result, provide new upper bounds for the concrete hardness of these LWE-based schemes.

6.5. On the Complexity of the Arora-Ge algorithm against LWE

Arora & Ge recently showed that solving LWE can be reduced to solve a high-degree non-linear system of equations. They used a linearization to solve the systems. We investigate in [34] the possibility of using Gröbner bases to improve Arora & Ge approach.

6.6. On enumeration of polynomial equivalence classes and their application to MPKC

The Isomorphism of Polynomials (IP) is one of the most fundamental problems in multivariate public key cryptography (MPKC). In [8], we introduce a new framework to study the counting problem associated to IP. Namely, we present tools of finite geometry allowing to investigate the counting problem associated to IP. Precisely, we focus on enumerating or estimating the number of isomorphism equivalence classes of homogeneous quadratic polynomial systems. These problems are equivalent to finding the scale of the key space of a multivariate cryptosystem and the total number of different multivariate cryptographic schemes respectively, which might impact the security and the potential capability of MPKC. We also consider their applications in the analysis of a specific multivariate public key cryptosystem. Our results not only answer how many cryptographic schemes can be derived from monomials and how big the key space is for a fixed scheme, but also show that quite many HFE cryptosystems are equivalent to a Matsumoto-Imai scheme.

6.7. Cryptanalysis of HFE, Multi-HFE and Variants for Odd and Even Characteristic

In [5], we investigate the security of HFE and Multi-HFE schemes as well as their minus and embedding variants. Multi-HFE is a generalization of the well-known HFE schemes. The idea is to use a multivariate quadratic system - instead of a univariate polynomial in HFE - over an extension field as a private key. According to the authors, this should make the classical direct algebraic (message-recovery) attack proposed by Faugère and Joux on HFE no longer efficient against Multi-HFE. We consider here the hardness of the key-recovery in Multi-HFE and its variants, but also in HFE (both for odd and even characteristic). We first improve and generalize the basic key recovery proposed by Kipnis and Shamir on HFE. To do so, we express this attack as matrix/vector operations. In one hand, this permits to improve the basic Kipnis-Shamir (KS) attack on HFE. On the other hand, this allows to generalize the attack on Multi-HFE. Due to its structure, we prove that a Multi-HFE scheme has much more equivalent keys than a basic HFE. This induces a structural weakness which can be exploited to adapt the KS attack against classical modifiers of multivariate schemes such as minus and embedding. Along the way, we discovered that the KS attack as initially described cannot be applied against HFE in characteristic 2. We have then strongly revised KS in characteristic 2 to make it work. In all cases, the cost of our attacks is related to the complexity of solving MinRank. Thanks to recent complexity results on this problem, we prove that our attack is polynomial in the degree of the extension field for all possible practical settings used in HFE and Multi-HFE. This makes then Multi-HFE less secure than basic HFE for equally-sized keys. As a proof of concept, we have been able to practically break the most conservative proposed parameters of multi-HFE in few days (256 bits security broken in 9 days).

6.8. Solving Polynomial Systems over Finite Fields: Improved Analysis of the Hybrid Approach

The Polynomial System Solving (PoSSo) problem is a fundamental NP-Hard problem in computer algebra. Among others, PoSSo have applications in area such as coding theory and cryptology. Typically, the security of multivariate public-key schemes (MPKC) such as the UOV cryptosystem of Kipnis, Shamir and Patarin is directly related to the hardness of PoSSo over finite fields. The goal of [22] is to further understand the influence of finite fields on the hardness of PoSSo. To this end, we consider the so-called *hybrid approach*. This is a polynomial system solving method dedicated to finite fields proposed by Bettale, Faugère and Perret (Journal of Mathematical Cryptography, 2009). The idea is to combine exhaustive search with Gröbner bases. The efficiency of the hybrid approach is related to the choice of a trade-off between the two methods. We propose here an improved complexity analysis dedicated to quadratic systems. Whilst the principle of the hybrid approach is simple, its careful analysis leads to rather surprising and somehow unexpected results. We prove that the optimal trade-off (i.e. number of variables to be fixed) allowing to minimize the complexity is achieved by fixing a number of variables proportional to the number of variables of the system considered, denoted n. Under some natural algebraic assumption, we show that the asymptotic complexity of the hybrid approach is $2^{(3.31-3.62\ \log_2(q)^{-1})\,n}$, where q is the size of the field (under the condition in particular that $\log(q) \ll n$). This is to date, the best complexity for solving PoSSo over finite fields (when $q > 2$). We have been able to quantify the gain provided by the hybrid approach compared to a direct Gröbner basis method. For quadratic systems, we show (assuming a natural algebraic assumption) that this gain is exponential in the number of variables. Asymptotically, the gain is $2^{1.49\,n}$ when both n and q grow to infinity and $\log(q)$.

6.9. Efficient Arithmetic in Successive Algebraic Extension Fields Using Symmetries

In [15] we present new results for efficient arithmetic operations in a number field $\mathbb{K}$ represented by successive extensions. These results are based on multi-modular and evaluation–interpolation techniques. We show how to use intrinsic symmetries in order to increase the efficiency of these techniques. Applications to splitting fields of univariate polynomials are presented.

6.10. Algebraic Crypanalysis with Side Channels Information

In [6] and [24] (see also the PhD thesis of C. Goyet [1]), we present new cryptanalyses of symmetric and asymmetric cryptosystems (e.g. AES and ECDSA). These analyses share the same fundamental hypotheses that some information are provided to the attacker by some oracle. In a practical point of view, such an oracle can be represented as a partial side channel attack realized in a first step (e.g. SPA, Fault attacks). The second step of the attack uses algorithms from computer algebra (e.g. Gröbner basis computation, LLL) in order to retrieve the secret key.

6.11. Worst case complexity of the Continued Fraction (CF) algorithm.

In [16] we consider the problem of isolating the real roots of a square-free polynomial with integer coefficients using the classic variant of the continued fraction algorithm (CF), introduced by Akritas. We compute a lower bound on the positive real roots of univariate polynomials using exponential search. This allows us to derive a worst case bound of $\widetilde{O}(d^4\tau^2)$ for isolating the real roots of a polynomial with integer coefficients using the *classic variant of CF*, where d is the degree of the polynomial and τ the maximum bitsize of its coefficients. This improves the previous bound of Sharma by a factor of d^3 and matches the bound derived by Mehlhorn and Ray for another variant of CF which is combined with subdivision; it also matches the worst case bound of the classical subdivision-based solvers STURM, DESCARTES, and BERNSTEIN.

6.12. Local Generic Position for Root Isolation of Zero-dimensional Triangular Polynomial Systems.

In [30] we present an algorithm based on local generic position (LGP) to isolate the complex or real roots and their multiplicities of a zero-dimensional triangular polynomial system. The Boolean complexity of the algorithm for computing the real roots is single exponential: $\widetilde{O}_B(N^{n^2})$, where $N = \max\{d, \tau\}$, d and τ, is the degree and the maximum coefficient bitsize of the polynomials, respectively, and n is the number of variables.

6.13. Univariate Real Root Isolation in Multiple Extension Fields

In [31] we present algorithmic, complexity and implementation results for the problem of isolating the real roots of a univariate polynomial in $K[x] \in L[y]$, where $L = \mathbb{Q}(\alpha\_1, \cdots, \alpha\_\ell)$ is an algebraic extension of the rational numbers. Our bounds are single exponential in ℓ and match the ones presented for the case $\ell = 1$. We consider two approaches. The first, indirect approach, using multivariate resultants, computes a univariate polynomial with integer coefficients, among the real roots of which are the real roots of B_α. The Boolean complexity of this approach is $\widetilde{O}_B(N^{4\ell+4})$, where N is the maximum of the degrees and the coefficient bitsize of the involved polynomials. The second, direct approach, tries to solve the polynomial directly, without reducing the problem to a univariate one. We present an algorithm that generalizes Sturm algorithm from the univariate case, and modified versions of well known solvers that are either numerical or based on Descartes' rule of sign. We achieve a Boolean complexity of $\widetilde{O}_B(\min\{N^{4\ell+7}, N^{2\ell^2+6}\})$ and $\widetilde{O}_B(N^{2\ell+4})$, respectively. We implemented the algorithms in C as part of the core library of Mathematica and we illustrate their efficiency over various data sets.

6.14. Mixed volume and distance geometry techniques for counting Euclidean embeddings of rigid graphs.

A graph G is called generically minimally rigid in $\mathbb{R}^d$ if, for any choice of sufficiently generic edge lengths, it can be embedded in $\mathbb{R}^d$ in a finite number of distinct ways, modulo rigid transformations. In [37] we deal with the problem of determining tight bounds on the number of such embeddings, as a function of the number of vertices. The study of rigid graphs is motivated by numerous applications, mostly in robotics, bioinformatics, and architecture. We capture embeddability by polynomial systems with suitable structure, so that their mixed volume, which bounds the number of common roots, yields interesting upper bounds on the number of embeddings. We explore different polynomial formulations so as to reduce the corresponding mixed volume, namely by introducing new variables that remove certain spurious roots, and by applying the theory of distance geometry. We focus on $\mathbb{R}^2$ and $\mathbb{R}^3$, where Laman graphs and 1-skeleta of convex simplicial polyhedra, respectively, admit inductive Henneberg constructions. Our implementation yields upper bounds for $n \leq 10$ in $\mathbb{R}^2$ and $\mathbb{R}^3$, which reduce the existing gaps and lead to tight bounds for $n \leq 7$ in both $\mathbb{R}^2$ and $\mathbb{R}^3$; in particular, we describe the recent settlement of the case of Laman graphs with 7 vertices. We also establish the first lower bound in $\mathbb{R}^3$ of about 2.52^n, where n denotes the number of vertices.

6.15. Variant Quantifier Elimination

In [10], we describe an algorithm (VQE) for a *variant* of the real quantifier elimination problem (QE). The variant problem requires the input to satisfy a certain *extra condition*, and allows the output to be *almost* equivalent to the input. The motivation/rationale for studying such a variant QE problem is that many quantified formulas arising in applications do satisfy the extra conditions. Furthermore, in most applications, it is sufficient that the output formula is almost equivalent to the input formula. The main idea underlying the algorithm is to substitute the repeated projection step of CAD by a single projection without carrying out a parametric existential decision over the reals. We find that the algorithm can tackle important and challenging problems, such as numerical stability analysis of the widely-used MacCormack's scheme. The problem has been practically out of reach for standard QE algorithms in spite of many attempts to tackle it. However the current implementation of VQE can solve it in about 12 hours.

6.16. Global optimization

Let $f_1, \cdots, f_p$ be in $\mathbb{Q}[\mathbf{X}]$, where $\mathbf{X} = (X_1, \cdots, X_n)^t$, that generate a radical ideal and let V be their complex zero-set. Assume that V is smooth and equidimensional. Given $f \in \mathbb{Q}[X]$ bounded below, consider the optimization problem of computing $f^{\bigstar} = \inf_{x \in V \cap \mathbb{R}^n} f(x)$. For $\mathbf{A} \in GL_n(\mathbb{C})$, we denote by $f^{\mathbf{A}}$ the polynomial $f(\mathbf{AX})$ and by $V^{\mathbf{A}}$ the complex zero-set of $f_1^{\mathbf{A}}, ..., f_p^{\mathbf{A}}$. In [9], we construct families of polynomials $\mathsf{M}_0^{\mathbf{A}}, ..., \mathsf{M}_d^{\mathbf{A}}$ in $\mathbb{Q}[\mathbf{X}]$: each $\mathsf{M}_i^{\mathbf{A}}$ is related to the section of a linear subspace with the critical locus of a linear projection. We prove that there exists a non-empty Zariski-open set $O \subset GL_n(\mathbb{C})$ such that for all $\mathbf{A} \in O \cap GL_n(\mathbb{Q})$, $f(x)$ is non-negative for all $x \in V \cap \mathbb{R}^n$ if, and only if, $f^{\mathbf{A}}$ can be expressed as a sum of squares of polynomials on the truncated variety generated by the ideal $\langle \mathsf{M}_i^{\mathbf{A}} \rangle$, for $0 \leq i \leq d$. Hence, we can obtain algebraic certificates for lower bounds on $f^{\bigstar}$ using semidefinite programs. Some numerical experiments are given. We also discuss how to decrease the number of polynomials in $\mathsf{M}_i^{\mathbf{A}}$.

6.17. Gröbner bases and critical points

We consider the problem of computing critical points of the restriction of a polynomial map to an algebraic variety. This is of first importance since the global minimum of such a map is reached at a critical point. Thus, these points appear naturally in non-convex polynomial optimization which occurs in a wide range of scientific applications (control theory, chemistry, economics,etc.). Critical points also play a central role in recent algorithms of effective real algebraic geometry. Experimentally, it has been observed that Gröbner basis algorithms are efficient to compute such points. Therefore, recent software based on the so-called Critical Point Method are built on Gröbner bases engines. Let $f_1, ..., f_p$ be polynomials in $\mathbb{Q}[x_1, ..., x_n]$ of degree D, $V \subset \mathbb{C}^n$ be their complex variety and π_1 be the projection map $(x_1, ..., x_n) \mapsto x_1$. The critical points of the restriction of π_1 to V are defined by the vanishing of $f_1, ..., f_p$ and some maximal minors of the Jacobian matrix Indus associated to $f_1, ..., f_p$. Such a system is algebraically structured: the ideal it generates is the sum of a determinantal ideal and the ideal generated by $f_1, ..., f_p$. In [26], we provide the first complexity estimates on the computation of Gröbner bases of such systems defining critical points. We prove that under genericity assumptions on $f_1, ..., f_p$, the complexity is polynomial in the generic number of critical points, i.e.$D^p(D-1)^{n-p}\begin{pmatrix} n-1 \\ p-1 \end{pmatrix}$ More particularly, in the quadratic case $D = 2$, the complexity of such a Gröbner basis computation is polynomial in the number of variables n and exponential in p. We also give experimental evidence supporting these theoretical results.

7. Bilateral Contracts and Grants with Industry

7.1. Oberthur Technologies

Oberthur Technologies is the World second largest provider of security and identification solutions and services based on smart card technologies for mobile, payment, transport, digital TV and convergence markets. Since 2007, SALSA co-supervised 3 internships of first year master student on cryptology in smart-cards, and one internship of a 2nd year master student. The goal of this last internship was to study the feasibility of implementing multivariate schemes in constrained environments (typically a smart card). A new jointly supervised PhD thesis (PolSys/Oberthur) has start in march 2012.

7.2. Gemalto

Gemalto is an international IT security company providing software applications, secure personal devices such as smart cards and token, ... Governments, wireless operators, banks, and enterprises use Gemalto's software and personal devices to deliver mobile services, payment security, authenticated cloud access, identity and privacy protection, eHealthcare, eGovernment, transport ticketing and machine to machine (M2M) communications applications.

PolSys is currently working Gemalto – thanks to PhD grabt CIFRE – on the security analysis of code-based cryptosystems (participants J.-C. Faugère, L. Perret, F. Urvoy de Portzamparc).

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

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

8.2. European Initiatives

8.2.1. FP7 Projects

ECRYPT II - European Network of Excellence for Cryptology II is a 4 1/2 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 (J.C. Faugère [contact], L. Perret, and G. Renault).

8.3. International Initiatives

8.3.1. Inria Associate Teams

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

8.3.2. Participation In International Programs

The POLSYS Team is part of the ECCA (Exact/Certified Computations with Algebraic systems) project at LIAMA in Beijing; our Chinese collaborators are from Beihang University, Peking University, the Chinese Academy of Sciences (Key Laboratory of Mathematics Mechnanization and State Key Laboratory of Information Security).

We are also part of an International Royal Society Joint Project with the Crypto team Royal Holloway, University of London, UK (2010-2012). The Royal Society Joint Project Grant Programme is designed to enable international collaboration. The main goal of the project is to investigate the viability of a wide range of new algebraic techniques in the cryptanalysis of block ciphers, and potentially other symmetric cryptographic algorithms (such as hash functions).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

As part of its collaboration with Guénaël Renault, the Professor Kazuhiro Yokoyama from Rikkyo University (Japan) visited the team during December 2012.

Erich Kaltofen (Professor at North Carolina State University) visited the group in June-July 2012 in the frame of the QOLAPS Associate Team.

Xiao-Shan Gao, Lihong Zhi, Jinsan Cheng (Chinese Academy of Sciences, KLMM) visited the group in July 2012 in the frame of the ECCA project and the ANR EXACTA project.

8.4.1.1. Internships

- T. Verron (Internship M2 and ENS Paris): Computation of Gröbner bases for quasi-homogeneous systems.
- F. Martani (Internship M2): Dedicated Linear Algebra for Gröbner Bases.

9. Dissemination

9.1. Scientific Animation

Elias Tsigaridas visited the Computer Science Department of Aarhus University, Denmark (28 May - 3 June) and gave a talk on random polynomials. He participated in ISSAC 2012 (July 22-25, 2012) in Grenoble, France and gave a talk on real solving polynomials with coefficients in multiple extension fields. He visited (23 Oct – 4 Noe) the Chinese Academy of Sciences, Beijing, China, as an invited speaker for the workshop Computational Geometry of the Asian Symposium on Computer Mathematics (ASCM), where he gave a talk on "Univariate Real Root Isolation in Extension Field and Applications to Topology of Curves". During his stay in China, he was also invited to give a talk at Institute of Software of the State Key Lab of Computer Science, about random polynomials. He was invited at the Department of Applied Mathematics, Univ. of Crete, Greece (15 Jun – 2 Jul) and gave a talk at the department's seminar about random polynomials. He participated and gave a talk in 7th Athens Colloquium on Algorithms and Complexity (ACAC) in Athens, Greece (27–28 July) on solving polynomials with coefficients on an extension field. He participated in the conference Computer Algebra in Scientific Computing (CASC) that was held in September 3 - 6, at Maribor, Slovenia. He visited in the North Carolina State University, USA (15 – 20 Oct) where he gave a talk at the Department's Symbolic Computation seminar with title "Real algebraic geometry and stochastic games". He participated in the Mathematics, Algorithms and Proofs 2012 (MAP) workshop of the GEOLMI ANR project (Univ. Konstanz, Germany, September 17 - September 21, 2012). Finally, he was invited to give a talk in the X-mas seminar of the ERGA lab of the Dept. of Informatics, Univ. of Athes, Greeece (27 December 2012) on real solving polynomials in the presence of logarithms.

J.C. Faugère was invited to give an invited talk in the international workshop on efficient linear algebra for Gröbner basis computation in Kaiserslautern. J.C. Faugère visited the Mathematics Department of the North Carolina State University and give a talk at the Computer Science Department of Duke University (USA). J.-C. Faugère, is member of the MEGA Advisory Board.

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).

L. Perret co-organized with C. Cid the Ecrypt II Summer School on Tools (Mykonos, Greece, 28 May - 1 June 2012 https://www.cosic.esat.kuleuven.be/ecrypt/courses/mykonos12/).

J.-C Faugère, and G. Renault delivered an invited talk at the Ecrypt II Summer School on Tools (Mykonos, Greece, 28 May - 1 June 2012 https://www.cosic.esat.kuleuven.be/ecrypt/courses/mykonos12/).

J.-C Faugère was the programm chair of third international conference on Symbolic Computation and Cryptography (SCC 2012) (International Centre for Mathematical meetings (CIEM), Castro Urdiales, 11-13 July 2012, http://scc2012.unican.es/).

L. Perret was in the programm comittee of SCC'12.

J.-C Faugère and L. Perret were in P.C. of the YACC'12 conference (September 24 – September 28, 2012, Porquerolles Island, France, http://yacc.univ-tln.fr/category/yacc-2012/).

L. Perret was in the programm comittee of International Conference on Practice and Theory in Public-Key Cryptography (PKC'2013) (Nara, Japan, February 26 - March 1, 2013, http://ohta-lab.jp/pkc2013/

J.-C Faugère and L. Perret are in the programm comittee of Symbolic Computations and Post-Quantum Cryptography Online Seminar organised by the Stevens Institute (USA, http://www.stevens.edu/algebraic/SCPQ/)

J.-C Faugère and L. Perret are guest editors of a Special issue of Journal of Symbolic Computation on "Mathematical and Computer Algebra Techniques in Cryptology" (in progress)

M. Safey El Din is member of the editorial board of Journal of Symbolic Computation. He was member of the Programm committee of CASC 2012. He visited the department of Computer Science at the Univ. of Western Ontario in February 2012 and Sept. 2012. With J.-C. Faugère, L. Perret and E. Tsigaridas, he visited the Symbolic Computation Group at North Carolina State University in October 2012. He was member of the National Council of Universities until Sept. 2012. Since Nov. 2012, he is the head of the Scientific Computing Department of LIP6. He has been nominated at the Institut Universitaire de France.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master : Ludovic Perret, Introduction à la Sécurité, 140 heures équivalent TD, niveau M1, Univ. Pierre-et-Marie-Curie, France

Master : J. Berthomieu, Modeling and numerical and symbolical resolutions of problems via MAPLE and MATLAB systems, 14 heures équivalent TD, niveau M1, Univ. Pierre-et-Marie-Curie, France

Master : J. Berthomieu, Linear Algebra and Applications, 35 heures équivalent TD, niveau M1, Univ. Pierre-et-Marie-Curie, France

Master : Guénaël Renault, Algèbre Linéaire et Applications, 35 heures équivalent TD, niveau M1, Univ. Pierre-et-Marie-Curie, France

Master : Guénaël Renault, Cryptologie Appliquée, 70 heures équivalent TD, niveau M2, Univ. Pierre-et-Marie-Curie, France

Master : Guénaël Renault, co-head of the speciality on"Sécurité, Fiabilité et Performance Numérique" in the Computer Science Master Program, niveaux M1-M2, Univ. Pierre-et-Marie-Curie, France

Master : M. Safey El Din, Modeling and numerical and symbolical resolutions of problems via MAPLE and MATLAB systems, 21 heures équivalent TD, niveau M1, Univ. Pierre-et-Marie-Curie, France

Master : M. Safey El Din, Polynomial Systems, Computer Algebra and Applications, 17 heures équivalent TD, niveau M2, Master Parisien de Recherche en Informatique, France

9.2.2. Supervision

PhD : Christopher Goyet, Cryptanalyse algébrique par canaux auxiliaires, Univ. Pierre-et-Marie-Curie, 7 novembre 2012, J.-C. Faugère, G. Renault

PhD : Pierre-Jean Spaenlehauer, Résolution de systèmes multi-homogènes et déterminantiels: algorithmes, complexités et applications, Univ. Pierre-et-Marie-Curie, 9 octobre 2012, J.-C. Faugère, M. Safey El Din

PhD in progress : Jules Svartz, Solving polynomial systems with symmetries, inscription octobre 2011, J.-C. Faugère

PhD in progress : Louise Huot, Étude des systèmes polynomiaux en cryptologie sur les courbes, Univ. Pierre-et-Marie-Curie, inscription octobre 2010, J.-C. Faugère, G. Renault

PhD in progress : Rina Zeitoun, Cryptologie sur cartes a puces et methodes algebriques, Univ. Pierre-et-Marie-Curie, inscription mars 2012, J.-C. Faugère, G. Renault

PhD in progress : Frederic Urvoy de Portzamparc, Cryptanalyse algébrique et étude de la sécurisation contre les attaques physiques des primitives fondées sur la théorie des codes, inscription février 2012, J.-C. Faugère, L. Perret

PhD in progress : Simone Naldi, Algorithmes de la géométrie algébrique réelle pour la théorie du contrôle, Univ. Paul Sabatier (Toulouse), inscription octobre 2012, D. Henrion, M. Safey El Din

9.2.3. Juries

J.-C. Faugère was member of 4 committees: 3 Prof. (UPMC, Montpellier, Rouen) and 1 MdC (UPMC).

9.3. Popularization

J.-C. Faugère gives a talk at Dassault Systèmes on applications of Gröbner Bases to industrial problems.

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] C. GOYET. *Cryptanalyse algébrique par canaux auxiliaires*, Université Paris 6, 2012.

[2] P.-J. SPAENLEHAUER. *Résolution de systèmes multi-homogènes et déterminantiels: algorithmes, complexités et applications*, Université Paris 6, 2012.

Articles in International Peer-Reviewed Journals

[3] M. ALBRECHT, C. CID, J.-C. FAUGÈRE, L. PERRET. *On the relation between the MXL family of algorithms and Gröbner basis algorithms*, in "Journal of Symbolic Computation", August 2012 [*DOI :* DOI:10.1016/J.JSC.2012.01.002], http://hal.inria.fr/hal-00776071.

[4] M. BARDET, J.-C. FAUGÈRE, B. SALVY, P.-J. SPAENLEHAUER. *On the Complexity of Solving Quadratic Boolean Systems*, in "Journal of Complexity", August 2012, vol. 29, n^{o} 1, p. 53-75 [*DOI :* 10.1016/J.JCO.2012.07.001], http://hal.inria.fr/hal-00655745.

[5] L. BETTALE, J.-C. FAUGÈRE, L. PERRET. *Cryptanalysis of HFE, Multi-HFE and Variants for Odd and Even Characteristic*, in "Designs, Codes and Cryptography", September 2012 [*DOI :* 10.1007/S10623-012-9617-2], http://hal.inria.fr/hal-00776072.

[6] C. CARLET, J.-C. FAUGÈRE, C. GOYET, G. RENAULT. *Analysis of the algebraic side channel attack*, in "Journal of Cryptographic Engineering", May 2012, vol. 2, n° 1, p. 45-62 [*DOI :* 10.1007/s13389-012-0028-0], http://hal.inria.fr/hal-00777829.

[7] X. CHEN, D. WANG. *Management of Geometric Knowledge in Textbooks*, in "Data & Knowledge Engineering", 2012, vol. 73, p. 43-57 [*DOI :* 10.1016/J.DATAK.2011.10.004], http://hal.inria.fr/hal-00779254.

[8] J.-C. FAUGÈRE, D. LIN, L. PERRET, T. WANG. *On enumeration of polynomial equivalence classes and their application to MPKC*, in "Finite Fields and Their Applications", March 2012, vol. 18, n° 2, p. 283-302 [*DOI :* 10.1016/J.FFA.2011.09.001], http://hal.inria.fr/hal-00776073.

[9] A. GREUET, G. FENG, M. SAFEY EL DIN, L. ZHI. *Global optimization of polynomials restricted to a smooth variety using sums of squares*, in "Journal of Symbolic Computation", 2012, vol. 47, n° 7, p. 503-518 [*DOI :* 10.1016/J.JSC.2011.12.003], http://hal.inria.fr/hal-00778239.

[10] H. HONG, M. SAFEY EL DIN. *Variant Quantififer Elimination*, in "Journal of Symbolic Computation", 2012, vol. 47, n° 7, p. 883-901 [*DOI :* 10.1016/J.JSC.2011.05.014], http://hal.inria.fr/hal-00778365.

[11] G. JERONIMO, D. PERRUCCI, E. TSIGARIDAS. *On the minimum of a polynomial function on a basic closed semialgebraic set and applications*, in "SIAM Journal on Optimization", 2012, p. 1-24, http://hal.inria.fr/hal-00776280.

[12] M. JIN, X. LI, D. WANG. *A New Algorithmic Scheme for Computing Characteristic Sets*, in "Journal of Symbolic Computation", 2012, p. 1–26, In press.

[13] C. MOU, D. WANG, X. LI. *Decomposing polynomial sets into simple sets over finite fields: The positive-dimensional case*, in "Theoretical Computer Science", November 2012, p. 1–7 [*DOI :* 10.1016/J.TCS.2012.11.009], http://hal.inria.fr/hal-00765840.

[14] W. NIU, D. WANG. *Algebraic Analysis of Stability and Bifurcation of a Self-assembling Micelle System*, in "Applied Mathematics and Computation", 2012, vol. 219, n° 1, p. 108-121 [*DOI :* 10.1016/J.AMC.2012.04.087], http://hal.inria.fr/hal-00779245.

[15] S. ORANGE, G. RENAULT, K. YOKOYAMA. *Efficient Arithmetic in Successive Algebraic Extension Fields Using Symmetries*, in "Mathematics in Computer Science", September 2012, vol. 6, n° 3, p. 217-233 [*DOI :* 10.1007/S11786-012-0112-Y], http://hal.inria.fr/hal-00777860.

[16] E. TSIGARIDAS. *Improved bounds for the CF algorithm*, in "Theoretical Computer Science", October 2012, p. 1-12, http://hal.inria.fr/hal-00776230.

[17] D. WANG. *Algebraic Stability Criteria and Symbolic Derivation of Stability Conditions for Feedback Control Systems*, in "International Journal of Control", 2012, vol. 85, n° 10, p. 1414-1421 [*DOI :* 10.1080/00207179.2012.686633], http://hal.inria.fr/hal-00779248.

Articles in National Peer-Reviewed Journals

[18] X. LI, D. WANG. *Simple Decomposition of Polynomial Sets over Finite Fields (in Chinese)*, in "Journal of Systems Science and Mathematical Sciences", 2012, vol. 32, n° 1, p. 15–26.

International Conferences with Proceedings

[19] M. ALBRECHT. *The M4RIE library for dense linear algebra over small fields with even characteristic*, in "ISSAC '12: Proceedings of the 2012 international symposium on Symbolic and algebraic computation", New York, NY, USA, ISSAC '12, ACM, 2012, p. 28–34, accepted.

[20] M. ALBRECHT, G. LEANDER. *An All-in-one Approach to Differential Cryptanalysis for Small Block Ciphers*, in "Conference on Selected Areas of Cryptography", Ontario, Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 2012, p. 1–12, accepted.

[21] A. BENOIT, A. BOSTAN, J. VAN DER HOEVEN. *Quasi-optimal multiplication of linear differential operators*, in "Foundations of Computer Science (FOCS), 2012 IEEE 53rd Annual Symposium on", Los Alamitos, CA, USA, FOCS '12, IEEE Computer Society, oct. 2012, vol. 1, p. 524 -530 [*DOI :* 10.1109/FOCS.2012.57], http://hal.inria.fr/hal-00685401.

[22] L. BETTALE, J.-C. FAUGÈRE, L. PERRET. *Solving Polynomial Systems over Finite Fields: Improved Analysis of the Hybrid Approach*, in "ISSAC 2012", Grenoble, France, July 2012, http://hal.inria.fr/hal-00776070.

[23] X. CHEN, W. LI, J. LUO, D. WANG. *Open Geometry Textbook: A Case Study of Knowledge Acquisition via Collective Intelligence (project description)*, in "Intelligent Computer Mathematics", Bremen, Allemagne, Lecture Notes in Computer Science, Springer, 2012, vol. 7362, p. 432-437 [*DOI :* 10.1007/978-3-642-31374-5_31], http://hal.inria.fr/hal-00779263.

[24] J.-C. FAUGÈRE, C. GOYET, G. RENAULT. *Attacking (EC)DSA Given Only an Implicit Hint*, in "Selected Areas in Cryptography", Windsor, Canada, L. R. KNUDSEN, H. WU (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7707, p. 252-274 [*DOI :* 10.1007/978-3-642-35999-6_17], http://hal.inria.fr/hal-00777804.

[25] J.-C. FAUGÈRE, L. PERRET, C. PETIT, G. RENAULT. *Improving the Complexity of Index Calculus Algorithms in Elliptic Curves over Binary Fields*, in "Eurocrypt'2012", Cambridge, Royaume-Uni, April 2012, http://hal.inria.fr/hal-00776066.

[26] J.-C. FAUGÈRE, M. SAFEY EL DIN, P.-J. SPAENLEHAUER. *Critical Points and Gröbner Bases: the Unmixed Case*, in "ISSAC 2012 - International Symposium on Symbolic and Algebraic Computation - 2012", Grenoble, France, July 2012, 17 pages, http://hal.inria.fr/hal-00667494.

[27] J.-C. FAUGÈRE, J. SVARTZ. *Solving Polynomial Systems Globally Invariant Under an Action of the Symmetric Group and Application to the Equilibria of N vortices in the Plane*, in "ISSAC '12: Proceedings of the 2012 international symposium on Symbolic and algebraic computation", Grenoble, France, ACM, July 2012, p. 170-178, http://hal.inria.fr/hal-00777791.

[28] J.-C. FAUGÈRE, P. GAUDRY, L. HUOT, G. RENAULT. *Using symmetries and fast change of ordering in the Index Calculus for Elliptic Curves Discrete Logarithm*, in "SCC'12: Proceedings of the 3nd International Conference on Symbolic Computation and Cryptography", Castro-Urdiales, July 2012, p. 113–118.

[29] D. GLIGOROSKI, R. S. ØDEGARD, R. E. JENSEN, L. PERRET, J.-C. FAUGÈRE, S. J. KNAPSKOG, S. MARKOVSKI. *MQQ-SIG - An Ultra-Fast and Provably CMA Resistant Digital Signature Scheme*, in "Trusted Systems - The Third International Conference on Trusted Systems - INTRUST 2011", Beijing, Chine, Y.

MOTI, C. LIQUN, Z. LIEHUANG (editors), Lecture Notes in Computer Science, Springer Verlag, January 2012, vol. 7222, p. 184-203 [*DOI :* 10.1007/978-3-642-32298-3_13], http://hal.inria.fr/hal-00778083.

[30] L. JI, J. CHENG, E. TSIGARIDAS. *Local Generic Position for Root Isolation of Zero-dimensional Triangular Polynomial Systems*, in "CASC", Maribor, Slovénie, W. KOEPF, E. VOROZHTSOV (editors), September 2012, vol. 7442, p. 186-197, http://hal.inria.fr/hal-00776212.

[31] A. STRZEBONSKI, E. TSIGARIDAS. *Univariate Real Root Isolation in Multiple Extension Fields*, in "ISSAC", Grenoble, France, 2012, p. 343-350, http://hal.inria.fr/hal-00776074.

[32] J. YANG, D. WANG, H. HONG. *Improving Angular Speed Uniformity by Optimal C0 Piecewise Reparameterization*, in "14th International Workshop on Computer Algebra in Scientific Computing", Maribor, Slovénie, Lecture Notes in Computer Science, Springer, 2012, vol. 7442, p. 349-360 [*DOI :* 10.1007/978-3-642-32973-9_29], http://hal.inria.fr/hal-00779259.

[33] T. ZHAO, D. WANG, H. HONG, P. AUBRY. *Real Solution Formulas of Cubic and Quartic Equations Applied to Generate Dynamic Diagrams with Inequality Constraints*, in "SAC 2012: Proceedings of the 27th ACM Symposium on Applied Computing", Riva del Garda, Italy, ACM Press, March 2012, p. 94–101 [*DOI :* 10.1145/2245276.2245297], http://hal.inria.fr/hal-00683596.

Conferences without Proceedings

[34] M. ALBRECHT, C. CID, J.-C. FAUGÈRE, R. FITZPATRICK, L. PERRET. *On the complexity of the Arora-Ge Algorithm against LWE*, in "SCC – Third international conference on Symbolic Computation and Cryptography", Castro Urdiales, Espagne, June 2012, http://hal.inria.fr/hal-00776434.

[35] M. ALBRECHT, C. CID, J.-C. FAUGÈRE, R. FITZPATRICK, L. PERRET. *On the Complexity of the BKW Algorithm on LWE*, in "SCC – Third international conference on Symbolic Computation and Cryptography", Castro Urdiales, Espagne, June 2012, http://hal.inria.fr/hal-00776069.

Scientific Books (or Scientific Book chapters)

[36] I. Z. EMIRIS, V. Y. PAN, E. TSIGARIDAS. *Algebraic Algorithms*, in "Computing Handbook Set - Computer Science", T. GONZALEZ (editor), CRC Press, 2012, vol. I, http://hal.inria.fr/hal-00776270.

[37] I. Z. EMIRIS, E. TSIGARIDAS, A. VARVITSIOTIS. *Mixed volume and distance geometry techniques for counting Euclidean embeddings of rigid graphs*, in "Distance Geometry: With Applications to Molecular Conformation and Sensor Networks", C. LAVOR, L. LIBERTI, N. MACULAN, A. MUCHERINO (editors), Springer-Verlag, 2012, http://hal.inria.fr/hal-00776252.