IN PARTNERSHIP WITH:
CNRS

Université Pierre et Marie Curie (Paris 6)

Activity Report 2017

Project-Team POLSYS

Polynomial Systems

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

RESEARCH CENTER
Paris

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Project-Team POLSYS

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

Keywords:

Computer Science and Digital Science:

A2.4. - Verification, reliability, certification
A4.3. - Cryptography
A4.3.1. - Public key cryptography
A4.3.4. - Quantum Cryptography
A5.10.1. - Design
A6.1. - Mathematical Modeling
A6.2.3. - Probabilistic methods
A6.2.6. - Optimization
A6.2.7. - High performance computing
A6.4.3. - Observability and Controlability
A8.1. - Discrete mathematics, combinatorics
A8.2. - Optimization
A8.3. - Geometry, Topology
A8.4. - Computer Algebra

Other Research Topics and Application Domains:

B5. - Industry of the future
B5.2. - Design and manufacturing
B5.2.3. - Aviation
B5.2.4. - Aerospace
B6. - IT and telecom
B6.3. - Network functions
B6.5. - Information systems
B9.4.1. - Computer science
B9.4.2. - Mathematics
B9.8. - Privacy

1. Personnel

Research Scientists

Jean-Charles Faugère [Team leader, Inria, Senior Researcher, HDR]
Elias Tsigaridas [Inria, Researcher]
Dongming Wang [CNRS, Senior Researcher, on leave at Beihang University, HDR]

Faculty Members

Jérémy Berthomieu [UPMC, Associate Professor]
Daniel Lazard [UPMC, Emeritus Professor, HDR]
Ludovic Perret [UPMC, Associate Professor, HDR]
Guénaël Renault [UPMC, Associate Professor, on leave at ANSSI, HDR]
Mohab Safey El Din [UPMC, Professor, HDR]

Post-Doctoral Fellows
Amine Mrabet [UPMC, ATER, from Sept. 2017]
Kaie Kubjas [UPMC, Post-Doctoral fellow, on leave at MIT, from Sept. 2017]

PhD Students
Ivan Bannwarth [UPMC, until Aug. 2017]
Matías Bender [Inria]
Olive Chakraborty [UPMC, from May 2017]
Nagardjun Chinthamani Dwarakanath [UPMC, from Dec. 2017]
Solane El Hirch [UPMC, from June 2017]
Thi Xuan Vu [UPMC, from Oct. 2017]

Technical staff
Jocelyn Ryckeghem [UPMC, from Apr. 2017 until Dec. 2017]

Administrative Assistants
Kevin Bonny [Inria]
Georgette Bonpapa [UPMC, Assistant, until July 2017]
Virginie Collette [Inria]
Irphane Khan [UPMC, Assistant]
Azzeddine Saidani [Inria]

External Collaborators
Emmanuel Prouff [ANSSI, Associate Member, HDR]
Victor Magron [CNRS, Researcher, from Oct. 2017]

2. Overall Objectives

2.1. Overall Objectives

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

Our main objectives are:

- **Fundamental Algorithms and Structured Systems.** The objective is to propose fast exponential exact algorithms for 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).

3. Research Program

3.1. Introduction

Polynomial system solving is a fundamental problem in Computer Algebra with many applications in cryptography, robotics, biology, error correcting codes, signal theory, ... Among all available methods for solving polynomial systems, computation of Gröbner bases remains one of the most powerful and versatile method since it can be applied in the continuous case (rational coefficients) as well as in the discrete case (finite fields). Gröbner bases are also 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: Jérémy Berthomieu, Jean-Charles Faugère, Guénaël Renault, Mohab Safey El Din, Elias Tsigaridas, Dongming Wang, Matías Bender, Thi Xuan Vu.

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.

[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.

3.3. Solving Systems over the Reals and Applications.

Participants: Mohab Safey El Din, Elias Tsigaridas, Daniel Lazard, Ivan Bannwarth, Thi Xuan Vu.

We shall 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.

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, Elias Tsigaridas, Olive Chakraborty, Jocelyn Ryckeghem.

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 these 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. The FGBlibrary is an efficient one 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 algebra 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 a 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 basis 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 bottleneck 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 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: Jérémy Berthomieu, Jean-Charles Faugère, Ludovic Perret, Guénaël Renault, Olive Chakraborty, Nagardjun Chinthamani, Solane El Hirch, Jocelyn Ryckeghem.

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*.

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

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.

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. Highlights of the Year

4.1. Highlights of the Year

Dongming Wang has been elected as a Member of the Academia Europaea.

Elias Tsigaridas was awarded an ANR "Jeune Chercheur Grant". The title of the project is GALOP (Games through the lens of ALgebra and OPptimization)

5. New Software and Platforms

5.1. Epsilon

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

- Contact: Dongming Wang
- URL: http://wang.cc4cm.org/epsilon/index.html

5.2. FGb

KEYWORDS: Gröbner bases - Nonlinear system - Computer algebra

FUNCTIONAL DESCRIPTION: FGb is a powerful software for computing Gröbner 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.

- Participant: Jean Charles Faugere
- Contact: Jean-Charles Faugère
- URL: http://www-polsys.lip6.fr/~jcf/FGb/index.html

5.3. FGb Light

FUNCTIONAL DESCRIPTION: Gröbner basis computation modulo p (p is a prime integer of 16 bits).

- Participant: Jean-Charles Faugère
- Contact: Jean-Charles Faugère
- URL: http://www-polsys.lip6.fr/~jcf/FGb/index.html

5.4. GBLA

FUNCTIONAL DESCRIPTION: GBLA is an open source C library for linear algebra specialized for eliminating matrices generated during Gröbner basis computations in algorithms like F4 or F5.

- Contact: Jean-Charles Faugère
- URL: http://www-polsys.lip6.fr/~jcf/GBLA/index.html

5.5. HFEBoost

FUNCTIONAL DESCRIPTION: Public-key cryptography system enabling an authentification of dematerialized data.

- Authors: Jean-Charles Faugère and Ludovic Perret
- Partner: UPMC
- Contact: Jean-Charles Faugère
- URL: http://www-polsys.lip6.fr/Links/hfeboost.html

5.6. RAGlib

Real Algebraic Geometry library
FUNCTIONAL DESCRIPTION: RAGLib is a powerful library, written in Maple, dedicated to solving over the reals polynomial systems. It is based on the FGb library for computing Grobner bases. It provides functionalities for deciding the emptiness and/or computing sample points to real solution sets of polynomial systems of equations and inequalities. This library provides implementations of the state-of-the-art algorithms with the currently best known asymptotic complexity for those problems.

- Contact: Mohab Safey El Din
- URL: http://www-polsys.lip6.fr/~safey/RAGLib/

5.7. SLV

FUNCTIONAL DESCRIPTION: SLV is a software package in C that provides routines for isolating (and subsequently refine) the real roots of univariate polynomials with integer or rational coefficients based on subdivision algorithms and on the continued fraction expansion of real numbers. Special attention is given so that the package can handle polynomials that have degree several thousands and size of coefficients hundrends of Megabytes. Currently the code consists of approx. 5000 lines.

- Contact: Elias Tsigaridas
- URL: http://www-polsys.lip6.fr/~elias/soft

5.8. SPECTRA

Semidefinite Programming solved Exactly with Computational Tools of Real Algebra
KEYWORD: Linear Matrix Inequalities
FUNCTIONAL DESCRIPTION: SPECTRA is a Maple library devoted to solving exactly Semi-Definite Programs. It can handle rank constraints on the solution. It is based on the FGb library for computing Gröbner bases and provides either certified numerical approximations of the solutions or exact representations thereof.

- Contact: Mohab Safey El Din
- URL: http://homepages.laas.fr/henrion/software/spectra/

6. New Results

6.1. Fundamental algorithms and structured polynomial systems

6.1.1. Linear Algebra for Computing Gröbner Bases of Linear Recursive Multidimensional Sequences

The so-called Berlekamp – Massey – Sakata algorithm computes a Gröbner basis of a 0-dimensional ideal of relations satisfied by an input table. It extends the Berlekamp – Massey algorithm to n-dimensional tables, for $n > 1$.

In [1], we investigate this problem and design several algorithms for computing such a Gröbner basis of an ideal of relations using linear algebra techniques. The first one performs a lot of table queries and is analogous to a change of variables on the ideal of relations.

As each query to the table can be expensive, we design a second algorithm requiring fewer queries, in general. This FGLM-like algorithm allows us to compute the relations of the table by extracting a full rank submatrix of a *multi-Hankel* matrix (a multivariate generalization of Hankel matrices).

Under some additional assumptions, we make a third, adaptive, algorithm and reduce further the number of table queries. Then, we relate the number of queries of this third algorithm to the *geometry* of the final staircase and we show that it is essentially linear in the size of the output when the staircase is convex. As a direct application to this, we decode n-cyclic codes, a generalization in dimension n of Reed Solomon codes.

We show that the multi-Hankel matrices are heavily structured when using the LEX ordering and that we can speed up the computations using fast algorithms for quasi-Hankel matrices. Finally, we design algorithms for computing the generating series of a linear recursive table.

6.1.2. In-depth comparison of the Berlekamp – Massey – Sakata and the Scalar-FGLM algorithms: the non adaptive variants

In [22], we compare thoroughly the BERLEKAMP – MASSEY – SAKATA algorithm and the SCALAR-FGLM algorithm, which compute both the ideal of relations of a multidimensional linear recurrent sequence.

Suprisingly, their behaviors differ. We detail in which way they do and prove that it is not possible to tweak one of the algorithms in order to mimic exactly the behavior of the other.

6.1.3. Resultants and Discriminants for Bivariate Tensor-product Polynomials

Optimal resultant formulas have been systematically constructed mostly for *unmixed polynomial systems*, that is, systems of polynomials which all have the same support. However, such a condition is restrictive, since *mixed systems* of equations arise frequently in practical problems. In [16] we present a square, *Koszul-type* matrix expressing the resultant of arbitrary (mixed) bivariate *tensor-product systems*. The formula generalizes the classical Sylvester matrix of two univariate polynomials, since it expresses a map of *degree one*, that is, the entries of the matrix are simply coefficients of the input polynomials. Interestingly, the matrix expresses a primal-dual multiplication map, that is, the tensor product of a univariate multiplication map with a map expressing derivation in a dual space. Moreover, for tensor-product systems with more than two (affine) variables, we prove an impossibility result: no universal degree-one formulas are possible, unless the system is unmixed. We also present applications of the new construction in the computation of discriminants and mixed discriminants as well as in solving systems of bivariate polynomials with tensor-product structure.

6.1.4. Sparse Rational Univariate Representation

In [15] we present explicit worst case degree and height bounds for the rational univariate representation of the isolated roots of polynomial systems based on mixed volume. We base our estimations on height bounds of resultants and we consider the case of 0-dimensional, positive dimensional, and parametric polynomial systems.

Multi-homogeneous polynomial systems arise in many applications. In [11], we provide bit complexity estimates for representing the solutions of these systems. These are the best currently known bounds. The assumptions essentially imply that the Jacobian matrix of the system under study has maximal rank at the solution set and that this solution set is finite.

We do not only obtain bounds but an algorithm is also given for solving such systems. We give bit complexity estimates which, up to a few extra other factors, are quadratic in the number of solutions and linear in the height of the input system, under some genericity assumptions.

The algorithm is probabilistic and a probability analysis is provided. Next, we apply these results to the problem of optimizing a linear map on the real trace of an algebraic set. Under some genericity assumptions, we provide bit complexity estimates for solving this polynomial minimization problem.

6.1.5. Improving Root Separation Bounds

Let f be a polynomial (or polynomial system) with all simple roots. The root separation of f is the minimum of the pair-wise distances between the complex roots. A root separation bound is a lower bound on the root separation. Finding a root separation bound is a fundamental problem, arising in numerous disciplines. In [7] we present two new root separation bounds: one univariate bound, and one multivariate bound. The new bounds improve on the old bounds in two ways: (1) The new bounds are usually significantly bigger (hence better) than the previous bounds. (2) The new bounds scale correctly, unlike the previous bounds. Crucially, the new bounds are not harder to compute than the previous bounds.

6.1.6. Accelerated Approximation of the Complex Roots and Factors of a Univariate Polynomial

The known algorithms approximate the roots of a complex univariate polynomial in nearly optimal arithmetic and Boolean time. They are, however, quite involved and require a high precision of computing when the degree of the input polynomial is large, which causes numerical stability problems. In [8] we observe that these difficulties do not appear at the initial stages of the algorithms, and in our present paper we extend one of these stages, analyze it, and avoid the cited problems, still achieving the solution within a nearly optimal complexity estimates, provided that some mild initial isolation of the roots of the input polynomial has been ensured. The resulting algorithms promise to be of some practical value for root-finding and can be extended to the problem of polynomial factorization, which is of interest on its own right. We conclude with outlining such an extension, which enables us to cover the cases of isolated multiple roots and root clusters.

6.1.7. Nearly optimal computations with structured matrices

In [9] we estimate the Boolean complexity of multiplication of structured matrices by a vector and the solution of nonsingular linear systems of equations with these matrices. We study four basic and most popular classes, that is, Toeplitz, Hankel, Cauchy and Vandermonde matrices, for which the cited computational problems are equivalent to the task of polynomial multiplication and division and polynomial and rational multipoint evaluation and interpolation. The Boolean cost estimates for the latter problems have been obtained by Kirrinnis, except for rational interpolation. We supply them now as well as the Boolean complexity estimates for the important problems of multiplication of transposed Vandermonde matrix and its inverse by a vector. All known Boolean cost estimates for such problems rely on using Kronecker product. This implies the d-fold precision increase for the d-th degree output, but we avoid such an increase by relying on distinct techniques based on employing FFT. Furthermore we simplify the analysis and make it more transparent by combining the representations of our tasks and algorithms both via structured matrices and via polynomials and rational functions. This also enables further extensions of our estimates to cover Trummer's important problem and computations with the popular classes of structured matrices that generalize the four cited basic matrix classes, as well as the transposed Vandermonde matrices. It is known that the solution of Toeplitz, Hankel, Cauchy, Vandermonde, and transposed Vandermonde linear systems of equations is generally prone to numerical stability problems, and numerical problems arise even for multiplication of Cauchy, Vandermonde, and transposed Vandermonde matrices by a vector. Thus our FFT-based results on the Boolean complexity of these important computations could be quite interesting because our estimates are reasonable even for more general classes of structured matrices, showing rather moderate growth of the complexity as the input size increases.

6.1.8. Sliding solutions of second-order differential equations with discontinuous right-hand side

In [2], we consider second-order ordinary differential equations with discontinuous right-hand side. We analyze the concept of solution of this kind of equations and determine analytical conditions that are satisfied by typical solutions. Moreover, the existence and uniqueness of solutions and sliding solutions are studied.

6.1.9. Sparse FGLM algorithms

Given a zero-dimensional ideal $I \subset \mathbb{K}[x_1, ..., x_n]$ of degree D, the transformation of the ordering of its Gröbner basis from DRL to LEX is a key step in polynomial system solving and turns out to be the bottleneck of the whole solving process. Thus it is of crucial importance to design efficient algorithms to perform the change of ordering. The main contributions of [3] are several efficient methods for the change of ordering which take advantage of the sparsity of multiplication matrices in the classical *FGLM* algorithm. Combining all these methods, we propose a deterministic top-level algorithm that automatically detects which method to use depending on the input. As a by-product, we have a fast implementation that is able to handle ideals of degree over $40,000$. Such an implementation outperforms the *Magma* and *Singular* ones, as shown by our experiments. First for the shape position case, two methods are designed based on the Wiedemann algorithm: the first is probabilistic and its complexity to complete the change of ordering is $O(D(N_1 + n \log D))$, where N_1 is the number of nonzero entries of a multiplication matrix; the other is deterministic and computes the LEX Gröbner basis of $\sqrt{I}$ via Chinese Remainder Theorem. Then for the general case, the designed method is characterized by the Berlekamp–Massey–Sakata algorithm from Coding Theory to handle the multi-dimensional linearly recurring relations. Complexity analyses of all proposed methods are also provided. Furthermore, for generic polynomial systems, we present an explicit formula for the estimation of the sparsity of one main multiplication matrix, and prove its construction is free. With the asymptotic analysis of such sparsity, we are able to show for generic systems the complexity above becomes $O(\sqrt{6/n\pi} D^{2+\frac{n-1}{n}})$.

6.2. Solving Systems over the Reals and Applications

6.2.1. Answering connectivity queries in real algebraic sets

A roadmap for a semi-algebraic set S is a curve which has a non-empty and connected intersection with all connected components of S. Hence, this kind of object, introduced by Canny, can be used to answer connectivity queries (with applications, for instance, to motion planning) but has also become of central importance in effective real algebraic geometry, since it is used in higher-level algorithms. In [10], we provide a probabilistic algorithm which computes roadmaps for smooth and bounded real algebraic sets. Its output size and running time are polynomial in $(nD)^{n \log d}$, where D is the maximum of the degrees of the input polynomials, d is the dimension of the set under consideration and n is the number of variables. More precisely, the running time of the algorithm is essentially subquadratic in the output size. Even under our assumptions, it is the first roadmap algorithm with output size and running time polynomial in $(nD)^{n \log d}$.

6.2.2. Polynomial optimization and semi-definite programming

In [6], we describe our freely distributed Maple library spectra, for Semidefinite Programming solved Exactly with Computational Tools of Real Algebra. It solves linear matrix inequalities, a fundamental object in effective real algebraic geometry and polynomial optimization, with symbolic computation in exact arithmetic and it is targeted to small-size, possibly degenerate problems for which symbolic infeasibility or feasibility certificates are required.

The positive semidefinite rank of a convex body C is the size of its smallest positive semi-definite formulation. In [5], we show that the positive semidefinite rank of any convex body C is at least $\sqrt{\log(d)}$ where d is the smallest degree of a polynomial that vanishes on the boundary of the polar of C. This improves on the existing bound which relies on results from quantifier elimination. Our proof relies on the Bézout bound applied to the Karush-Kuhn-Tucker conditions of optimality. We discuss the connection with the algebraic degree of semidefinite programming and show that the bound is tight (up to constant factor) for random spectrahedra of suitable dimension.

6.2.3. The Complexity of an Adaptive Subdivision Method for Approximating Real Curves

In [14] we present the first complexity analysis of the algorithm by Plantinga and Vegter for approximating real implicit curves and surfaces. This approximation algorithm certifies the topological correctness of the output using both subdivision and interval arithmetic. In practice, it has been seen to be quite efficient; our goal is to quantify this efficiency. We focus on the subdivision step (and not the approximation step) of the Plantinga and Vegter algorithm. We begin by extending the subdivision step to arbitrary dimensions. We provide *a priori* worst-case bounds on the complexity of this algorithm both in terms of the number of subregions constructed and the bit complexity for the construction. Then, we use continuous amortization to derive adaptive bounds on the complexity of the subdivided region. We also provide examples showing our bounds are tight.

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

6.3.1. Private Multiplication over Finite Fields

The notion of privacy in the probing model, introduced by Ishai, Sahai, and Wagner in 2003, is nowadays frequently involved to assess the security of circuits manipulating sensitive information. However, provable security in this model still comes at the cost of a significant overhead both in terms of arithmetic complexity and randomness complexity. In [13], we deal with this issue for circuits processing multiplication over finite fields. Our contributions are manifold. Extending the work of Belaïd, Benhamouda, Passelègue, Prouff, Thillard, and Vergnaud at Eurocrypt 2016, we introduce an algebraic characterization of the privacy for multiplication in any finite field and we propose a novel algebraic characterization for non-interference (a stronger security notion in this setting). Then, we present two generic constructions of multiplication circuits in finite fields that achieve non-interference in the probing model. The second proposal achieves a linear complexity in terms of randomness consumption. This complexity is proved to be almost optimal. Eventually, we show that our constructions can always be instantiated in large enough finite fields.

6.3.2. Convolutional Neural Networks with Data Augmentation Against Jitter-Based Countermeasures - Profiling Attacks Without Pre-processing

In the context of the security evaluation of cryptographic implementations, profiling attacks (aka Template Attacks) play a fundamental role. Nowadays the most popular Template Attack strategy consists in approximating the information leakages by Gaussian distributions. Nevertheless this approach suffers from the difficulty to deal with both the traces misalignment and the high dimensionality of the data. This forces the attacker to perform critical preprocessing phases, such as the selection of the points of interest and the temporal realignment of measurements. Some software and hardware countermeasures have been conceived exactly to create such a misalignment. In [17], we propose an end-to-end profiling attack strategy based on Deep Learning algorithms combined with Data Augmentation strategies.

6.3.3. Submissions to the NIST Post-Quantum Standardization Process

We have submitted three cryptosystems to the current process leads by NIST for standardizing post-quantum public-key algorithms.

6.3.3.1. GeMSS

The acronym stands for a Great Multivariate Signature Scheme [18]. As suggested by its name, *GeMSS* is a multivariate-based signature scheme producing small signatures. It has a fast verification process, and a medium/large public-key. *GeMSS* is in direct lineage from QUARTZ and borrows some design rationale of the Gui multivariate signature scheme. The former schemes are built from the *Hidden Field Equations* crypotsystem (HFE) by using the so-called minus and vinegar modifiers. It is fair to say that HFE and its variants, are the most studied schemes in multivariate cryptography. QUARTZ produces signatures of 128 bits for a security level of 80 bits and was submitted to the *Nessie Ecrypt* competition for public-key signatures. In contrast to many multivariate schemes, no practical attack has been reported against QUARTZ. This is remarkable knowing the intense activity in the cryptanalysis of multivariate schemes.

GeMSS is a faster variant of QUARTZ that incorporates the latest results in multivariate cryptography to reach higher security levels than QUARTZ whilst improving efficiency.

6.3.3.2. DualModeMS

DualModeMS [20] is a multivariate-based signature scheme with a rather peculiar property. Its public-key is small whilst the signature is large. This is in sharp contrast with traditional multivariate signature schemes based on the so-called *Matsumoto and Imai* (MI) principle, such as QUARTZ or Gui, that produce short signatures but have larger public-keys.

DualModeMS is based on the method proposed by A. Szepieniec, W. Beullens, and B. Preneel at PQC'17 where they present a generic technique permitting to transform any (MI-based multivariate signature scheme into a new scheme with much shorter public-key but larger signatures. This technique can be viewed as a *mode of operations* that offers a new flexibility for MI-like signature schemes. Thus, we believe that *DualModeMS* could also be useful for others multivariate-based signature candidates proposed to NIST.

6.3.3.3. CPFKM

CPFKM [19] is a based on the problem of solving a system of noisy non-linear polynomials, also known as the PoSSo with Noise Problem. Our scheme largely borrows its design rationale from key encapsulation schemes based on the Learning With Errors (LWE) problem and its derivatives. The main motivation of building this scheme is to have a key exchange and encapsulation scheme based on the hardness of solving system of noisy polynomials.

6.3.4. The Point Decomposition Problem over Hyperelliptic Curves: toward efficient computations of Discrete Logarithms in even characteristic

Computing discrete logarithms is generically a difficult problem. For divisor class groups of curves defined over extension fields, a variant of the Index-Calculus called Decomposition attack is used, and it can be faster than generic approaches. In this situation, collecting the relations is done by solving multiple instances of

the Point m-Decomposition Problem (PDP_m). An instance of this problem can be modelled as a zero-dimensional polynomial system. Solving is done with Gröbner bases algorithms, where the number of solutions of the system is a good indicator for the time complexity of the solving process. For systems arising from a PDP_m context, this number grows exponentially fast with the extension degree. To achieve an efficient harvesting, this number must be reduced as much as possible. Extending the elliptic case, we introduce in [4] a notion of Summation Ideals to describe PDP_m instances over higher genus curves, and compare to Nagao's general approach to PDP_m. In even characteristic we obtain reductions of the number of solutions for both approaches, depending on the curve's equation. In the best cases, for a hyperelliptic curve of genus g, we can divide the number of solutions by $2^{(n-1)(g+1)}$. For instance, for a type II genus 2 curve defined over $\mathbb{F}_{293}$ whose divisor class group has cardinality a near-prime 184 bits integer, the number of solutions is reduced from 4096 to 64. This is enough to build the matrix of relations in around 7 days with 8000 cores using a dedicated implementation.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Grants with Industry

Until the mid 2000's, multivariate cryptography was developing very rapidly, producing many interesting and versatile public-key schemes. However, many of them were soon successfully cryptanalysed (a lot have been done in this group). As a consequence, the confidence in multivariate cryptography cryptosystems declined. It seems that there have emerged new important reasons for renewal of the interest in a new generation of multivariate schemes. In the past two years, the algorithms for solving the Discrete Logarithm Problem over small characteristic fields underwent an extraordinary development. This clearly illustrates the risk to not consider alternatives to classical assumptions based on number theory. In parallel, two of the most important standardization bodies in the world, NIST and ETSI have recently started initiatives for developing cryptographic standards not based on number theory, with a particular focus on primitives resistant to quantum algorithms. An objective here is then to focus on the design of multivariate schemes.

The team is involved in the industrial transfer of post-quantum cryptography. The maturation project, called HFEBOOST, is supervised by SATT-LUTECH.

SATT-LUTECH specializes in the processing and transfer of technologies from research laboratories of its shareholders: Inria, CNRS, University of Technology of Compiègne, National Museum of Natural History, Institute Curie, Université Panthéon-Assas, Paris Sorbonne University and National School of Industrial Creation).

The team has recently developed, in partnership with a mobile application development company (WASSA), an Android app for smartphones (Samsung S5 type) that uses multivariate cryptography. The application has been tested mid-November in a series of experiments supervised by DGA and French Ministry of Defense. The experiment gathered a total of hundred participants from various operational units. This is a first milestone in the maturation project whose goal is to create a start-up.

7.2. Public Contracts

CEA LETI / DSYS / CESTI

In smart card domain, the emanations of a component during a cryptographic computation may compromise the information that is directly or not linked to the secret keys. The most part of the side channel attacks are based on statistical tools that exploit relations between the handled data and the signals. However these methods do not take advantage of all the signal information. The goal is to study the existing algorithms in pattern and speech recognition and to apply them to signals related to cryptographic computations. The objective will be to improve the attacks efficiency and resolve more complex problems.

8. Partnerships and Cooperations

8.1. Regional Initiatives

- **French Ministry of Armies**

  POLSYS has a collaboration with the French Ministry of Armies.

- **Grant GAMMA** (funded by PGMO).

  GLOBAL ALGEBRAIC SHOOTING METHOD IN OPTIMAL CONTROL AND APPLICATIONS

  Optimal control consists in steering a system from an initial configuration to a final one, while minimizing some given cost criterion. One of the current main challenges is to develop innovative methods for computing global solutions. This is crucial for applications where validating the global control laws is a crucial but a highly time consuming and expensive phase. GAMMA focuses on the wide range of optimal control problems having an algebraic structure, involving for instance polynomial or semi-algebraic dynamics and costs, or switches between polynomial models. In this case, GAMMA aims at designing methods relying on algebraic computations to the mainstream shooting method in order to yield optimal solutions that purely numerical techniques cannot provide.

8.2. National Initiatives

8.2.1. ANR

- **ANR Jeunes Chercheurs GALOP (Games through the lens of ALgebra and OPptimization)**

  `Duration:` 2018–2022

  GALOP is a Young Researchers (JCJC) project with the purpose of extending the limits of the state-of-the-art algebraic tools in computer science, especially in stochastic games. It brings original and innovative algebraic tools, based on symbolic-numeric computing, that exploit the geometry and the structure and complement the state-of-the-art. We support our theoretical tools with a highly efficient open-source software for solving polynomials. Using our algebraic tools we study the geometry of the central curve of (semi-definite) optimization problems. The algebraic tools and our results from the geometry of optimization pave the way to introduce algorithms and precise bounds for stochastic games.

  `Participants:` E. Tsigaridas [contact], F. Johansson, H. Gimbert, J.-C. Faugère, M. Safey El Din.

8.2.2. Programme d'investissements d'avenir (PIA)

- **PIA grant RISQ: Regroupement of the Security Industry for Quantum-Safe security (2017-2020).** The goal of the RISQ project is to prepare the security industry to the upcoming shift of classical cryptography to quantum-safe cryptography. (J.-C. Faugère [contact], and L. Perret).

  The RISQ project is certainly the biggest industrial project ever organized in quantum-safe cryptography. RISQ is one of few projects accepted in the call Grands Défis du Numérique which is managed by BPI France, and will be funded thanks to the so-called Plan d'Investissements d'Avenir.

  The RISQ project is a natural continuation of POLSYS commitment to the industrial transfert of quantum-safe cryptography. RISQ is a large scale version of the HFEBoost project; which demonstrated the potential of quantum-safe cryptography.

  POLSYS actively participated to shape the RISQ project. POLSYS is now a member of the strategic board of RISQ, and is leading the task of designing and analyzing quantum-safe algorithms. In particular, a first milestone of this task was to prepare submissions to NIST's quantum-safe standardisation process.

8.3. European Initiatives

8.3.1. FP7 & H2020 Projects

8.3.1.1. A3

Type: PEOPLE

Instrument: Career Integration Grant

Duration: May 2013 - Apr. 2017

Coordinator: Jean-Charles Faugère

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

Inria contact: Elias Tsigaridas

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

8.3.2. Collaborations in European Programs, Except FP7 & H2020

Program: COST

Project acronym: CryptoAction

Project title: Cryptography for Secure Digital Interaction

Duration: Apr. 2014 - Apr. 2018

Coordinator: Claudio ORLANDI

Abstract: As increasing amounts of sensitive data are exchanged and processed every day on the Internet, the need for security is paramount. Cryptography is the fundamental tool for securing digital interactions, and allows much more than secure communication: recent breakthroughs in cryptography enable the protection - at least from a theoretical point of view - of any interactive data processing task. This includes electronic voting, outsourcing of storage and computation, e-payments, electronic auctions, etc. However, as cryptography advances and becomes more complex, single research groups become specialized and lose contact with "the big picture". Fragmentation in this field can be dangerous, as a chain is only as strong as its weakest link. To ensure that the ideas produced in Europe's many excellent research groups will have a practical impact, coordination among national efforts and different skills is needed. The aim of this COST Action is to stimulate interaction between the different national efforts in order to develop new cryptographic solutions and to evaluate the security of deployed algorithms with applications to the secure digital interactions between citizens, companies and governments. The Action will foster a network of European research centers thus promoting movement of ideas and people between partners.

Program: COST

Project acronym: CRYPTACUS

Project title: Cryptanalysis of ubiquitous computing systems

Duration: Dec. 2014 - Dec. 2018

Coordinator: Gildas AVOINE

Abstract: Recent technological advances in hardware and software have irrevocably affected the classical picture of computing systems. Today, these no longer consist only of connected servers, but involve a wide range of pervasive and embedded devices, leading to the concept of "ubiquitous computing systems". The objective of the Action is to improve and adapt the existent cryptanalysis methodologies and tools to the ubiquitous computing framework. Cryptanalysis, which is the assessment of theoretical and practical cryptographic mechanisms designed to ensure security and privacy, will be implemented along four axes: cryptographic models, cryptanalysis of building blocks, hardware and software security engineering, and security assessment of real-world systems. Researchers have only recently started to focus on the security of ubiquitous computing systems. Despite the critical flaws found, the required highly-specialized skills and the isolation of the involved disciplines are a true barrier for identifying additional issues. The Action will establish a network of complementary skills, so that expertise in cryptography, information security, privacy, and embedded systems can be put to work together. The outcome will directly help industry stakeholders and regulatory bodies to increase security and privacy in ubiquitous computing systems, in order to eventually make citizens better protected in their everyday life.

8.4. International Initiatives

8.4.1. Inria Associate Teams Not Involved in an Inria International Labs

8.4.1.1. GOAL

Title: Geometry and Optimization with ALgebraic methods.

International Partner (Institution - Laboratory - Researcher):

University of California Berkeley (United States) - Dept. of Mathematics - Bernd Sturmfels

Start year: 2015

See also: http://www-polsys.lip6.fr/GOAL/index.html

Polynomial optimization problems form a subclass of general global optimization problems, which have received a lot of attention from the research community recently; various solution techniques have been designed. One reason for the spectacular success of these methods is the potential impact in many fields: data mining, big data, energy savings, etc. More generally, many areas in mathematics, as well as applications in engineering, biology, statistics, robotics etc. require a deeper understanding of the algebraic structure of their underlying objects.

A new trend in the polynomial optimization community is the combination of algebraic and numerical methods. Understanding and characterizing the algebraic properties of the objects occurring in numerical algorithms can play an important role in improving the efficiency of exact methods. Moreover, this knowledge can be used to estimate the quality (for example the number of significant digits) of numerical algorithms. In many situations each coordinate of the optimum is an algebraic number. The degree of the minimal polynomials of these algebraic numbers is the Algebraic Degree of the problem. From a methodological point of view, this notion of Algebraic Degree emerges as an important complexity parameter for both numerical and the exact algorithms. However, algebraic systems occurring in applications often have special algebraic structures that deeply influence the geometry of the solution set. Therefore, the (true) algebraic degree could be much less than what is predicted by general worst case bounds (using Bézout bounds, mixed volume, etc.), and would be very worthwhile to understand it more precisely.

The goal of this proposal is to develop algorithms and mathematical tools to solve geometric and optimization problems through algebraic techniques. As a long-term goal, we plan to develop new software to solve these problems more efficiently. These objectives encompass the challenge of identifying instances of these problems that can be solved in polynomial time with respect to the number of solutions and modeling these problems with polynomial equations.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

- May – July 2017, Delaram Kahrobaei, Professor, CUNY, NYC, USA

8.5.1.1. Internships

- May – July 2017, Kelsey Horan, PhD student, CUNY, NYC, USA.
- Apr. – Nov. 2017, Eliane Koussa, Université de Versailles
- Apr. – Aug. 2017, Pascal Fong, Université de Versailles

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. Member of the Organizing Committees

Emmanuel Prouff was a member of the organization committee of Eurocrypt 2017 (Paris, France, 2017, April 30 - May 4).

Jean-Charles Faugère and Ludovic Perret were members of the organization committee of the Quantum-Safe Cryptography for Industry (Paris, France, 2017, April 30).

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

Mohab Safey El Din was PC Chair of the International Symposium on Symbolic and Algebraic Computation (ISSAC), Kaiserslautern, Germany, 2017.

Jean-Charles Faugère was PC co-Chair of the International workshop on Parallel Symbolic Computation (PASCO), Kaiserslautern, Germany, 2017.

9.1.2.2. Member of the Conference Program Committees

Ludovic Perret was a member of the program-committee of

- 20th IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC'17), Amsterdam, 28-31 March 2017

Emmanuel Prouff was a member of the steering committees of the following conferences

- Conference on Cryptographic Hardware and Embedded Systems 2017 (CHES 2017) (Taipei, Taiwan, 2017, Sept. 25-28);
- Smart Card Research and Advanced Application Conference (CARDIS 2017) (Lugano, Switzerland, 2017, Nov. 13-17).

Guénaël Renault was a member of the program committee of

- 7th Int'l Conference on Mathematical Aspects of Computer and Information Sciences (MACIS) 2017;

Elias Tsigaridas was a member of the program committees of the following conferences

- 7th Int'l Conference on Mathematical Aspects of Computer and Information Sciences (MACIS) 2017;
- 19th International Workshop on Computer Algebra in Scientific Computing (CASC) 2017.

Dongming Wang was a member of the program committees of the following conferences

- 11th International Workshop on Automated Deduction in Geometry (ADG 2016) (Strasbourg, France, June 27-29, 2016);
- 8th International Symposium on Symbolic Computation in Software Science (SCSS 2017) (Gammarth, Tunisia, 2017, April 6-9).

Dongming Wang was a member of the steering committees of the following conferences

- International Conference on Mathematical Aspects of Computer and Information Sciences (MACIS),
- International Symposium on Symbolic Computation in Software Science (SCSS).

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

Ludovic Perret is an Associate Editor for:

- Designs, Codes and Cryptography (Springer, Berlin).
- The Computer Journal (Oxford University Press)
- Groups, Complexity, Cryptology (De Gruyter)

Emmanuel Prouff is an Associate Editor of the Journal of Cryptographic Engineering (Springer, Berlin).

Mohab Safey El Din is an Associate Editor of the Journal of Symbolic Computation.

Dongming Wang has the following editorial activities:

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

9.1.4. Invited Talks

Jean-Charles Faugère was a plenary invited speaker at the

- SIAM Conference on Applied Algebraic Geometry, Atlanta (August 2017).

Ludovic Perret was invited speaker at the

- HEXATRUST Summer school 2017 (Paris, September 2017)

Emmanuel Prouff was invited speaker at the

- Journées du GDR-IM (Montpellier, France, 2017, Mar. 14-16).
- Aix-Marseille Cyber Security Forum (AMUSEC) (Marseille, France, 2017, Oct. 12-13).

Guénaël Renault was invited speaker at the

- Third French-Japanese Meeting on Cybersecurity (Tokyo, Japan, April 2017)

Mohab Safey El Din was invited speaker at:

- The mini-symposium on Euclidean Distance Degree at the 2017 SIAM Conference on Applied Algebraic Geometry, Atlanta, USA 2017;
- The math. seminar of the University of Dortmund, Germany;
- The Berlin-Leipzig Seminar on Algebra, Geometry and Combinatorics, Germany;
- The mini-symposium on Numeric and Symbolic Convex Programming for Polynomial Optimization, at the PGMO days, Saclay, France.

Dongming Wang invited speaker at the

- 7th International Conference on Mathematical Aspects of Computer and Information Sciences (Vienna, Austria, 2017, Nov. 15-17).
- 19th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (Timisoara, Romania, 2017, Sept. 21-24).
- 5th Summer School in Symbolic Computation (Nanning, China, 2017, July 16-22).

9.1.5. Scientific Expertise

Mohab Safey El Din was evaluator for the FWF International Program (Austrian funding agency).

Jean-Charles Faugère was the head of the hiring Committee for an associate professor in Grenoble.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Jérémy Berthomieu had the following teaching activities:

Master : Computation Modeling, 35 hours, M1, Université Pierre-et-Marie-Curie, France.

Master : In charge of Basics of Algebraic Algorithms, 73 hours, M1, Université Pierre-et-Marie-Curie & Polytech' UPMC, France.

Master : Introduction to Security, 20 hours, M1, Université Pierre-et-Marie-Curie, France.

Master : Projects supervision, 8 hours, M1, Université Pierre-et-Marie-Curie, France.

Licence : Introduction to Algorithmics, 40,5 hours, L2, Université Pierre-et-Marie-Curie, France.

Licence : Representations and Numerical Methods, 38,5 hours, L2, Université Pierre-et-Marie-Curie, France.

Licence : Projects supervision, 10 hours, L2, Université Pierre-et-Marie-Curie, France.

Jean-Charles Faugère had the following teaching activities:

Master: Fundamental Algorithms in Real Algebraic Geometry, 13,5 hours, M2, ENS de Lyon, France.

Master : Polynomial Systems solving, 12 hours, M2, MPRI, France.

Ludovic Perret is teaching a full service (192 hours), balanced between master and licence in cryptography, complexity and introduction to algorithms.

Mohab Safey El Din had the following teaching activities:

Master : In charge of Modeling and problems numerical and symbolic solving through MAPLE and MATLAB software, 36 hours, M1, Université Pierre-et-Marie-Curie, France

Master : In charge of Introduction to polynomial system solving, 48 hours, M2, Université Pierre-et-Marie-Curie, France

Master : In charge of the Security, Reliability and Numerical Efficiency Program in Master, 40 hours, M1 and M2, Université Pierre-et-Marie-Curie, France

Licence : Introduction to Cryptology, 20 hours, L3, Université Pierre-et-Marie-Curie, France

9.2.2. Supervision

PhD in progress : Ivan Bannwarth, Fast algorithms for studying real algebraic sets, started in Sept. 2014, Mohab Safey El Din.

PhD in progress : Matías Bender, Algorithms for Sparse Gröbner basis and applications, started in Dec. 2015, Jean-Charles Faugère and Elias Tsigaridas.

PhD in progress : Eleonora Cagli, Analysis and interest points research in the attacks by observation context, Emmanuel Prouff.

PhD in progress : Loïc Masure, Recognition and Side Channel Analysis, Emmanuel Prouff.

PhD in progress, Olive Chakraborty, Design and Analysis of Post-Quantum Schemes, started in May 2017, Jean-Charles Faugère and Ludovic Perret.

PhD in progress, Nagardjun Chinthamani Dwarakanath, Design and Analysis of Fully Homomorphic Schemes, started in Dec. 2017, Jean-Charles Faugère and Ludovic Perret.

PhD in progress, Solane El Hirch Design and Analysis of Post-Quantum Schemes, started in June 2017, Jean-Charles Faugère and Ludovic Perret.

PhD in progress, Xuan Vu. Algorithms for solving structured semi-algebraic systems, started in October 2017, Jean-Charles Faugère and Mohab Safey El Din.

9.2.3. Juries

Emmanuel Prouff was examiner in the PhD committee of N. Bruneau and M. Dugardin and in the HDR committees of J.-M. Dutertre and N. El Mrabet.

Guénaël Renault was referee in the Phd committee of T. Mefenza.

9.3. Popularization

The activity of POLSYS in post-quantum cryptography has been covered in several large audience magazines:

- "Enfin! La révolution quantique", L'Usine Nouvelle, November 2017.
- "QUANTIQUE : THE NEXT BIG THING(K)", L'Informaticien, November 2017.
- "L'ORDINATEUR QUANTIQUE VA-T-IL METTRE À MAL LA CYBERSÉCURITÉ MONDIALE?", Bouygues Blog, October 2017.

Ludovic Perret is member of the Cloud Security Alliance (CSA) quantum-safe security working group. In particular, he contributed to the following documents:

- B. Huttner, J. Melia, G. Carter, L. Perret and L. Wilson. "Applied Quantum-Safe Security", Feb. 2017.
- B. Huttner, J. Melia, G. Carter, L. Perret and L. Wilson. "Quantum Safe Security Glossary", January 2017.

Ludovic Perret is also member of the quantum-safe cryptography specification group of the European Telecommunications Standards Institute (ETSI) where is the referee for a document on quantum-safe signatures.

Since May 2010, Daniel Lazard is engaged in a strong edition work on the English Wikipedia (more than 6 000 contributions, including vandalism revert and talk pages). Initially focused on the themes of POLSYS, these contributions were later enlarged to general algebra and algebraic geometry, because many elementary articles require to be expanded to be useful as a background for computer algebra. Examples of articles that have been subject of major editing: "System of polynomial equations" (created), "Computer algebra", "Algebra", "Algebraic geometry", "Polynomial greatest common divisor", "Polynomial factorization", "Finite field", "Hilbert series and Hilbert polynomial",...

For the year 2017, this contribution amounts to about $2,000$ edits on the English Wikipedia.

Mohab Safey El Din was invited by FMJH to present and popularize symbolic and algebraic computation to Master students in Mathematics following the curricula proposed by Univ. Paris-Saclay.

10. Bibliography

Publications of the year

Articles in International Peer-Reviewed Journals

[1] J. BERTHOMIEU, B. BOYER, J.-C. FAUGÈRE. *Linear Algebra for Computing Gröbner Bases of Linear Recursive Multidimensional Sequences*, in "Journal of Symbolic Computation", November 2017, vol. 83, n° Supplement C, pp. 36-67, Special issue on the conference ISSAC 2015: Symbolic computation and computer algebra [*DOI :* 10.1016/J.JSC.2016.11.005], https://hal.inria.fr/hal-01253934

[2] C. E. L. DA SILVA, P. R. DA SILVA, A. JACQUEMARD. *Sliding solutions of second-order differential equations with discontinuous right-hand side*, in "Mathematical Methods in the Applied Sciences", September 2017, vol. 40, n° 14, pp. 5295 - 5306 [*DOI :* 10.1002/MMA.4387], https://hal-univ-bourgogne.archives-ouvertes.fr/hal-01609363

[3] J.-C. FAUGÈRE, C. MOU. *Sparse FGLM algorithms*, in "Journal of Symbolic Computation", May 2017, vol. 80, n° 3, pp. 538 - 569 [*DOI :* 10.1016/J.JSC.2016.07.025], https://hal.inria.fr/hal-00807540

[4] J.-C. FAUGÈRE, A. WALLET. *The Point Decomposition Problem over Hyperelliptic Curves: toward efficient computations of Discrete Logarithms in even characteristic*, in "Designs, Codes and Cryptography", 2017, forthcoming [*DOI :* 10.1007/S10623-017-0449-Y], https://hal.inria.fr/hal-01658573

[5] H. FAWZI, M. SAFEY EL DIN. *A lower bound on the positive semidefinite rank of convex bodies*, in "SIAM Journal on Applied Algebra and Geometry", 2017, pp. 1-14, forthcoming, https://hal.inria.fr/hal-01657849

[6] D. HENRION, S. NALDI, M. SAFEY EL DIN. *SPECTRA -a Maple library for solving linear matrix inequalities in exact arithmetic*, in "Optimization, Methods and Software", 2017, https://arxiv.org/abs/1611.01947 - Significantly extended version, https://hal.laas.fr/hal-01393022

[7] A. HERMAN, H. HONG, E. TSIGARIDAS. *Improving Root Separation Bounds*, in "Journal of Symbolic Computation", 2017, https://hal.inria.fr/hal-01456686

[8] V. Y. PAN, E. TSIGARIDAS. *Accelerated Approximation of the Complex Roots and Factors of a Univariate Polynomial*, in "Theoretical Computer Science", June 2017, To appear, https://hal.inria.fr/hal-01105267

[9] V. Y. PAN, E. TSIGARIDAS. *Nearly optimal computations with structured matrices*, in "Theoretical Computer Science", June 2017, https://hal.inria.fr/hal-01105263

[10] M. SAFEY EL DIN, É. SCHOST. *A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets*, in "Journal of the ACM (JACM)", 2017, vol. 63, n° 6, pp. 48:1–48:37, https://arxiv.org/abs/1307.7836v2 - Major revision, accepted for publication to Journal of the ACM [*DOI :* 10.1145/2996450], https://hal.inria.fr/hal-00849057

[11] M. SAFEY EL DIN, É. SCHOST. *Bit complexity for multi-homogeneous polynomial system solving Application to polynomial minimization*, in "Journal of Symbolic Computation", 2017, pp. 1-32, https://arxiv.org/abs/1605.07433 , forthcoming [*DOI :* 10.1016/J.JSC.2017.08.001], https://hal.inria.fr/hal-01319729

[12] A. STRZEBONSKI, E. TSIGARIDAS. *Univariate real root isolation in an extension field and applications*, in "Journal of Symbolic Computation", 2018, forthcoming, https://hal.inria.fr/hal-01248390

International Conferences with Proceedings

[13] S. BELAID, F. BENHAMOUDA, A. PASSELÈGUE, E. PROUFF, A. THILLARD, D. VERGNAUD. *Private Multiplication over Finite Fields*, in "Advances in Cryptology - CRYPTO 2017", Santa Barbara, United States, J. KATZ, H. SHACHAM (editors), Lecture Notes in Computer Science, Springer, August 2017, vol. 10403, pp. 397-426 [*DOI :* 10.1007/978-3-319-63697-9_14], https://hal.inria.fr/hal-01613773

[14] M. BURR, S. GAO, E. TSIGARIDAS. *The Complexity of an Adaptive Subdivision Method for Approximating Real Curves*, in "ISSAC 2017 - International Symposium on Symbolic and Algebraic Computation", Kaiserslautern, Germany, July 2017, 8 p. [*DOI :* 10.1145/3087604.3087654], https://hal.inria.fr/hal-01528392

[15] A. MANTZAFLARIS, É. SCHOST, E. TSIGARIDAS. *Sparse Rational Univariate Representation*, in "ISSAC 2017 - International Symposium on Symbolic and Algebraic Computation", Kaiserslautern, Germany, July 2017, 8 p. [*DOI :* 10.1145/3087604.3087653], https://hal.inria.fr/hal-01528377

[16] A. MANTZAFLARIS, E. TSIGARIDAS. *Resultants and Discriminants for Bivariate Tensor-product Polynomials*, in "ISSAC 2017 - International Symposium on Symbolic and Algebraic Computation", Kaiserslautern, Germany, Mohab Safey El Din, July 2017, 8 p. [*DOI :* 10.1145/3087604.3087646], https://hal.inria.fr/hal-01525560

Conferences without Proceedings

[17] E. CAGLI, C. DUMAS, E. PROUFF. *Convolutional Neural Networks with Data Augmentation against Jitter-Based Countermeasures*, in "Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference", Taipei, Taiwan, September 2017, https://hal.archives-ouvertes.fr/hal-01661212

Research Reports

[18] A. CASANOVA, J.-C. FAUGÈRE, G. MACARIO-RAT, J. PATARIN, L. PERRET, J. RYCKEGHEM. *GeMSS: A Great Multivariate Short Signature*, UPMC - Paris 6 Sorbonne Universités ; Inria Paris Research Centre, MAMBA Team, F-75012, Paris, France ; LIP6 - Laboratoire d'Informatique de Paris 6, December 2017, pp. 1-4, https://hal.inria.fr/hal-01662158

[19] O. CHAKRABORTY, J.-C. FAUGÈRE, L. PERRET. *CFPKM : A Key Encapsulation Mechanism based on Solving System of non-linear multivariate Polynomials 20171129*, UPMC - Paris 6 Sorbonne Universités ; Inria Paris ; CNRS, December 2017, https://hal.inria.fr/hal-01662175

[20] J.-C. FAUGÈRE, L. PERRET, J. RYCKEGHEM. *DualModeMS: A Dual Mode for Multivariate-based Signature 20170918 draft*, UPMC - Paris 6 Sorbonne Universités ; Inria Paris ; CNRS, December 2017, https://hal.inria.fr/hal-01662165

Patents and standards

[21] L. PERRET, J.-C. FAUGÈRE. *Mise en Oeuvre Optimisée du HFE*, January 2017, n^{o} WO 2017001809 A1, https://hal.inria.fr/hal-01668254

Other Publications

[22] J. BERTHOMIEU, J.-C. FAUGÈRE. *In-depth comparison of the Berlekamp – Massey – Sakata and the Scalar-FGLM algorithms: the non adaptive variants*, May 2017, working paper or preprint, https://hal.inria.fr/hal-01516708

[23] B. BONNARD, O. COTS, J.-C. FAUGÈRE, A. JACQUEMARD, J. ROUOT, M. SAFEY EL DIN, T. VERRON. *Algebraic-geometric techniques for the feedback classification and robustness of the optimal control of a pair of Bloch equations with application to Magnetic Resonance Imaging*, 2017, submitted, https://hal.inria.fr/hal-01556806

[24] L. BUSÉ, A. MANTZAFLARIS, E. TSIGARIDAS. *Matrix formulae for Resultants and Discriminants of Bivariate Tensor-product Polynomials*, December 2017, working paper or preprint, https://hal.inria.fr/hal-01654263

[25] I. Z. EMIRIS, B. MOURRAIN, E. TSIGARIDAS. *Separation bounds for polynomial systems*, February 2017, working paper or preprint, https://hal.inria.fr/hal-01105276

[26] D. HENRION, S. NALDI, M. SAFEY EL DIN. *Real root finding for low rank linear matrices*, October 2017, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01159210

[27] V. MAGRON, M. SAFEY EL DIN, M. SCHWEIGHOFER. *Algorithms for Weighted Sums of Squares Decomposition of Non-negative Univariate Polynomials*, June 2017, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01538729