IN PARTNERSHIP WITH:
CNRS

Sorbonne Université (UPMC)

Activity Report 2018

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. - Formal method for verification, reliability, certification
A4.3. - Cryptography
A4.3.1. - Public key cryptography
A4.3.4. - Quantum Cryptography
A5.10.1. - Design
A6.1. - Methods in 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
B9.5.1. - Computer science
B9.5.2. - Mathematics
B9.10. - Privacy

1. Team, Visitors, External Collaborators

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

Post-Doctoral Fellows

Rachel Player [Sorbonne Université, Post-Doctoral fellow, until Dec. 2018]
Kaie Kubjas [Sorbonne Université, Post-Doctoral fellow]
Amine Mrabet [Sorbonne Université, ATER, until Aug. 2018]

PhD Students

Matías Bender [Inria, until Jun. 2019]
Olive Chakraborty [Sorbonne Université]
Nagardjun Chinthamani Dwarakanath [Sorbonne Université]
Solane El Hirch [Sorbonne Université]
Phuoc Le [Sorbonne Université]
Jocelyn Ryckeghem [Sorbonne Université]
Thi Xuan Vu [Sorbonne Université]

Interns

Reine Abi Rached [Sorbonne Université, Internship, from Apr. 2018 until Aug. 2018]
Phuoc Le [Sorbonne Université, Internship, from Apr. 2018 until Aug. 2018]

Administrative Assistants

Christelle Guiziou [Inria, from Nov. 2018]
Irphane Khan [Sorbonne Université, Assistant]

External Collaborators

Emmanuel Prouff [ANSSI, Associate Member, HDR]
Victor Magron [CNRS, Researcher, until Aug. 2018]

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 that 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 FGB library 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 [2] 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.

[2] http://www.linalg.org/

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 [3]. 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 [4] 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*.

[3] 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

[4] 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

Jean-Charles Faugère and Ludovic Perret received the Atos-Joseph Fourier 2018 prize [5] for their project on Quantum Safe Security.

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

[5] https://atos.net/fr/2018/communiques-de-presse_2018_07_06/atos-et-genci-annoncent-les-laureats-du-prix-atos-joseph-fourier-2018

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. RealCertify

KEYWORDS: Polynomial or analytical systems - Univariate polynomial - Real solving

FUNCTIONAL DESCRIPTION: The package RealCertify aims at providing a full suite of hybrid algorithms for computing certificates of non-negativity based on numerical software for solving linear matrix inequalities. The module univsos handles the univariate case and the module multivsos is designed for the multivariate case.

- Contact: Mohab Safey El Din
- URL: https://gricad-gitlab.univ-grenoble-alpes.fr/magronv/RealCertify

5.8. 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

5.9. 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. Towards Mixed Gröbner Basis Algorithms: the Multihomogeneous and Sparse Case

One of the biggest open problems in computational algebra is the design of efficient algorithms for Gröbner basis computations that take into account the sparsity of the input polynomials. We can perform such computations in the case of unmixed polynomial systems, that is systems with polynomials having the same support, using the approach of Faugère, Spaenlehauer, and Svartz [ISSAC'14]. In [15] we present two algorithms for sparse Gröbner bases computations for mixed systems. The first one computes with mixed sparse systems and exploits the supports of the polynomials. Under regularity assumptions, it performs no reductions to zero. For mixed, square, and 0-dimensional multihomogeneous polynomial systems, we present a dedicated, and potentially more efficient, algorithm that exploits different algebraic properties that performs no reduction to zero. We give an explicit bound for the maximal degree appearing in the computations.

6.1.2. Bilinear Systems with Two Supports: Koszul Resultant Matrices, Eigenvalues, and Eigenvectors

A fundamental problem in computational algebraic geometry is the computation of the resultant. A central question is when and how to compute it as the determinant of a matrix whose elements are the coefficients of the input polynomials up-to sign. This problem is well understood for unmixed multihomogeneous systems, that is for systems consisting of multihomogeneous polynomials with the same support. However, little is known for mixed systems, that is for systems consisting of polynomials with different supports. In [14] we consider the computation of the multihomogeneous resultant of bilinear systems involving two different supports. We present a constructive approach that expresses the resultant as the exact determinant of a *Koszul resultant matrix*, that is a matrix constructed from maps in the Koszul complex. We exploit the resultant matrix to propose an algorithm to solve such systems. In the process we extend the classical eigenvalues and eigenvectors criterion to a more general setting. Our extension of the eigenvalues criterion applies to a general class of matrices, including the Sylvester-type and the Koszul-type ones.

6.1.3. A Polynomial-Division-Based Algorithm for Computing Linear Recurrence Relations

Sparse polynomial interpolation, sparse linear system solving or modular rational reconstruction are fundamental problems in Computer Algebra. They come down to computing linear recurrence relations of a sequence with the Berlekamp–Massey algorithm. Likewise, sparse multivariate polynomial interpolation and multidimensional cyclic code decoding require guessing linear recurrence relations of a multivariate sequence.

Several algorithms solve this problem. The so-called Berlekamp–Massey–Sakata algorithm (1988) uses polynomial additions and shifts by a monomial. The SCALAR-FGLM algorithm (2015) relies on linear algebra operations on a multi-Hankel matrix, a multivariate generalization of a Hankel matrix. The Artinian Gorenstein border basis algorithm (2017) uses a Gram-Schmidt process.

In [16], we propose a new algorithm for computing the Gröbner basis of the ideal of relations of a sequence based solely on multivariate polynomial arithmetic. This algorithm allows us to both revisit the Berlekamp–Massey–Sakata algorithm through the use of polynomial divisions and to completely revise the SCALAR-FGLM algorithm without linear algebra operations.

A key observation in the design of this algorithm is to work on the mirror of the truncated generating series allowing us to use polynomial arithmetic modulo a monomial ideal. It appears to have some similarities with Padé approximants of this mirror polynomial.

Finally, we give a partial solution to the transformation of this algorithm into an adaptive one.

As an addition from the paper published at the ISSAC conferance, in [24], we give an adaptive variant of this algorithm taking into account the shape of the final Gröbner basis gradually as it is discovered. The main advantage of this algorithm is that its complexity in terms of operations and sequence queries only depends on the output Gröbner basis.

All these algorithms have been implemented in MAPLE and we report on our comparisons.

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

The BERLEKAMP–MASSEY–SAKATA algorithm and the SCALAR-FGLM algorithm both compute the ideal of relations of a multidimensional linear recurrent sequence.

Whenever quering a single sequence element is prohibitive, the bottleneck of these algorithms becomes the computation of all the needed sequence terms. As such, having adaptive variants of these algorithms, reducing the number of sequence queries, becomes mandatory.

A native adaptive variant of the SCALAR-FGLM algorithm was presented by its authors, the so-called ADAPTIVE SCALAR-FGLM algorithm.

In [25], our first contribution is to make the BERLEKAMP–MASSEY–SAKATA algorithm more efficient by making it adaptive to avoid some useless relation testings. This variant allows us to divide by four in dimension 2 and by seven in dimension 3 the number of basic operations performed on some sequence family.

Then, we compare the two adaptive algorithms. We show that their behaviors differ in a way that it is not possible to tweak one of the algorithms in order to mimic exactly the behavior of the other. We detail precisely the differences and the similarities of both algorithms and conclude that in general the ADAPTIVE SCALAR-FGLM algorithm needs fewer queries and performs fewer basic operations than the ADAPTIVE BERLEKAMP–MASSEY–SAKATA algorithm.

We also show that these variants are always more efficient than the original algorithms.

6.1.5. Bit complexity for multi-homogeneous polynomial system solving Application to polynomial minimization

Multi-homogeneous polynomial systems arise in many applications. In [10] we provide bit complexity estimates for solving them 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 assumptions essentially imply that the Jacobian matrix of the system under study has maximal rank at the solution set and that this solution set if finite. 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.

6.2. Solving Systems over the Reals and Applications

6.2.1. Univariate real root isolation in an extension field and applications

In [11] we present algorithmic, complexity and implementation results for the problem of isolating the real roots of a univariate polynomial in $B_\alpha \in L[y]$, where $L = \mathbb{Q}(\alpha)$ is a simple algebraic extension of the rational numbers. We revisit two approaches for the problem. In the first approach, using resultant computations, we perform a reduction to a polynomial with integer coefficients and we deduce a bound of $\widetilde{\mathcal{O}}_B(N^8)$ for isolating the real roots of B_α, where N is an upper bound on all the quantities (degree and bitsize) of the input polynomials. The bound becomes $\widetilde{\mathcal{O}}_B(N^7)$ if we use Pan's algorithm for isolating the real roots. In the second approach we isolate the real roots working directly on the polynomial of the input. We compute improved separation bounds for the roots and we prove that they are optimal, under mild assumptions. For isolating the real roots we consider a modified Sturm algorithm, and a modified version of `descartes`' algorithm. For the former we prove a Boolean complexity bound of $\widetilde{\mathcal{O}}_B(N^{12})$ and for the latter a bound of $\widetilde{\mathcal{O}}_B(N^5)$. We present aggregate separation bounds and complexity results for isolating the real roots of all polynomials B_{α_k}, when α_k runs over all the real conjugates of α. We show that we can isolate the real roots of all polynomials in $\widetilde{\mathcal{O}}_B(N^5)$. Finally, we implemented the algorithms in `C` as part of the core library of `MATHEMATICA` and we illustrate their efficiency over various data sets.

6.2.2. On the Maximal Number of Real Embeddings of Spatial Minimally Rigid Graphs

The number of embeddings of minimally rigid graphs in $\mathbb{R}^D$ is (by definition) finite, modulo rigid transformations, for every generic choice of edge lengths. Even though various approaches have been proposed to compute it, the gap between upper and lower bounds is still enormous. Specific values and its asymptotic behavior are major and fascinating open problems in rigidity theory. Our work in [13] considers the maximal number of real embeddings of minimally rigid graphs in $\mathbb{R}^3$. We modify a commonly used parametric semi-algebraic formulation that exploits the Cayley-Menger determinant to minimize the *a priori* number of complex embeddings, where the parameters correspond to edge lengths. To cope with the huge dimension of the parameter space and find specializations of the parameters that maximize the number of real embeddings, we introduce a method based on coupler curves that makes the sampling feasible for spatial minimally rigid graphs. Our methodology results in the first full classification of the number of real embeddings of graphs with 7 vertices in $\mathbb{R}^3$, which was the smallest open case. Building on this and certain 8-vertex graphs, we improve the previously known general lower bound on the maximum number of real embeddings in $\mathbb{R}^3$.

6.2.3. Lower bounds on the number of realizations of rigid graphs

Computing the number of realizations of a minimally rigid graph is a notoriously difficult problem. Towards this goal, for graphs that are minimally rigid in the plane, we take advantage of a recently published algorithm, which is the fastest available method, although its complexity is still exponential. Combining computational results with the theory of constructing new rigid graphs by gluing, in [4] we give a new lower bound on the maximal possible number of (complex) realizations for graphs with a given number of vertices. We extend these ideas to rigid graphs in three dimensions and we derive similar lower bounds, by exploiting data from extensive Gröbner basis computations.

6.2.4. The Complexity of Subdivision for Diameter-Distance Tests

In [1] we present a general framework for analyzing the complexity of subdivision-based algorithms whose tests are based on the sizes of regions and their distance to certain sets (often varieties) intrinsic to the problem under study. We call such tests diameter-distance tests. We illustrate that diameter-distance tests are common in the literature by proving that many interval arithmetic-based tests are, in fact, diameter-distance tests. For this class of algorithms, we provide both non-adaptive bounds for the complexity, based on separation bounds, as well as adaptive bounds, by applying the framework of continuous amortization. Using this structure, we provide the first complexity analysis for the algorithm by Plantinga and Vegeter for approximating real implicit curves and surfaces. We present both adaptive and non-adaptive a priori worst-case bounds on the complexity of this algorithm both in terms of the number of subregions constructed and in terms of the bit complexity for the construction. Finally, we construct families of hypersurfaces to prove that our bounds are tight.

6.2.5. Real root finding for equivariant semi-algebraic systems

Let R be a real closed field. In [19] we consider basic semi-algebraic sets defined by n-variate equations/inequalities of s symmetric polynomials and an equivariant family of polynomials, all of them of degree bounded by $2d < n$. Such a semi-algebraic set is invariant by the action of the symmetric group. We show that such a set is either empty or it contains a point with at most $2d-1$ distinct coordinates. Combining this geometric result with efficient algorithms for real root finding (based on the critical point method), one can decide the emptiness of basic semi-algebraic sets defined by s polynomials of degree d in time $(sn)^{O(d)}$. This improves the state-of-the-art which is exponential in n. When the variables $x_1, ..., x_n$ are quantified and the coefficients of the input system depend on parameters $y_1, ..., y_t$, one also demonstrates that the corresponding one-block quantifier elimination problem can be solved in time $(sn)^{O(dt)}$.

6.2.6. Exact algorithms for semidefinite programs with degenerate feasible set

Let $A_0, ..., A_nn$ be $m \times m$ symmetric matrices with entries in Q, and let $A(x)$ be the linear pencil $A_0 + x_1 A_1 + \cdots + x_n A_n$, where $x = (x1, ..., xn)$ are unknowns. The linear matrix inequality (LMI) $A(x) \succeq 0$ defines the subset of R^n, called spectrahedron, containing all points x such that $A(x)$ has nonnegative eigenvalues. The minimization of linear functions over spectrahedra is called semidefinite programming (SDP). Such problems appear frequently in control theory and real algebra, especially in the context of nonnegativity certificates for multivariate polynomials based on sums of squares. Numerical software for solving SDP are mostly based on the interior point method, assuming some non-degeneracy properties such as the existence of interior points in the admissible set. In [21], we design an exact algorithm based on symbolic homotopy for solving semidefinite programs without assumptions on the feasible set, and we analyze its complexity. Because of the exactness of the output, it cannot compete with numerical routines in practice but we prove that solving such problems can be done in polynomial time if either n or m is fixed.

6.2.7. A lower bound on the positive semidefinite rank of convex bodies

The positive semidefinite rank of a convex body C is the size of its smallest positive semidef-inite formulation. In [3] 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.

6.2.8. On the complexity of computing real radicals of polynomial systems

Let $f = (f_1, ..., f_s)$ be a sequence of polynomials in $Q[X_1, ..., X_n]$ of maximal degree D and $V \subset C^n$ be the algebraic set defined by f and r be its dimension. The real radical $\sqrt[re]{\langle f \rangle}$ associated to f is the largest ideal which defines the real trace of V. In [20] when V is smooth, we show that $\sqrt[re]{\langle f \rangle}$ has a finite set of generators with degrees bounded by V. Moreover, we present a probabilistic algorithm of complexity $(snDn)^{O(1)}$ to compute the minimal primes of $\sqrt[re]{\langle f \rangle}$. When V is not smooth, we give a probabilistic algorithm of complexity $s^{O(1)}(nD)^{O(nr2^r)}$ to compute rational parametrizations for all irreducible components of the real algebraic set $V \cap R^n$. Experiments are given to show the efficiency of our approaches.

6.2.9. Algorithms for Weighted Sums of Squares Decomposition of Non-negative Univariate Polynomials

It is well-known that every non-negative univariate real polynomial can be written as the sum of two polynomial squares with real coefficients. When one allows a weighted sum of finitely many squares instead of a sum of two squares, then one can choose all coefficients in the representation to lie in the field generated by the coefficients of the polynomial. In particular, this allows an effective treatment of polynomials with rational coefficients. In [9], we describe, analyze and compare both from the theoretical and practical points of view, two algorithms computing such a weighted sums of squares decomposition for univariate polynomials with rational coefficients. The first algorithm, due to the third author relies on real root isolation, quadratic approximations of positive polynomials and square-free decomposition but its complexity was not analyzed. We provide bit complexity estimates, both on the runtime and the output size of this algorithm. They are exponential in the degree of the input univariate polynomial and linear in the maximum bitsize of its complexity. This analysis is obtained using quantifier elimination and root isolation bounds. The second algorithm, due to Chevillard, Harrison, Joldes and Lauter, relies on complex root isolation and square-free decomposition and has been introduced for certifying positiveness of poly-nomials in the context of computer arithmetics. Again, its complexity was not analyzed. We provide bit complexity estimates, both on the runtime and the output size of this algorithm, which are polynomial in the degree of the input polynomial and linear in the maximum bitsize of its complexity. This analysis is obtained using Vieta's formula and root isolation bounds. Finally, we report on our implementations of both algorithms and compare them in practice on several application benchmarks. While the second algorithm is, as expected from the complexity result, more efficient on most of examples, we exhibit families of non-negative polynomials for which the first algorithm is better.

6.2.10. On Exact Polya and Putinar's Representations

We consider the problem of finding exact sums of squares (SOS) decompositions for certain classes of non-negative multivariate polynomials, relying on semidefinite programming (SDP) solvers. In [18] we start by providing a hybrid numeric-symbolic algorithm computing exact rational SOS decompositions for polynomials lying in the interior of the SOS cone. It computes an approximate SOS decomposition for a perturbation of the input polynomial with an arbitrary-precision SDP solver. An exact SOS decomposition is obtained thanks to the perturbation terms. We prove that bit complexity estimates on output size and runtime are both polynomial in the degree of the input polynomial and simply exponential in the number of variables. Next, we apply this algorithm to compute exact Polya and Putinar's representations respectively for positive definite forms and positive polynomials over basic compact semi-algebraic sets. We also compare the implementation of our algorithms with existing methods in computer algebra including cylindrical algebraic decomposition and critical point method.

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

6.3.1. Linear Repairing Codes and Side-Channel Attacks

To strengthen the resistance of countermeasures based on secret sharing, several works have suggested to use the scheme introduced by Shamir in 1978, which proposes to use the evaluation of a random d-degree polynomial into n $d+1$ public points to share the sensitive data. Applying the same principles used against the classical Boolean sharing, all these works have assumed that the most efficient attack strategy was to exploit the minimum number of shares required to rebuild the sensitive value; which is $d+1$ if the reconstruction is made with Lagrange's interpolation. In [2], we highlight first an important difference between Boolean and Shamir's sharings which implies that, for some signal-to-noise ratio, it is more advantageous for the adversary to observe strictly more than d + 1 shares. We argue that this difference is related to the existence of so-called exact linear repairing codes, which themselves come with reconstruction formulae that need (much) less information (counted in bits) than Lagrange's interpolation. In particular, this result implies that, contrary to what was believed, the choice of the public points in Shamir's sharing has an impact on the countermeasure strength. As another contribution, we exhibit a positive impact of the existence of linear exact repairing schemes; we indeed propose to use them to improve the state-of-the-art multiplication algorithms dedicated to Shamir's sharing. We argue that the improvement can be effective when the multiplication operation in the base field is at least two times smaller than in its sub-fields.

6.3.2. On the Use of Independent Component Analysis to Denoise Side-Channel Measurements

Independent Component Analysis (ICA) is a powerful technique for blind source separation. It has been successfully applied to signal processing problems, such as feature extraction and noise reduction , in many different areas including medical signal processing and telecommunication. In [17], we propose a framework to apply ICA to denoise side-channel measurements and hence to reduce the complexity of key recovery attacks. Based on several case studies, we afterwards demonstrate the overwhelming advantages of ICA with respect to the commonly used preprocessing techniques such as the singular spectrum analysis. Mainly, we target a software masked implementation of an AES and a hardware unprotected one. Our results show a significant Signal-to-Noise Ratio (SNR) gain which translates into a gain in the number of traces needed for a successful side-channel attack. This states the ICA as an important new tool for the security assessment of cryptographic implementations.

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.

- CIFRE Contract with ST Micro electronics that funds the PhD thesis of Simon Landry on "Threshold Implementations Against Side Channel Analysis". Supervisor Emmanuel Prouff.

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 [6] 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.

[6] https://project.inria.fr/galop/

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 [7] project is certainly the biggest industrial project ever organized in quantum-safe cryptography. RISQ is one of few projects accepted in the call Grands DГ©fis du NumГ©rique 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.

- **ANR SESAME (Singularités Et Stabilité des AsservisseMEnts référencés capteurs)**

  Duration: 2018–2022

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

8.3. European Initiatives

8.3.1. FP7 & H2020 Projects

- **Innovative Training Network POEMA (Polynomial Optimization, Efficiency through Moments and Algebra)**

  Duration: 2019-2022.

  POEMA is a Marie Skłodowska-Curie Innovative Training Network (2019-2022).

  Its goal is to train scientists at the interplay of algebra, geometry and computer science for polynomial optimization problems and to foster scientific and technological advances, stimulating interdisciplinary and intersectoriality knowledge exchange between algebraists, geometers, computer scientists and industrial actors facing real-life optimization problems.

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

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,

[7] http://risq.fr/

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 Research Visitors

8.4.1. Visits of International Scientists

8.4.1.1. Internships

Reine Abi Rached

Date: Apr. 2018 - Aug. 2018

Institution: Université de Versailles –St-Quentin-en-Yvelines

Supervisor: Jean-Charles Faugère, Jérémy Berthomieu

Hadrien Brochet

Date: Jun. 2018 - Aug. 2018

Institution: ENS Lyon

Supervisor: Elias Tsigaridas

Phuoc Le

Date: Apr. 2018 - Aug. 2018

Institution: Université de Versailles –St-Quentin-en-Yvelines

Supervisor: Jean-Charles Faugère, Mohab Safey El Din

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

Elias Tsigaridas was a visiting research scientist at the ICERM institute (Brown University) during the special semester on "Nonlinear Algebra" (Sep – Nov 2018).

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

Dongming Wang was the General Chair of International Conference on Automated Deduction in Geometry (ADG 2018) (Nanning, China, September 11-14, 2018).

Dongming Wang was the General co-Chair of the 44th International Symposium on Symbolic and Algebraic Computation (ISSAC 2019) , Beijing, China, July 15-18, 2019), and the 13th International Conference on Artificial Intelligence and Symbolic Computation (AISC 2018) (Suzhou, China, September 16-19, 2018).

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

Elias Tsigaridas was a member of the program committees of the 20th International Workshop on Computer Algebra in Scientific Computing (CASC) 2018.

Mohab Safey El Din was member of the program committee of the 43rd International Symposium on Symbolic and Algebraic Computation (ISSAC) 2018.

Emmanuel Prouff was a member of the programm committee of the Conference on Cryptographic Hardware and Embedded Systems 2018 (CHES), Smart Card Research and Advanced Application Conference (CARDIS) 2018, and Constructive Side-Channel Analysis and Secure Design (COSADE) 2018.

Dongming Wang was a member of the program committee of 13th International Conference on Artificial Intelligence and Symbolic Computation (AISC 2018) (Suzhou, China, September 16-19, 2018) and the 4th International Conference on Numerical and Symbolic Computation (SYMCOMP 2019) (Porto, Portugal, April 11-12, 2019).

9.1.2.2. Reviewer

Mohab Safey El Din was reviewer of the M. Skomra's Phd (CMAP, École polytechnique).

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

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

Mohab Safey El Din (with Chee Yap, Courant Inst. NYU) is guest editor of the Journal of Symbolic Computation Special Issue on the 2017 International Symposium on Symbolic and Algebraic Computation.

Dongming Wang is a member of the editorial board of

- 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).

Dongming Wang is a member of the Advisory Board for the journal SCIENCE CHINA Information Sciences (published by Science China Press, Beijing and Springer, Berlin).

Dongming Wang is the Editor-in-Chief for the journal Mathematics in Computer Science (published by Birkhäuser/Springer, Basel).

9.1.4. Invited Talks

Elias Tsigaridas was invited speaker at

- IBM T.J. Watson Research Center, (*Invited talk*) 28 Nov 2018.
- *Applied Algebra Day*. MIT, 17 Nov 2018.
- ICERM, University of Brown, *Main seminar*, Nov, 2018.

Mohab Safey El Din was invited speaker at

- Key Lab on Math. Mechanization, Chinese Academy of Sciences, *Invited talk*.
- Dep. of Math. of Univ. of Tromso, *Invited talk*.
- ICERM, Semester Prog. on Non-linear Algebra, Workshop on Real algebraic geometry and optimization, *Plenary talk*.

Emmanuel Prouff was an invited speaker at

- PANDA 2018 Conference (China) and talked on "Deep Learning for Embedded Security Evaluation".
- COSADE 2018 Conference (Singapur) and talked on "Deep Learning for Embedded Security Evaluation".

9.1.5. Scientific Expertise

Mohab Safey El Din is Chargé de Mission for Computer Science at Sorbonne Univ. (Faculté des Sciences et Ingéniérie).

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Jérémy Berthomieu had the following teaching activities:

Master : Computation Modeling, 38 hours, M1, Sorbonne Université, France.

Master : In charge of Basics of Algebraic Algorithms, 74 hours, M1, Sorbonne Université & Polytech' UPMC, France.

Master : Projects supervision, 6 hours, M1, Sorbonne Université, France.

Licence : Introduction to Algorithmics, 33 hours, L2, Sorbonne Université , France.

Licence : Projects supervision, 10 hours, L2, Sorbonne Université, France.

Licence : In charge of Basics of Programmation 2, 50 hours, L1, Sorbonne Université, France.

Mohab Safey El Din has the following teaching activities:

Master : Computation Modeling, 33 hours, M1, Sorbonne Université, France.

Master : Polynomial System Solving, 40 hours, M1, Sorbonne Université, France.

Master : In charge of the curriculum on Security, Reliability of Performance in Computing, 30 hours, M1, Sorbonne Université , France.

Master : Projects management, 20 hours, M1, Sorbonne Université, France.

Licence : Projects supervision, 10 hours, L2, Sorbonne Université, France.

9.2.2. Supervision

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 : Thi Xuan Vu, Faster algorithms for structured polynomial systems, started in Oct. 2017, Jean-Charles Faugère and Mohab Safey El Din.

PhD in progress : Phuoc Le, Real root classification and polar varieties, started in Oct. 2018, Jean-Charles Faugère and Mohab Safey El Din.

PhD in progress : Simon Landry, Threshold Implementations Against Side Channel Analysis, Emmanuel Prouff.
CIFRE/Contract with ST Micro electronics.

9.2.3. Juries

Mohab Safey El Din was member of the PhD committees of M. Skomra (CMAP, École polytechnique) and T. Weisser (LAAS, CNRS).

10. Bibliography

Publications of the year

Articles in International Peer-Reviewed Journals

[1] M. Burr, S. Gao, E. Tsigaridas. *The Complexity of Subdivision for Diameter-Distance Tests*, in "Journal of Symbolic Computation", 2018, https://hal.inria.fr/hal-01953446

[2] H. Chabanne, H. Maghrebi, E. Prouff. *Linear Repairing Codes and Side-Channel Attacks*, in "IACR Transactions on Cryptographic Hardware and Embedded Systems", February 2018, vol. 2018, n^{o} 1, pp. 118-141 [*DOI :* 10.13154/TCHES.V2018.I1.118-141], https://hal.archives-ouvertes.fr/hal-01973360

[3] 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", 2018, vol. 2, n^{o} 1, pp. 126-139 [*DOI :* 10.1137/17M1142570], https://hal.inria.fr/hal-01657849

[4] G. Grasegger, C. Koutschan, E. Tsigaridas. *Lower bounds on the number of realizations of rigid graphs*, in "Experimental Mathematics", 2018, pp. 1-22, https://hal.inria.fr/hal-01711441

[5] J.-B. B. Lasserre, V. Magron. *Optimal data fitting: a moment approach*, in "SIAM Journal on Optimization", November 2018, vol. 28, n^{o} 4, pp. 3127-3144, https://arxiv.org/abs/1802.03259 - 21 pages, 5 figures [*DOI :* 10.1137/18M1170108], https://hal.archives-ouvertes.fr/hal-01706850

[6] V. Magron. *Interval Enclosures of Upper Bounds of Roundoff Errors using Semidefinite Programming*, in "ACM Transactions on Mathematical Software", August 2018, vol. 44, n^{o} 4, pp. 41:1–41:18, https://arxiv.org/abs/1611.01318 - 18 pages, 2 tables, 1 figure [*DOI :* 10.1145/3206430], https://hal.archives-ouvertes.fr/hal-01956815

[7] V. Magron, A. Rocca, T. Dang. *Certified Roundoff Error Bounds using Bernstein Expansions and Sparse Krivine-Stengle Representations*, in "IEEE Transactions on Computers", 2018, https://arxiv.org/abs/1802.04385 - 14 pages, 2 figures, 2 tables. Extension of the work in arXiv:1610.07038 [*DOI :* 10.1109/TC.2018.2851235], https://hal.archives-ouvertes.fr/hal-01956817

[8] V. Magron, M. Safey El Din. *RealCertify: a Maple package for certifying non-negativity*, in "ACM Communications in Computer Algebra", June 2018, vol. 52, n^{o} 2, pp. 34-37, https://arxiv.org/abs/1805.02201 - 4 pages, 2 tables [*DOI :* 10.1145/3282678.3282681], https://hal.archives-ouvertes.fr/hal-01956812

[9] V. Magron, M. Safey El Din, M. Schweighofer. *Algorithms for Weighted Sums of Squares Decomposition of Non-negative Univariate Polynomials*, in "Journal of Symbolic Computation", 2018, https://hal.archives-ouvertes.fr/hal-01538729

[10] M. Safey El Din, É. Schost. *Bit complexity for multi-homogeneous polynomial system solving Application to polynomial minimization*, in "Journal of Symbolic Computation", 2018, vol. 87, pp. 176-206, https://arxiv.org/abs/1605.07433 [*DOI :* 10.1016/J.JSC.2017.08.001], https://hal.inria.fr/hal-01319729

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

International Conferences with Proceedings

[12] L. BARTHELEMY, D. KAHROBAEI, G. RENAULT, Z. ŠUNIĆ. *Quadratic time algorithm for inversion of binary permutation polynomials*, in "ICMS 2018 - International Congress on Mathematical Software", South Bend, IN, United States, J. H. DAVENPO, M. KAUERS, G. LABAH, J. URBA (editors), Lecture Notes in Computer Science, Springer, July 2018, vol. 10931, pp. 19-27 [*DOI :* 10.1007/978-3-319-96418-8_3], https://hal.archives-ouvertes.fr/hal-01981320

[13] E. BARTZOS, I. EMIRIS, J. LEGERSKÝ, E. TSIGARIDAS. *On the maximal number of real embeddings of spatial minimally rigid graphs*, in "ISSAC '18 International Symposium on Symbolic and Algebraic Computation", New York, United States, C. ARRECHE (editor), ACM, July 2018, pp. 55-62 [*DOI :* 10.1145/3208976.3208994], https://hal.archives-ouvertes.fr/hal-01710518

[14] M. R. BENDER, J.-C. FAUGÈRE, A. MANTZAFLARIS, E. TSIGARIDAS. *Bilinear systems with two supports: Koszul resultant matrices, eigenvalues, and eigenvectors*, in "ISSAC 2018 - 43rd International Symposium on Symbolic and Algebraic Computation", New York, United States, July 2018, https://arxiv.org/abs/1805.05060 [*DOI :* 10.1145/3208976.3209011], https://hal.inria.fr/hal-01787549

[15] M. R. BENDER, J.-C. FAUGÈRE, E. TSIGARIDAS. *Towards Mixed Gröbner Basis Algorithms: the Multihomogeneous and Sparse Case*, in "ISSAC 2018 - 43rd International Symposium on Symbolic and Algebraic Computation", New York, United States, July 2018, https://arxiv.org/abs/1805.03577 [*DOI :* 10.1145/3208976.3209018], https://hal.inria.fr/hal-01787423

[16] J. BERTHOMIEU, J.-C. FAUGÈRE. *A Polynomial-Division-Based Algorithm for Computing Linear Recurrence Relations*, in "ISSAC 2018 - 43rd International Symposium on Symbolic and Algebraic Computation", New York, United States, July 2018 [*DOI :* 10.1145/3208976.3209017], https://hal.inria.fr/hal-01784369

[17] H. MAGHREBI, E. PROUFF. *On the Use of Independent Component Analysis to Denoise Side-Channel Measurements*, in "COSADE 2018 - 9th International Workshop on Constructive Side-Channel Analysis and Secure Design", Singapore, Singapore, Lecture Notes in Computer Science, Springer, April 2018, vol. 10815, pp. 61-81 [*DOI :* 10.1007/978-3-319-89641-0_4], https://hal.archives-ouvertes.fr/hal-01973322

[18] V. MAGRON, M. SAFEY EL DIN. *On Exact Polya and Putinar's Representations*, in "ISSAC '18 International Symposium on Symbolic and Algebraic Computation", New-York, United States, ACM, July 2018, pp. 279-286, https://arxiv.org/abs/1802.10339 - 19 pages, 4 algorithms, 3 tables [*DOI :* 10.1145/3208976.3208986], https://hal.archives-ouvertes.fr/hal-01720612

[19] C. RIENER, M. SAFEY EL DIN. *Real root finding for equivariant semi-algebraic systems*, in "ISSAC 20018 - 43rd International Symposium on Symbolic and Algebraic Computation", New-York, United States, July 2018, https://arxiv.org/abs/1806.08121 , https://hal.inria.fr/hal-01819106

[20] M. SAFEY EL DIN, Z.-H. YANG, L. ZHI. *On the complexity of computing real radicals of polynomial systems*, in "ISSAC '18 - The 2018 ACM on International Symposium on Symbolic and Algebraic Computation", New-York, United States, ACM, July 2018, pp. 351-358 [*DOI :* 10.1145/3208976.3209002], https://hal.inria.fr/hal-01956596

Conferences without Proceedings

[21] D. HENRION, S. NALDI, M. SAFEY EL DIN. *Exact algorithms for semidefinite programs with degenerate feasible set*, in "ISSAC 2018 - 43rd International Symposium on Symbolic and Algebraic Computation", New York City, United States, July 2018, 17 p. , https://arxiv.org/abs/1802.02834 , https://hal.archives-ouvertes.fr/hal-01705590

Other Publications

[22] J. G. ALCÁZAR, J. CARAVANTES, G. M. DIAZ-TOCA, E. TSIGARIDAS. *Computing the topology of a planar or space hyperelliptic curve*, January 2019, working paper or preprint, https://hal.inria.fr/hal-01968776

[23] M. R. BENDER, J.-C. FAUGÈRE, L. PERRET, E. TSIGARIDAS. *A nearly optimal algorithm to decompose binary forms*, June 2018, https://arxiv.org/abs/1810.12588 - In submission, https://hal.inria.fr/hal-01907777

[24] J. BERTHOMIEU, J.-C. FAUGÈRE. *A Polynomial-Division-Based Algorithm for Computing Linear Recurrence Relations*, November 2018, working paper or preprint, https://hal.inria.fr/hal-01935229

[25] J. BERTHOMIEU, J.-C. FAUGÈRE. *In-depth comparison of the Berlekamp–Massey–Sakata and the Scalar-FGLM algorithms: the adaptive variants*, June 2018, https://arxiv.org/abs/1806.00978 - working paper or preprint, https://hal.inria.fr/hal-01805478

[26] J. D. HAUENSTEIN, M. SAFEY EL DIN, É. SCHOST, T. X. VU. *Solving determinantal systems using homotopy techniques*, February 2018, https://arxiv.org/abs/1802.10409 - working paper or preprint, https://hal.inria.fr/hal-01719170

[27] V. MAGRON, M. FORETS, D. HENRION. *Semidefinite Approximations of Invariant Measures for Polynomial Systems*, July 2018, https://arxiv.org/abs/1807.00754 - 28 pages, 14 figures, https://hal.archives-ouvertes.fr/hal-01828443

[28] V. MAGRON, M. SAFEY EL DIN. *On Exact Polya, Hilbert-Artin and Putinar's Representations*, November 2018, https://arxiv.org/abs/1811.10062 - 29 pages, 4 tables, extended version of the paper from ISSAC'18 conference (available at arXiv::1802.10339), https://hal.archives-ouvertes.fr/hal-01935727

[29] F. MORAIN, G. RENAULT, B. SMITH. *Deterministic factoring with oracles*, February 2018, https://arxiv.org/abs/1802.08444 - working paper or preprint, https://hal.inria.fr/hal-01715832