IN PARTNERSHIP WITH:
CNRS
Sorbonne Université (UPMC)

Activity Report 2019

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, end of the Project-Team: 2019 December 31

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, until Aug 2019]
Dongming Wang [CNRS, Senior Researcher, HDR]

Faculty Members

Mohab Safey El Din [Team leader, Sorbonne Université, Professor, HDR]
Jérémy Berthomieu [Sorbonne Université, Associate Professor]
Ludovic Perret [Sorbonne Université, Associate Professor, HDR]

PhD Students

Matías Bender [Inria, PhD Student, until May 2019]
Olive Chakraborty [Sorbonne Université, PhD Student]
Solane El Hirch [Sorbonne Université, PhD Student]
Jocelyn Ryckeghem [DGA, PhD Student]
Thi Xuan Vu [Sorbonne Université, PhD Student]

Administrative Assistants

Christelle Guiziou [Inria, Administrative Assistant]
Mathieu Mourey [Inria, Administrative Assistant]

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, 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.

3.3. Solving Systems over the Reals and Applications.

Participants: Mohab Safey El Din, Elias Tsigaridas, Daniel Lazard, 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.

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

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

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

Participants: Jean-Charles Faugère, Mohab Safey El Din, 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.

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.

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

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, 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*.

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.

[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.

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

CryptoNext Security, a spinoff of the PolSys team, was founded in June 2019 and has already been selected in the Future 40 group by STATION F of the most promising young startups.

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. 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

KEYWORDS: Univariate polynomial - Real solving

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: https://who.paris.inria.fr/Elias.Tsigaridas/soft.html

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

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 [3], our first contribution is to make the Berlekamp–Massey–Sakata algorithm more efficient by making it adaptive to avoid some useless relation test-ings. 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.

The problem of finding $m \times s$ matrices (with $m \geq s$) of rank r in a real affine subspace of dimension n has many applications in information and systems theory, where low rank is synonymous of structure and parsimony. In [8], we design computer algebra algorithms to solve this problem efficiently and exactly: the input are the rational coefficients of the matrices spanning the affine subspace as well as the expected maximum rank, and the output is a rational parametrization encoding a finite set of points that intersects each connected component of the low rank real algebraic set. The complexity of our algorithm is studied thoroughly. It is essentially polynomial in $n+m(s-r)$; it improves on the state-of-the-art in the field. Moreover, computer experiments show the practical efficiency of our approach.

Gröbner bases is one the most powerful tools in algorithmic non-linear algebra. Their computation is an intrinsically hard problem with a complexity at least single exponential in the number of variables. However, in most of the cases, the polynomial systems coming from applications have some kind of structure. For example , several problems in computer-aided design, robotics, vision, biology , kinematics, cryptography, and optimization involve sparse systems where the input polynomials have a few non-zero terms. In [16], our approach to exploit sparsity is to embed the systems in a semigroup algebra and to compute Gröbner bases over this algebra. Up to now, the algorithms that follow this approach benefit from the sparsity only in the case where all the polynomials have the same sparsity structure, that is the same Newton polytope. We introduce the first algorithm that overcomes this restriction. Under regularity assumptions, it performs no redundant computations. Further, we extend this algorithm to compute Gröbner basis in the standard algebra and solve sparse polynomials systems over the torus $(\mathbb{C}^{\star})^{n}$. The complexity of the algorithm depends on the Newton polytopes.

In [10], we consider the problem of approximating numerically the moments and the supports of measures which are invariant with respect to the dynamics of continuous- and discrete-time polynomial systems, under semialgebraic set constraints. First, we address the problem of approximating the density and hence the support of an invariant measure which is absolutely continuous with respect to the Lebesgue measure. Then, we focus on the approximation of the support of an invariant measure which is singular with respect to the Lebesgue measure. Each problem is handled through an appropriate reformulation into a linear optimization problem over measures, solved in practice with two hierarchies of finite-dimensional semidefinite moment-sum-of-square relaxations, also called Lasserre hierarchies. Under specific assumptions, the first Lasserre hierarchy allows to approximate the moments of an absolutely continuous invariant measure as close as desired and to extract a sequence of polynomials converging weakly to the density of this measure. The second Lasserre hierarchy allows to approximate as close as desired in the Hausdorff metric the support of a singular invariant measure with the level sets of the Christoffel polynomials associated to the moment matrices of this measure. We also present some application examples together with numerical results for several dynamical systems admitting either absolutely continuous or singular invariant measures.

6.2. Solving systems over the reals and applications

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 [11], 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.

[9] describes our freely distributed Maple library SPECTRA, for Semidefinite Programming solved Exactly with Computational Tools of Real Algebra. It solves linear matrix inequalities 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.

Let $S \subset \mathbb{R}^n$ be a compact basic semi-algebraic set defined as the real solution set of multivariate polynomial inequalities with rational coefficients. In [19], we design an algorithm which takes as input a polynomial system defining S and an integer $p \geq 0$ and returns the n-dimensional volume of S at absolute precision 2^{-p}. Our algorithm relies on the relationship between volumes of semi-algebraic sets and periods of rational integrals. It makes use of algorithms computing the Picard-Fuchs differential equation of appropriate periods, properties of critical points, and high-precision numerical integration of differential equations. The algorithm runs in essentially linear time with respect to p. This improves upon the previous exponential bounds obtained by Monte-Carlo or moment-based methods. Assuming a conjecture of Dimca, the arithmetic cost of the algebraic subroutines for computing Picard-Fuchs equations and critical points is singly exponential in n and polynomial in the maximum degree of the input.

Let $\mathbf{f} = (f_1, ..., f_s)$ be a sequence of polynomials in $\mathbb{Q}[X_1, ..., X_n]$ of maximal degree D and $V \subset \mathbb{C}^n$ be the algebraic set defined by $\mathbf{f}$ and r be its dimension. The real radical $\sqrt{\langle \mathbf{f} \rangle}$ associated to $\mathbf{f}$ is the largest ideal which defines the real trace of V. When V is smooth, we show in [13], that $\sqrt[re]{\langle \mathbf{f} \rangle}$, has a finite set of generators with degrees bounded by $\deg V$. Moreover, we present a probabilistic algorithm of complexity $(snD^n)^{O(1)}$ to compute the minimal primes of $\sqrt[re]{\langle \mathbf{f} \rangle}$. 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 $V \cap \mathbb{R}^n$.

Let $(g_1, ..., g_p)$ in $\mathbb{Q}[X_1, ..., X_n]$ and S be the basic closed semi-algebraic set defined by $g_1 \geq 0, ..., g_p \geq 0$. The S-radical of $\langle \mathbf{f} \rangle$, which is denoted by $\sqrt[S]{\langle \mathbf{f} \rangle}$, is the ideal associated to the Zariski closure of $V \cap S$. We give a probabilistic algorithm to compute rational parametrizations of all irreducible components of that Zariski closure, hence encoding $\sqrt[S]{\langle \mathbf{f} \rangle}$. Assuming now that D is the maximum of the degrees of the f_i's and the g_i's, this algorithm runs in time $2^p(s+p)^{O(1)}(nD)^{O(rn2^r)}$.

Experiments are performed to illustrate and show the efficiency of our approaches on computing real radicals.

In [14], we consider the second-order discontinuous differential equation $y'' + \eta \mathrm{sgn}(y) = \theta y + \alpha \sin(\beta t)$ where the parameters $\eta, \theta, \alpha, \beta$ are real. The main goal is to discuss the existence of periodic solutions. Under explicit conditions, the number of such solutions is given. Furthermore, for each of these periodic solutions, an explicit formula is provided.

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

6.3.1. *Algebraic Cryptanalysis of a Quantum Money Scheme – The Noisy Case.*

At STOC 2012, Aaronson and Christiano proposed a noisy and a noiseless version of the first public-key quantum money scheme endowed with a security proof. [5] addresses the so-called noisy hidden subspaces problem, on which the noisy version of their scheme is based. The first contribution of this work is a non-quantum cryptanalysis of the above-mentioned noisy quantum money scheme extended to prime fields $\mathbb{F}$, with $|\mathbb{F}| \neq 2$, that runs in randomised polynomial time. This finding is supported with experimental results showing that, in practice, the algorithm presented is efficient and succeeds with overwhelming probability. The second contribution is a non-quantum randomised polynomial-time cryptanalysis of the noisy quantum money scheme over $\mathbb{F}_2$ succeeding with a certain probability for values of the noise lying within a certain range. This result disproves a conjecture made by Aaronson and Christiano about the non-existence of an algorithm that solves the noisy hidden subspaces problem over $\mathbb{F}_2$ and succeeds with such probability.

6.3.2. *On the Complexity of MQ in the Quantum Setting.*

In August 2015 the cryptographic world was shaken by a sudden and surprising announcement by the US National Security Agency NSA concerning plans to transition to post-quantum algorithms. Since this announcement post-quantum cryptography has become a topic of primary interest for several standardization bodies. The transition from the currently deployed public-key algorithms to post-quantum algorithms has been found to be challenging in many aspects. In particular the problem of evaluating the quantum-bit security of such post-quantum cryptosystems remains vastly open. Of course this question is of primarily concern in the process of standardizing the post-quantum cryptosystems. In [21] we consider the quantum security of the problem of solving a system of *m Boolean multivariate quadratic equations in n variables* (MQb); a central problem in post-quantum cryptography. When $n = m$, under a natural algebraic assumption, we present a Las-Vegas quantum algorithm solving MQb that requires the evaluation of, on average, $O(2^{0.462n})$ quantum gates. To our knowledge this is the fastest algorithm for solving MQb.

6.3.3. *MQsoft.*

In 2017, NIST shook the cryptographic world by starting a process for standardizing post-quantum cryptography. Sixty-four submissions have been considered for the first round of the on-going NIST Post-Quantum

Cryptography (PQC) process. Multivariate cryptography is a classical post-quantum candidate that turns to be the most represented in the signature category. At this stage of the process, it is of primary importance to investigate efficient implementations of the candidates. [17] presents `MQsoft`, an efficient library which permits to implement `HFE`-based multivariate schemes submitted to the NIST PQC process such as *GeMSS*, `Gui` and *DualModeMS*. The library is implemented in `C` targeting Intel 64-bit processors and using `avx2` set instructions. We present performance results for our library and its application to *GeMSS*, `Gui` and *DualModeMS*. In particular, we optimize several crucial parts for these schemes. These include root finding for `HFE` polynomials and evaluation of multivariate quadratic systems in $\mathbb{F}_2$. We propose a new method which accelerates root finding for specific `HFE` polynomials by a factor of two. For *GeMSS* and `Gui`, we obtain a speed-up of a factor between 2 and 19 for the keypair generation, between 1.2 and 2.5 for the signature generation, and between 1.6 and 2 for the verifying process. We have also improved the arithmetic in F_{2^n} by a factor of 4 compared to the `NTL` library. Moreover, a large part of our implementation is protected against timing attacks.

7. Bilateral Contracts and Grants with Industry

7.1. Technological Transfer

The group have had a continuous commitment into industrial transfer as well as a strong involvement into standardization bodies.

Industrial transfer. This activity is related to our long-standing activity in post-quantum cryptography. The transfer started at the beginning of the current evaluation period and culminated this year with the creation of a new spin-off, called CRYPTONEXT SECURITY [5], from Inria Paris and Sorbonne Université. The goal of CRYPTONEXT SECURITY is to propose security products that are resistant against the quantum computers. Its business model is based on B2B and targeted customers are Fortune 500 companies.

The activity has been partially founded and supervised by SATT-LUTECH who is specialized 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, University Panthéon-Assas, Paris Sorbonne University and National School of Industrial Creation). Typically, SATT-LUTECH has funded the post-quantum experiment described in the dedicated Section. The impact of such experiment can be partially measured by the press released covering out the test [6] (La Recherche, l'Usine Nouvelle, L'Informaticien).

As a preliminary step for launching the spin-off, two members of the team (J.-C. Faugère and L. Perret) followed two entrepreneurship programs for creating innovative companies : HEC Challenge plus [7] (1 week of courses by month, 9 months) and Deep Tech Founders [8] (3 months, 2 sessions by weeks). This was a necessary, but significant effort, before launching CRYPTONEXT in which the two members will work full-time from now on.

Post-quantum standardization. Besides the `NIST` PQC standardization process, we are involved in the on-going world effort for standardizing post-quantum cryptography. More precisely, the European Telecommunications Standards Institute (`ETSI`) has a strong standardization activity on post-quantum cryptography. `ETSI` is a EU standardization body with a worldwide scope. We are an active member of `ETSI` regarding post-quantum cryptography. In particular, we are the rapporteur of a technical document on post-quantum cryptosystems. The goal of our involvement is to bring our scientific expertise to define trustworthy post-quantum public-key standards; that are going to be the basis of our digital economy within $10/15$ years.

[5] https://cryptonext-security.com/
[6] https://www-polsys.lip6.fr/Links/index.html
[7] http://entrepreneurship-center.hec.edu/learn-program/hec-challenge-plus/
[8] https://deeptechfounders.com/

We are also involved in the Cloud Security Alliance (CSA). This is a large non-profit organization (80.000 member worldwide) whose main goal is to promote the best practices with the secure usage of cloud computing. CSA has a group dedicated to quantum-safe security. The group is ideation catalyzer for promoting the transition of companies to a quantum-safe security. In particular, the group has a significant educational activity in order to increase awareness regarding the quantum risk and the techniques to mitigate this risk. We are co-chairing this group and participated to several white papers. The group is probably now the main channel for promoting quantum-safe security. Standardization is a long-term effort.

8. Partnerships and Cooperations

8.1. Regional Initiatives

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

  COMPUTER ALGEBRA METHODS FOR SEMI-ALGEBRAIC PROGRAMMING

  `Participants`: J. Berthomieu [contact], M. Safey El Din.

  Semi-Algebraic Programming is the art of optimizing some quantity subject to semi-algebraic constraints. The very basic and natural instance of semi-algebraic programming is the problem of optimizating a polynomial function subject to polynomial inequalities and is known as the polynomial optimization problem (POP). More general instances of semi-algebraic programming are as follows: given a system of polynomial equations/inequalities depending on parameters, what are the parameters' values which maximize the dimension of the semi-algebraic set defined by the instantiated system? And when the number of solutions is finite, what is this maximum number of solutions? Hence Semi-Algebraic Programming encompasses a wide range of computational issues related to semi-algebraic sets. It finds applications in many engineering sciences. Let us mention the few ones that we target in CAMiSAdo: Path-planning optimization in robotics, Mobility properties of manipulators in mechanism design, Stability analysis for sensor-based controllers.

8.2. National Initiatives

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

  `Duration`: 2018–2022

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

  The demand for flexible, adaptable robots capable of interacting with their environment (e.g. navigation, handling, cooperation) is growing. This is why the sensor-based controllers, which make it possible to include external sensory feedback in robot control, have been widely developed in recent years, both for industrial, medical, air, space and marine robotics and in the context of autonomous vehicles (ground mobile robotics).

  The first research on sensor-based control techniques took place at the end of the 1980s, with the use of proximal and force and vision sensors, and much work has been done to improve the performance of this type of controllers, in particular by modelling various sensor primitives.

  Despite the fact that, empirically, sensor-based controllers have shown that they have interesting performances, these performances are by no means guaranteed, which is a major obstacle to the widespread use of their large-scale use. This is related to the fact that, despite three decades of research on the subject, two broad classes of problems have been little explored:

  – The study of the singularities of sensor-based controllers

  – The study of their stability.

  The objectives of the project SESAME are take advantage on recent mathematical advances in order to:

  - study singularities and stability of certain classes of sensor-based controllers
  - synthesize globally asymptotically stable sensor-based controllers, whose performance (i.e. convergence properties towards the desired configuration, abseance of local singularities and minima) are guaranteed in all object/sensor related configurations.

  Many of the computational tools SESAME relies on involve computer algebra and polynomial system solving.

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

  `Duration:` 2018–2022

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

  GALOP [9] 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.

- **ANR ECARP (Efficient Certified Algorithms for Robot Motion Planning)**

  `Duration:` 2020–2024

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

  ECARP is an international project, jointly funded by ANR and FWF (the funding agency of Austria). It targets the design and implementation of high-performance computer algebra algorithms for semi-algebraic sets in order to answer connectivity queries over those sets. This is applied to motion planning issues in robotics, e.g. for analyzing kinematic singularities ; parallel and serial manipulators will be investigated. The consortium gathers experts in geometry and robotics from J. Kepler Univ. (Austria) and LS2N (Nantes).

- **ANR DRN (DeRerumNatura)**

  `Duration:` 2020–2024

  `Participants:` J. Berthomieu [contact], M. Safey El Din.

  Classifying objects, determining their nature is more often than not the endgame of a theory. Yet, even the most established theory can be impractible on a concrete instance, either because of a lack of efficiency or because of a computational wall. In both cases, an algorithm is lacking: we need to systematize efficiently and automatically. This is what DRN proposes to do to solve classification problems related to numbers, analytic functions and combinactorics generating series. The consortium gathers experts in computer algebra (Inria Saclay, Limoges, Lyon, POLSYS), Combinactorics (Inria Saclay, Lyon) and Galois Theory (Toulouse, Strasbourg, Versailles).

8.2.1. 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 [10] 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.

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

[10] http://risq.fr/

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

- Innovative Training Network POEMA (Polynomial Optimization, Efficiency through Moments and Algebra) - ITN Marie Curie H2020 program.

  `Duration:` 2019–2023

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

  POEMA is part of the Marie Sklodowska-Curie Actions — Innovative Training Networks (ITN) funding scheme.

  POEMA aims 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.

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events: Organisation

9.1.1.1. General Chair, Scientific Chair

D. Wang was General co-chair of the 44th International Symposium on Symbolic and Algebraic Computation (ISSAC 2019) , Beijing, China, July 15-18, 2019).

9.1.1.2. Member of the Organizing Committees

J. Berthomieu was Poster chair of the 44th International Symposium on Symbolic and Algebraic Computation (ISSAC 2019), Beijing, China, July 15-18, 2019).

9.1.2. Scientific Events: Selection

9.1.2.1. Member of the Conference Program Committees

E. Prouff was member of the program committees of the following conferences:

- Smart Card Research and Advanced Application Conference (CARDIS) 2019
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES) 2019

D. Wang was member of the program committee of the International Symposium on Wen-Tsun Wu's Academic Thought and Mathematics Mechanization (Wu 2019) (Beijing, China, May 12-17, 2019). He was member of the scientific committee of the 4th International Conference on Numerical and Symbolic Computation (SYMCOMP 2019) (Porto, Portugal, April 11-12, 2019).

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

E. Prouff is member of the editorial board of Journal of Cryptographic Engineering.

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

D. Wang is Editor-In-Chief of Mathematics in Computer Science (published by Birkhäuser- Springer, Basel) and member of the Advisory Board for the journal • SCIENCE CHINA Information Sciences (published by Science China Press, Beijing and Springer, Berlin).

D. Wang is member of the Editorial Boards for the Journal of Symbolic Computation (published by Academic Press/Elsevier, London), SN Computer Science (published by Springer Nature, Switzerland) , Texts and Monographs in Symbolic Computation (published by Springer, Wien New York).

D. Wang is member of the International Advisory Board for Communications of JSSAC (Japan Society for Symbolic and Algebraic Computation) (published by JSSAC).

9.1.4. Invited Talks

E. Prouff was invited speaker at Spring School on Hardware Security (UK), the NIST Threshold Cryptography Workshop (USA), the Summer School on Real World Crypto and Privacy and the conference on Boolean Functions and Applications (BFA).

M. Safey El Din was invited speaker at the Arctic Applied Algebra conference (Norway), the workshop on Geometry of Real Polynomials, Convexity and Optimization at BIRS Banff International Research Station (Canada), the and the Conference in memory of Wen-tsun Wu's centennial birthday (China).

9.1.5. Scientific Expertise

M. Safey El Din was expert for the Czech Republic funding agency.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Jérémy Berthomieu had the following teaching activities:

Master : Polynomial System Solving, 13 hours, M2, Sorbonne Université & Polytech' Sorbonne, France.

Master : Computation Modeling, 42 hours, M1, Sorbonne Université, France.

Master : In charge of Basics of Algebraic Algorithms, 50 hours, M1, Sorbonne Université & Polytech' Sorbonne, France.

Master : Projects supervision, 7 hours, M1, Sorbonne Université, France.

Licence : Introduction to Cryptology, 15,75 hours, L3, Sorbonne Université , France.

Licence : Introduction to Numerical Algorithmic, 4,75 hours, L3, Sorbonne Université , France.

Licence : Introduction to Shell, 38,75 hours, L2, Sorbonne Université , France.

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

Jean-Charles Faugère had the following teaching activities:

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

Ludovic Perret had the following teaching activities:

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

Mohab Safey El Din has the following teaching activities:

Master : Polynomial System Solving, 40 hours, M1, Sorbonne Université & Polytech' Sorbonne, 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 : Matías Bender, Algorithms for sparse polynomial systems: Grbner basis and resultants, June 2019, 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 : Olive Chakraborty, Conception and cryptanalysis in secure quantic cryptography, started in May 2017, Jean-Charles Faugère and Ludovic Perret.

9.2.2.1. Juries

E. Prouff was member of the PhD committes of:

- Nicolas Belleville, Université Grenoble Alpes, 21-11-2019, "Compilation pour l'application de contre-mesures contre les attaques par canal auxiliaire"
- Joey Green, Université de Bristol, 20-10-2019, "A Study of Inference-Based Attacks with Neural Networks"
- Aberrahman DAIF, Université Paris 8, 03-05-2019, "Les codes correcteurs au service de la cryptographie symétrique et asymétrique"

J.C. Faugère was member of the PhD committes of:

- Robin Larrieu, École Polytechnique, dec. 2019, "Arithmetique rapide pour des corps finis"

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] M. BENDER. *Algorithms for sparse polynomial systems : Gröbner basis and resultants*, Sorbonne Université, 6 2019, http://page.math.tu-berlin.de/ mbender/etc/thesis.pdf

Articles in International Peer-Reviewed Journals

[2] E. BARTZOS, I. Z. EMIRIS, J. LEGERSKÝ, E. TSIGARIDAS. *On the maximal number of real embeddings of minimally rigid graphs in $\mathbb{R}^2$, $\mathbb{R}^3$ and S^2*, in "Journal of Symbolic Computation", 2019, https://arxiv.org/abs/1811.12800 , forthcoming [*DOI :* 10.1016/J.JSC.2019.10.015], https://hal.archives-ouvertes.fr/hal-02271782

[3] J. BERTHOMIEU, J.-C. FAUGÈRE. *In-depth comparison of the Berlekamp–Massey–Sakata and the Scalar-FGLM algorithms: the adaptive variants*, in "Journal of Symbolic Computation", 2019, https://arxiv.org/abs/1806.00978 , forthcoming [*DOI :* 10.1016/J.JSC.2019.09.001], https://hal.inria.fr/hal-01805478

[4] L. BUSÉ, A. MANTZAFLARIS, E. TSIGARIDAS. *Matrix formulae for Resultants and Discriminants of Bivariate Tensor-product Polynomials*, in "Journal of Symbolic Computation", June 2020, vol. 98, pp. 65-83 [*DOI :* 10.1016/J.JSC.2019.07.007], https://hal.inria.fr/hal-01654263

[5] M. CONDE PENA, R. DURÁN DÍAZ, J.-C. FAUGÈRE, L. HERNÁNDEZ ENCINAS, L. PERRET. *Non-quantum cryptanalysis of the noisy version of Aaronson–Christiano's quantum money scheme*, in "IET Information Security", July 2019, vol. 13, n^{o} 4, pp. 362-366 [*DOI :* 10.1049/IET-IFS.2018.5307], https://hal.inria.fr/hal-02395072

[6] I. Z. Emiris, A. Mantzaflaris, E. Tsigaridas. *Multilinear Polynomial Systems: Root Isolation and Bit Complexity*, in "Journal of Symbolic Computation", 2019, Special Issue of the Journal of Symbolic Computation on Milestones in Computer Algebra (MICA 2016), forthcoming, https://hal.inria.fr/hal-02099556

[7] I. Z. Emiris, B. Mourrain, E. Tsigaridas. *Separation bounds for polynomial systems*, in "Journal of Symbolic Computation", 2019 [*DOI :* 10.1016/j.jsc.2019.07.001], https://hal.inria.fr/hal-01105276

[8] D. Henrion, S. Naldi, M. Safey El Din. *Real root finding for low rank linear matrices*, in "Applicable Algebra in Engineering, Communication and Computing", 2019, https://arxiv.org/abs/1506.05897 [*DOI :* 10.1007/s00200-019-00396-w], https://hal.archives-ouvertes.fr/hal-01159210

[9] 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", January 2019, vol. 34, n^o 1, pp. 62-78, https://arxiv.org/abs/1611.01947 - Significantly extended version [*DOI :* 10.1080/10556788.2017.1341505], https://hal.laas.fr/hal-01393022

[10] V. Magron, M. Forets, D. Henrion. *Semidefinite Approximations of Invariant Measures for Polynomial Systems*, in "Discrete and Continuous Dynamical Systems - Series B", December 2019, vol. 24, n^o 12, pp. 6745-6770, https://arxiv.org/abs/1807.00754 - 28 pages, 14 figures [*DOI :* 10.3934/dcdsb.2019165], https://hal.archives-ouvertes.fr/hal-01828443

[11] 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", 2019, vol. 93, pp. 200-220 [*DOI :* 10.1016/j.jsc.2018.06.005], https://hal.archives-ouvertes.fr/hal-01538729

[12] L. Masure, C. Dumas, E. Prouff. *A Comprehensive Study of Deep Learning for Side-Channel Analysis*, in "IACR Transactions on Cryptographic Hardware and Embedded Systems", November 2019, vol. 2020, n^o 1, pp. 348-375 [*DOI :* 10.13154/tches.v2020.i1.348-375], https://hal.archives-ouvertes.fr/hal-02425261

[13] M. Safey El Din, Z.-H. Yang, L. Zhi. *Computing real radicals and S-radicals of polynomial systems*, in "Journal of Symbolic Computation", November 2019 [*DOI :* 10.1016/j.jsc.2019.10.018], https://hal.sorbonne-universite.fr/hal-02388168

[14] C. da Silva, A. Jacquemard, M. Teixeira. *Periodic Solutions of a Class of Non-autonomous Discontinuous Second-Order Differential Equations*, in "Journal of Dynamical and Control Systems", 2019, pp. 1-28, forthcoming [*DOI :* 10.1007/s10883-018-9426-7], https://hal-univ-bourgogne.archives-ouvertes.fr/hal-02094522

International Conferences with Proceedings

[15] A. Bauer, H. Gilbert, G. Renault, M. Rossi. *Assessment of the Key-Reuse Resilience of NewHope*, in "CT-RSA 2019 - The Cryptographers' Track at the RSA Conference", San Francisco, United States, M. Matsui (editor), Lecture Notes in Computer Science, Springer, February 2019, vol. 11405, pp. 272-292 [*DOI :* 10.1007/978-3-030-12612-4_14], https://hal.archives-ouvertes.fr/hal-02139910

[16] M. R. Bender, J.-C. Faugère, E. P. Tsigaridas. *Gröbner Basis over Semigroup Algebras: Algorithms and Applications for Sparse Polynomial Systems*, in "ISSAC 2019 - 44th International Symposium on Symbolic and Algebraic Computation", Beijing, China, ACM, July 2019, pp. 42-49, https://arxiv.org/abs/1902.00208 [*DOI :* 10.1145/3326229.3326248], https://hal.inria.fr/hal-02002689

[17] J.-C. FAUGÈRE, L. PERRET, J. RYCKEGHEM. *Software Toolkit for HFE-based Multivariate Schemes*, in "CHES 2019 : International Conference on Cryptographic Hardware and Embedded Systems", Atlanta, United States, IACR Transactions on Cryptographic Hardware and Embedded Systems, May 2019, vol. 2019, n^{o} 3, pp. 257-304 [*DOI :* 10.13154/TCHES.V2019.I3.257-304], https://hal.sorbonne-universite.fr/hal-02389747

[18] E. KUSHILEVITZ, R. OSTROVSKY, E. PROUFF, A. ROSÉN, A. THILLARD, D. VERGNAUD. *Lower and Upper Bounds on the Randomness Complexity of Private Computations of AND*, in "TCC 2019 - 17th International Conference on Theory of Cryptography", Nuremberg, Germany, D. HOFHEINZ, A. ROSEN (editors), Lecture Notes in Computer Science, Springer, November 2019, vol. 11892, pp. 386-406 [*DOI :* 10.1007/978-3-030-36033-7_15], https://hal.archives-ouvertes.fr/hal-02395052

[19] P. LAIREZ, M. MEZZAROBBA, M. SAFEY EL DIN. *Computing the volume of compact semi-algebraic sets*, in "ISSAC 2019 - International Symposium on Symbolic and Algebraic Computation", Beijing, China, ACM, July 2019, https://arxiv.org/abs/1904.11705 , https://hal.archives-ouvertes.fr/hal-02110556

Other Publications

[20] M. R. BENDER, J.-C. FAUGÈRE, L. PERRET, E. TSIGARIDAS. *A nearly optimal algorithm to decompose binary forms*, April 2019, https://arxiv.org/abs/1810.12588 - Accepted to JSC, https://hal.archives-ouvertes.fr/hal-01907777

[21] J.-C. FAUGÈRE, K. HORAN, D. KAHROBAEI, M. KAPLAN, E. KASHEFI, L. PERRET. *Fast Quantum Algorithm for Solving Multivariate Quadratic Equations*, August 2019, https://arxiv.org/abs/1712.07211 - working paper or preprint, https://hal.inria.fr/hal-01995374

[22] T.-H. VU. *Solution maps of polynomial variational inequalities*, February 2020, working paper or preprint, https://hal.sorbonne-universite.fr/hal-02468977