IN PARTNERSHIP WITH:
CNRS

Université Pierre et Marie Curie (Paris 6)

Activity Report 2015

Project-Team POLSYS

Polynomial Systems

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

RESEARCH CENTER
Paris - Rocquencourt

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:

2.4. - Reliability, certification
4.3. - Cryptography
4.3.1. - Public key cryptography
6.2.6. - Optimization
6.2.7. - High performance computing
7.2. - Discrete mathematics, combinatorics
7.5. - Geometry
7.6. - Computer Algebra

Other Research Topics and Application Domains:

5. - Industry of the future
5.2. - Design and manufacturing
6. - IT and telecom
6.3. - Network functions
6.5. - Information systems
9.4.1. - Computer science
9.4.2. - Mathematics
9.8. - Privacy

1. Members

Research Scientists

Jean-Charles Faugère [Team leader, Inria, Senior Researcher, HdR]
Alain Jacquemard [Univ. Bourgogne, Professor, Délégation Inria, HdR]
Elias Tsigaridas [Inria, Researcher]

Faculty Members

Jérémy Berthomieu [UPMC, Associate Professor]
Ludovic Perret [UPMC, Associate Professor]
Guénaël Renault [UPMC, Associate Professor]
Mohab Safey El Din [UPMC, Professor, HdR]

Engineer

Jérôme Govinden [SATT-LUTECH, from Nov. 2015]

PhD Students

Ivan Bannwarth [UPMC]
Matías Bender [Inria, from Dec. 2015]
Simone Naldi [LAAS/CNRS, until Sept. 2015]
Ulrick Severin [Dassault Systèmes]
Frédéric Urvoy de Portzamparc [Inria, until Mar. 2015]
Thibaut Verron [UPMC]
Alexandre Wallet [Inria]

Rina Zeitoun [Oberthur Technologies, until Jul. 2015]

Post-Doctoral Fellow

Brice Boyer [UPMC, until Aug. 2015]

Visiting Scientists

Carlos Améndola Cerón [Technische Universität Berlin, Germany, Sept. 2015]
Marta Conde Pena [Instituto de Tecnologías Físicas y de la Información, Spain, since May 2015 until Oct 2015]
Christian Eder [Technische Universität Kaiserslautern, Germany, regularly]
Kaie Kubjas [Aalto-yliopisto, Finland, Oct. 2015]
Cordian Riener [Aalto-yliopisto, Finland, May 2015]
Rheka Thomas [University of Washington, USA, Feb. 2015]
Igor Shparlinki [University of New South Wales, Australia, Sept. 2015]

Administrative Assistants

Nelsia Euphrasie [Inria]
Irphane Khan [UPMC]
Nelly Maloisel [Inria]

Others

Matías Bender [Inria, Internship, until Feb. 2015]
Jérôme Govinden [UPMC, Internship, from Feb. 2015 until Sept 2015]
Daniel Lazard [UPMC, Professor, Émérite, HdR]
Emmanuel Prouff [ANSSI, from Sept. 2015, Associate Member, HdR]
Dongming Wang [CNRS, Senior Researcher, Associate Member, HdR]

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 a building blocks for higher level algorithms who compute real sample points in the solution set of polynomial systems, decide connectivity queries and quantifier elimination over the reals. The major challenge facing the designer or the user of such algorithms is the intrinsic exponential behaviour of the complexity for computing Gröbner bases. The current proposal is an attempt to tackle these issues in a number of different ways: improve the efficiency of the fundamental algorithms (even when the complexity is exponential), develop high performance implementation exploiting parallel computers, and investigate new classes of structured algebraic problems where the complexity drops to polynomial time.

3.2. Fundamental Algorithms and Structured Systems

Participants: Jean-Charles Faugère, Mohab Safey El Din, Elias Tsigaridas, Guénaël Renault, Dongming Wang, Jérémy Berthomieu, Thibaut Verron.

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

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

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

[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, Daniel Lazard, Elias Tsigaridas, Simone Naldi, Ivan Bannwarth.

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, Christian Eder, Elias Tsigaridas.

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

Dedicated algebraic tools for Algebraic Number Theory. Recent results in Algebraic Number Theory tend to show that the computation of Gröbner basis is a key step toward the resolution of difficult problems in this domain [2]. Using existing resolution methods is simply not enough to solve relevant problems. The main algorithmic bottleneck to overcome is to adapt the Gröbner basis computation step to the specific problems. Typically, problems coming from Algebraic Number Theory usually have a lot of symmetries or the input systems are very structured. This is the case in particular for problems coming from the algorithmic theory of Abelian varieties over finite fields [3] where the objects are represented by polynomial system and are endowed with intrinsic group actions. The main goal here is to provide dedicated algebraic resolution algorithms and implementations for solving such problems. We do not restrict our focus on problems in positive characteristic. For instance, tower of algebraic fields can be viewed as triangular sets; more generally, related problems (e.g. effective Galois theory) which can be represented by polynomial systems will receive our attention. This is motivated by the fact that, for example, computing small integer solutions of Diophantine polynomial systems in connection with Coppersmith's method would also gain in efficiency by using a dedicated Gröbner bases computations step.

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

Participants: Jean-Charles Faugère, Ludovic Perret, Guénaël Renault, Frédéric Urvoy de Portzamparc, Rina Zeitoun, Jérémy Berthomieu.

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

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

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

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

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

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

4. Highlights of the Year

4.1. Highlights of the Year

Our joint research project GOAL@SiliconValley with Californian University UC Berkeley has been selected by Inria (2015-2018). GOAL led by Bernd Sturmfels (UC Berkeley) and Jean-Charles Faugère (POLSYS, Inria Paris-Rocquencourt) on "Geometry and Optimization with ALgebraic methods": The goal of this project is to develop algorithms and mathematical tools to solve geometric and optimization problems through algebraic techniques. As a long-term goal, the joint team plans to develop new software to solve these problems more efficiently. These objectives encompass the challenge of identifying instances of these problems that can be solved in polynomial time with respect to the number of solutions and modeling these problems with polynomial equations.

The webpage of the research project is http://www-polsys.lip6.fr/GOAL/index.html

The kickoff workshop was held at UC Berkeley in May 2015, see https://math.berkeley.edu/~bernd/GOALworkshop.html.

5. New Software and Platforms

5.1. FGb

FUNCTIONAL DESCRIPTION

FGb is a powerful software for computing Groebner bases.It includes the new generation of algorihms for computing Gröbner bases polynomial systems (mainly the F4,F5 and FGLM algorithms).It is implemented in C/C++ (approximately 250000 lines), standalone servers are available on demand. Since 2006, FGb is dynamically linked with Maple software (version 11 and higher) and is part of the official distribution of this software.

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

5.2. FGb Light

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

5.3. 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: Brice Boyer
- URL: http://www-polsys.lip6.fr/~jcf/Software/index.html

5.4. RAGlib

FUNCTIONAL DESCRIPTION

RAGLib is a Maple library for solving over the reals polynomial systems and computing sample points in semi-algebraic sets.

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

5.5. 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 $\sim 5\,000$ lines.

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

6. New Results

6.1. Fundamental algorithms and structured polynomial systems

6.1.1. On the complexity of the F5 Gröbner basis algorithm

We study the complexity of Gröbner bases computation, in particular in the generic situation where the variables are in simultaneous Noether position with respect to the system.

We give a bound on the number of polynomials of degree d in a Gröbner basis computed by F_5 algorithm in this generic case for the grevlex ordering (which is also a bound on the number of polynomials for a reduced Gröbner basis, independently of the algorithm used). Next, we analyse more precisely the structure of the polynomials in the Gröbner bases with signatures that F_5 computes and use it to bound the complexity of the algorithm.

Our estimates show that the version of F_5 we analyse, which uses only standard Gaussian elimination techniques, outperforms row reduction of the Macaulay matrix with the best known algorithms for moderate degrees, and even for degrees up to the thousands if Strassen's multiplication is used. The degree being fixed, the factor of improvement grows exponentially with the number of variables.

6.1.2. On the complexity of computing Gröbner bases for weighted homogeneous systems

Solving polynomial systems arising from applications is frequently made easier by the structure of the systems. Weighted homogeneity (or quasi-homogeneity) is one example of such a structure: given a system of weights $W = (w_1, ..., w_n)$, W-homogeneous polynomials are polynomials which are homogeneous w.r.t the weighted degree $\deg\left(X_1^{\alpha_1} \cdots X_n^{\alpha_n}\right) = \sum_{i=1}^{n} w_i \alpha_i$. Gröbner bases for weighted homogeneous systems can be computed by adapting existing algorithms for homogeneous systems to the weighted homogeneous case. In [6], we show that in this case, the complexity estimate for Algorithm F_5 $\left(\binom{n+d_{\max}-1}{d_{\max}}^{\omega}\right.$ can be divided by a factor $\left(\prod_{i=1} w_i\right)^{\omega}$). For zero-dimensional systems, the complexity of Algorithm FGLM nD^{ω} (where D is the number of solutions of the system) can be divided by the same factor $\left(\prod_{i=1} w_i\right)^{\omega}$. Under genericity assumptions, for zero-dimensional weighted homogeneous systems of W-degree $(d_1, ..., d_n)$, these complexity estimates are polynomial in the weighted Bézout bound $\prod_{i=1}^{n} d_i / \prod_{i=1}^{n} w_i$. Furthermore, the maximum degree reached in a run of Algorithm F_5 is bounded by the weighted Macaulay bound $\sum_{i=1}^{n} (d_i - w_i) + w_n$, and this bound is sharp if we can order the weights so that $w_n = 1$. For overdetermined semi-regular systems, estimates from the homogeneous case can be adapted to the weighted case. We provide some experimental results based on systems arising from a cryptography problem and from polynomial inversion problems. They show that taking advantage of the weighted homogeneous structure yields substantial speed-ups, and allows us to solve systems which were otherwise out of reach.

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

Sakata generalized the Berlekamp – Massey algorithm to n dimensions in 1988. The Berlekamp – Massey – Sakata (BMS) algorithm can be used for finding a Gröbner basis of a 0-dimensional ideal of relations verified by a table. We investigate this problem using linear algebra techniques, with motivations such as accelerating change of basis algorithms (FGLM) or improving their complexity. In [12], we first define and characterize multidimensional linear recursive sequences for 0-dimensional ideals. Under genericity assumptions, we propose a randomized preprocessing of the table that corresponds to performing a linear change of coordinates on the polynomials associated with the linear recurrences. This technique then essentially reduces our problem to using the efficient 1-dimensional Berlekamp – Massey (BM) algorithm. However, the number of probes to the table in this scheme may be elevated. We thus consider the table in the *black-box* model: we assume probing the table is expensive and we minimize the number of probes to the table in our complexity model. We produce an FGLM-like algorithm for finding the relations in the table, which lets us use linear algebra techniques. Under some additional assumptions, we make this algorithm adaptive and reduce further the number of table probes. This number can be estimated by counting the number of distinct elements in a multi-Hankel matrix (a multivariate generalization of Hankel matrices); we can relate this quantity with the *geometry* of the final staircase. Hence, in favorable cases such as convex ones, the complexity is essentially linear in the size of the output. Finally, when using the LEX ordering, we can make use of fast structured linear algebra similarly to the Hankel interpretation of Berlekamp – Massey.

6.1.4. Nearly optimal computations with structured matrices

In [9] we estimate the Boolean complexity of multiplication of structured matrices by a vector and the solution of nonsingular linear systems of equations with these matrices. We study four basic and most popular classes,

that is, Toeplitz, Hankel, Cauchy and Vandermonde matrices, for which the cited computational problems are equivalent to the task of polynomial multiplication and division and polynomial and rational multipoint evaluation and interpolation. The Boolean cost estimates for the latter problems have been obtained by Kirrinnis in [10], except for rational interpolation. We supply them now as well as the Boolean complexity estimates for the important problems of multiplication of transposed Vandermonde matrix and its inverse by a vector. All known Boolean cost estimates for such problems rely on using Kronecker product. This implies the d-fold precision increase for the d-th degree output, but we avoid such an increase by relying on distinct techniques based on employing FFT. Furthermore we simplify the analysis and make it more transparent by combining the representations of our tasks and algorithms both via structured matrices and via polynomials and rational functions. This also enables further extensions of our estimates to cover Trummer's important problem and computations with the popular classes of structured matrices that generalize the four cited basic matrix classes, as well as the transposed Vandermonde matrices. It is known that the solution of Toeplitz, Hankel, Cauchy, Vandermonde, and transposed Vandermonde linear systems of equations is generally prone to numerical stability problems, and numerical problems arise even for multiplication of Cauchy, Vandermonde, and transposed Vandermonde matrices by a vector. Thus our FFT-based results on the Boolean complexity of these important computations could be quite interesting because our estimates are reasonable even for more general classes of structured matrices, showing rather moderate growth of the complexity as the input size increases.

6.2. Solving Polynomial Systems over the Reals and Applications

6.2.1. Probabilistic Algorithm for Computing the Dimension of Real Algebraic Sets

Let $f \in \mathbb{Q}[X_1, ..., X_n]$ be a polynomial of degree D. We consider the problem of computing the real dimension of the real algebraic set defined by $f = 0$. Such a problem can be reduced to quantifier elimination. Hence it can be tackled with Cylindrical Algebraic Decomposition within a complexity that is doubly exponential in the number of variables. More recently, denoting by d the dimension of the real algebraic set under study, deterministic algorithms running in time $D^{O(d(n-d))}$ have been proposed. However, no implementation reflecting this complexity gain has been obtained and the constant in the exponent remains unspecified. In [11], we design a probabilistic algorithm which runs in time which is essentially cubic in $D^{d(n-d)}$. Our algorithm takes advantage of genericity properties of polar varieties to avoid computationally difficult steps of quantifier elimination. We also report on a first implementation. It tackles examples that are out of reach of the state-of-the-art and its practical behavior reflects the complexity gain.

6.2.2. Real root finding for determinants of linear matrices

Let $A_0, A_1, ..., A_n$ be given square matrices of size m with rational coefficients. The paper [7] focuses on the exact computation of one point in each connected component of the real determinantal variety $\{x \in \mathbb{R}^n : \det(A_0 + x_1A_1 + \cdots + x_nA_n) = 0\}$. Such a problem finds applications in many areas such as control theory, computational geometry, optimization, etc. Using standard complexity results this problem can be solved using $m^{O(n)}$ arithmetic operations. Under some genericity assumptions on the coefficients of the matrices, we provide in an algorithm solving this problem whose runtime is essentially quadratic in $\binom{n+m}{n}^3$. We also report on experiments with a computer implementation of this algorithm. Its practical performance illustrates the complexity estimates. In particular, we emphasize that for subfamilies of this problem where m is fixed, the complexity is polynomial in n.

6.2.3. Real root finding for rank defects in linear Hankel matrices

Let $H_0, ..., H_n$ be $m \times m$ matrices with entries in $\mathbb{Q}$ and Hankel structure, i.e. constant skew diagonals. We consider the linear Hankel matrix $H(X) = H_0 + X_1H_1 + \cdots + X_nH_n$ and the problem of computing sample points in each connected component of the real algebraic set defined by the rank constraint $\mathsf{rank}(H(X)) \leq r$, for a given integer $r \leq m - 1$. Computing sample points in real algebraic sets defined by rank defects in linear matrices is a general problem that finds applications in many areas such as control theory, computational geometry, optimization, etc. Moreover, Hankel matrices appear in many areas of engineering sciences. Also, since Hankel matrices are symmetric, any algorithmic development for this problem

can be seen as a first step towards a dedicated exact algorithm for solving semi-definite programming problems, i.e. linear matrix inequalities. Under some genericity assumptions on the input (such as smoothness of an incidence variety), we design in [18] a probabilistic algorithm for tackling this problem. It is an adaptation of the so-called critical point method that takes advantage of the special structure of the problem. Its complexity reflects this: it is essentially quadratic in specific degree bounds on an incidence variety. We report on practical experiments and analyze how the algorithm takes advantage of this special structure. A first implementation outperforms existing implementations for computing sample points in general real algebraic sets: it tackles examples that are out of reach of the state-of-the-art.

6.2.4. Optimizing a Parametric Linear Function over a Non-compact Real Algebraic Variety

In [17], we consider the problem of optimizing a parametric linear function over a non-compact real trace of an algebraic set. Our goal is to compute a representing polynomial which defines a hypersurface containing the graph of the optimal value function. Rostalski and Sturmfels showed that when the algebraic set is irreducible and smooth with a compact real trace, then the least degree representing polynomial is given by the defining polynomial of the irreducible hypersurface dual to the projective closure of the algebraic set. First, we generalize this approach to non-compact situations. We prove that the graph of the opposite of the optimal value function is still contained in the affine cone over a dual variety similar to the one considered in compact case. In consequence, we present an algorithm for solving the considered parametric optimization problem for generic parameters' values. For some special parameters' values, the representing polynomials of the dual variety can be identically zero, which give no information on the optimal value. We design a dedicated algorithm that identifies those regions of the parameters' space and computes for each of these regions a new polynomial defining the optimal value over the considered region.

6.2.5. Bounds for the Condition Number of Polynomials Systems with Integer Coefficients

Polynomial systems of equations are a central object of study in computer algebra. Among the many existing algorithms for solving polynomial systems, perhaps the most successful numerical ones are the homotopy algorithms. The number of operations that these algorithms perform depends on the condition number of the roots of the polynomial system. Roughly speaking the condition number expresses the sensitivity of the roots with respect to small perturbation of the input coefficients. A natural question to ask is how can we bound, in the worst case, the condition number when the input polynomials have integer coefficients? In [19] we address this problem and we provide effective bounds that depend on the number of variables, the degree and the maximum coefficient bitsize of the input polynomials. Such bounds allows to estimate the bit complexity of the algorithms that depend on the separation bound, like the homotopy algorithms, for solving polynomial systems.

6.2.6. Nearly Optimal Refinement of Real Roots of a Univariate Polynomial

In [10] we assume that a real square-free polynomial A has a degree d, a maximum coefficient bitsize τ and a real root lying in an isolating interval and having no nonreal roots nearby (we quantify this assumption). Then, we combine the *Double Exponential Sieve* algorithm (also called the *Bisection of the Exponents*), the bisection, and Newton iteration to decrease the width of this inclusion interval by a factor of $t = 2^{-L}$. The algorithm has Boolean complexity $\widetilde{O}_B(d^2\tau + dL)$. Our algorithms support the same complexity bound for the refinement of r roots, for any $r \leq d$.

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

The known algorithms approximate the roots of a complex univariate polynomial in nearly optimal arithmetic and Boolean time. They are, however, quite involved and require a high precision of computing when the degree of the input polynomial is large, which causes numerical stability problems. We observe that these difficulties do not appear at the initial stages of the algorithms, and in [8] we extend one of these stages, analyze it, and avoid the cited problems, still achieving the solution within a nearly optimal complexity estimates, provided that some mild initial isolation of the roots of the input polynomial has been ensured. The resulting algorithms promise to be of some practical value for root-finding and can be extended to the

problem of polynomial factorization, which is of interest on its own right. We conclude with outlining such an extension, which enables us to cover the cases of isolated multiple roots and root clusters.

6.2.8. Polynomial Interrupt Timed Automata

Interrupt Timed Automata (ITA) form a subclass of stopwatch automata where reachability and some variants of timed model checking are decidable even in presence of parameters. They are well suited to model and analyze real-time operating systems. Here we extend ITA with polynomial guards and updates, leading to the class of polynomial ITA (polITA). In [13], we prove that reachability is decidable in 2EXPTIME on polITA, using an adaptation of the cylindrical algebraic decomposition algorithm for the first-order theory of reals using symbolic computation. Compared to previous approaches, our procedure handles parameters and clocks in a unified way. We also obtain decidability for the model checking of a timed version of CTL and for reachability in several extensions of polITA.

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

6.3.1. Polynomial-Time Algorithms for Quadratic Isomorphism of Polynomials: The Regular Case

Let $\mathbf{f} = (f_1, ..., f_m)$ and $\mathbf{g} = (g_1, ..., g_m)$ be two sets of $m \geq 1$ nonlinear polynomials in $\mathbb{K}[x_1, ..., x_n]$ ($\mathbb{K}$ being a field). In [3], we consider the computational problem of finding – if any – an invertible transformation on the variables mapping $\mathbf{f}$ to $\mathbf{g}$. The corresponding equivalence problem is known as *Isomorphism of Polynomials with one Secret* (`IP1S`) and is a fundamental problem in multivariate cryptography. Amongst its applications, we can cite Graph Isomorphism (`GI`) which reduces to equivalence of cubic polynomials with respect to an invertible linear change of variables, according to Agrawal and Saxena. The main result is a randomized polynomial-time algorithm for solving `IP1S` for quadratic instances, a particular case of importance in cryptography. To this end, we show that `IP1S` for quadratic polynomials can be reduced to a variant of the classical module isomorphism problem in representation theory. We show that we can essentially *linearize* the problem by reducing quadratic-`IP1S` to test the orthogonal simultaneous similarity of symmetric matrices; this latter problem was shown by Chistov, Ivanyos and Karpinski (ISSAC 1997) to be equivalent to finding an invertible matrix in the linear space $\mathbb{K}^{n\times n}$ of $n \times n$ matrices over $\mathbb{K}$ and to compute the square root in a certain representation in a matrix algebra. While computing square roots of matrices can be done efficiently using numerical methods, it seems difficult to control the bit complexity of such methods. However, we present exact and polynomial-time algorithms for computing a representation of the square root of a matrix in $\mathbb{K}^{n\times n}$, for various fields (including finite fields), as a product of two matrices. Each coefficient of these matrices lie in an extension field of $\mathbb{K}$ of polynomial degree. We then consider `#IP1S`, the counting version of `IP1S` for quadratic instances. In particular, we provide a (complete) characterization of the automorphism group of homogeneous quadratic polynomials. Finally, we also consider the more general *Isomorphism of Polynomials* (`IP`) problem where we allow an invertible linear transformation on the variables *and* on the set of polynomials. A randomized polynomial-time algorithm for solving `IP` when $\mathbf{f} = (x_1^d, ..., x_n^d)$ is presented. From an algorithmic point of view, the problem boils down to factoring the determinant of a linear matrix (*i.e.* a matrix whose components are linear polynomials). This extends to `IP` a result of Kayal obtained for `PolyProj`.

6.3.2. Factoring $N = p^r q^s$ for Large r and s

Boneh *et al.* showed at Crypto 99 that moduli of the form $N = p^r q$ can be factored in polynomial time when $r \simeq \log p$. Their algorithm is based on Coppersmith's technique for finding small roots of polynomial equations. In [15] we show that $N = p^r q^s$ can also be factored in polynomial time when r or s is at least $(\log p)^3$; therefore we identify a new class of integers that can be efficiently factored. We also generalize our algorithm to moduli with k prime factors $N = \prod_{i=1}^{k} p_i^{r_i}$; we show that a non-trivial factor of N can be extracted in polynomial-time if one of the exponents r_i is large enough.

6.3.3. On the Complexity of the BKW Algorithm on LWE

This work [1] presents a study of the complexity of the Blum–Kalai–Wasserman (BKW) algorithm when applied to the Learning with Errors (LWE) problem, by providing refined estimates for the data and computational effort requirements for solving concrete instances of the LWE problem. We apply this refined analysis to suggested parameters for various LWE-based cryptographic schemes from the literature and compare with alternative approaches based on lattice reduction. As a result, we provide new upper bounds for the concrete hardness of these LWE-based schemes. Rather surprisingly, it appears that BKW algorithm outperforms known estimates for lattice reduction algorithms starting in dimension $n \approx 250$ when LWE is reduced to SIS. However, this assumes access to an unbounded number of LWE samples.

6.3.4. Structural Cryptanalysis of McEliece Schemes with Compact Keys

A very popular trend in code-based cryptography is to decrease the public-key size by focusing on subclasses of alternant/Goppa codes which admit a very compact public matrix, typically quasi-cyclic (QC), quasi-dyadic (QD), or quasi-monoidic (QM) matrices. In [5], we show that the very same reason which allows to construct a compact public-key makes the key-recovery problem intrinsically much easier. The gain on the public-key size induces an important security drop, which is as large as the compression factor p on the public-key. The fundamental remark is that from the $k \times n$ public generator matrix of a compact McEliece, one can construct a $k/p \times n/p$ generator matrix which is - from an attacker point of view - as good as the initial public-key. We call this new smaller code the folded code. Any key-recovery attack can be deployed equivalently on this smaller generator matrix. To mount the key-recovery in practice, we also improve the algebraic technique of Faugère, Otmani, Perret and Tillich (FOPT). In particular, we introduce new algebraic equations allowing to include codes defined over any prime field in the scope of our attack. We describe a so-called "structural elimination" which is a new algebraic manipulation which simplifies the key-recovery system. As a proof of concept, we report successful attacks on many cryptographic parameters available in the literature. All the parameters of CFS-signatures based on QD/QM codes that have been proposed can be broken by this approach. In most cases, our attack takes few seconds (the harder case requires less than 2 hours). In the encryption case, the algebraic systems are harder to solve in practice. Still, our attack succeeds against several cryptographic challenges proposed for QD and QM encryption schemes, but there are still some parameters that have been proposed which are out of reach for the methods given here. However, regardless of the key-recovery attack used against the folded code, there is an inherent weakness arising from Goppa codes with QM or QD symmetries. It is possible to derive from the public key a much smaller public key corresponding to the folding of the original QM or QD code, where the reduction factor of the code length is precisely the order of the QM or QD group used for reducing the key size. To summarize, the security of such schemes are not relying on the bigger compact public matrix but on the small folded code which can be efficiently broken in practice with an algebraic attack for a large set of parameters.

6.3.5. A Polynomial-Time Key-Recovery Attack on MQQ Cryptosystems

In [16], we investigate the security of the family of MQQ public key cryptosystems using multivariate quadratic quasigroups (MQQ). These cryptosystems show especially good performance properties. In particular, the MQQ-SIG signature scheme is the fastest scheme in the ECRYPT benchmarking of cryptographic systems (eBACS). We show that both the signature scheme MQQ-SIG and the encryption scheme MQQ-ENC, although using different types of MQQs, share a common algebraic structure that introduces a weakness in both schemes. We use this weakness to mount a successful polynomial time key-recovery attack that finds an equivalent key using the idea of so-called good keys. In the process we need to solve a MinRank problem that, because of the structure, can be solved in polynomial-time assuming some mild algebraic assumptions. We highlight that our theoretical results work in characteristic 2 which is known to be the most difficult case to address in theory for MinRank attacks and also without any restriction on the number of polynomials removed from the public-key. This was not the case for previous MinRank like-attacks against $\mathcal{MQ}$ schemes. From a practical point of view, we are able to break an MQQ-SIG instance of 80 bits security in less than 2 days, and one of the more conservative MQQ-ENC instances of 128 bits security in little bit over 9 days. Altogether, our attack shows that it is very hard to design a secure public key scheme based on an easily invertible MQQ structure.

6.3.6. Algebraic Cryptanalysis of a Quantum Money Scheme The Noise-Free Case

In [14], we investigate the Hidden Subspace Problem (HSP_q) over $\mathbb{F}_q$ which is as follows:

Input : $p_1, ..., p_m, q_1, ..., q_m \in \mathbb{F}_q[x_1, ..., x_n]$ of degree $d \geq 3$ (and $n \leq m \leq 2n$).
Find : a subspace $A \subset {\mathbb{F}_q}^n$ of dimension $n/2$ (n is even) such that

$$p_i(A) = 0 \ \forall i \in \{1, ..., m\} \text{ and } q_j(A^\perp) = 0 \ \forall j \in \{1, ..., m\},$$

where $A^\perp$ denotes the orthogonal complement of A with respect to the usual scalar product in $\mathbb{F}_q$.

This problem underlies the security of the first public-key quantum money scheme that is proved to be cryptographically secure under a non quantum but classic hardness assumption. This scheme was proposed by S. Aaronson and P. Christiano at STOC'12. In particular, it depends upon the hardness of HSP_2. More generally, Aaronson and Christiano left as an open problem to study the security of the scheme for a general field $\mathbb{F}_q$. We present a randomized polynomial-time algorithm that solves the HSP_q for $q > d$ with success probability $\approx 1 - 1/q$. So, the quantum money scheme extended to $\mathbb{F}_q$ is not secure for big q. Finally, based on experimental results and a structural property of the polynomials that we prove, we conjecture that there is also a randomized polynomial-time algorithm solving the HSP_2 with high probability. To support our theoretical results we also present several experimental results confirming that our algorithms are very efficient in practice. We emphasize that S. Aaronson and P. Christiano proposes a non-noisy and a noisy version of the public-key quantum money scheme. The noisy version of the quantum money scheme remains secure.

6.3.7. Folding Alternant and Goppa Codes with Non-Trivial Automorphism Groups

The main practical limitation of the McEliece public-key encryption scheme is probably the size of its key. A famous trend to overcome this issue is to focus on subclasses of alternant/Goppa codes with a non trivial automorphism group. Such codes display then symmetries allowing compact parity-check or generator matrices. For instance, a key-reduction is obtained by taking quasi-cyclic (QC) or quasi-dyadic (QD) alternant/Goppa codes. We show that the use of such symmetric alternant/Goppa codes in cryptography introduces a fundamental weakness. It is indeed possible to reduce the key-recovery on the original symmetric public-code to the key-recovery on a (much) smaller code that has not anymore symmetries. This result [4] is obtained thanks to a new operation on codes called folding that exploits the knowledge of the automorphism group. This operation consists in adding the coordinates of codewords which belong to the same orbit under the action of the automorphism group. The advantage is twofold: the reduction factor can be as large as the size of the orbits, and it preserves a fundamental property: folding the dual of an alternant (resp. Goppa) code provides the dual of an alternant (resp. Goppa) code. A key point is to show that all the existing constructions of alternant/Goppa codes with symmetries follow a common principal of taking codes whose support is globally invariant under the action of affine transformations (by building upon prior works of T. Berger and A. Dür). This enables not only to present a unified view but also to generalize the construction of QC, QD and even quasi-monoidic (QM) Goppa codes. All in all, our results can be harnessed to boost up any key-recovery attack on McEliece systems based on symmetric alternant or Goppa codes, and in particular algebraic attacks.

6.3.8. Improved Sieving on Algebraic Curves

The best algorithms for discrete logarithms in Jacobians of algebraic curves of small genus are based on index calculus methods coupled with large prime variations. For hyperelliptic curves, relations are obtained by looking for reduced divisors with smooth Mumford representation (Gaudry); for non-hyperelliptic curves it is faster to obtain relations using special linear systems of divisors (Diem, Diem and Kochinke). Recently, Sarkar and Singh have proposed a sieving technique, inspired by an earlier work of Joux and Vitse, to speed up the relation search in the hyperelliptic case. In [20], we give a new description of this technique, and show that this new formulation applies naturally to the non-hyperelliptic case with or without large prime variations. In particular, we obtain a speed-up by a factor approximately 3 for the relation search in Diem and Kochinke's methods.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

Gemalto. Gemalto is an international IT security company providing software applications, secure personal devices such as smart cards and token, POLSYS is currently working with Gemalto – thanks to a CIFRE PhD grant – on the security analysis of code-based cryptosystems (Participants: J.-C. Faugère, L. Perret, F. Urvoy de Portzamparc).

7.2. Industrial Transfer

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 now involved in the industrial transfer of post-quantum cryptography. The project 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 G5 type) that uses multivariate cryptography. The application has been tested mid-November in a series of experiments supervised by DGA and French Minsitry 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.

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- **ANR Grant HPAC: High Performance Algebraic Computing (2012-2016).** The pervasive ubiquity of parallel architectures and memory hierarchy has led to a new quest for parallel mathematical algorithms and software capable of exploiting the various levels of parallelism: from hardware acceleration technologies (multi-core and multi-processor system on chip, GPGPU, FPGA) to cluster and global computing platforms. For giving a greater scope to symbolic and algebraic computing, beyond the optimization of the application itself, the effective use of a large number of resources (memory and specialized computing units) is expected to enhance the performance multi-criteria objectives: time, resource usage, reliability, even energy consumption. The design and the implementation of mathematical algorithms with provable, adaptive and sustainable performance is a major challenge. In this context, this project is devoted to fundamental and practical research specifically in exact linear algebra and system solving that are two essential "dwarfs" (or "killer kernels") in scientific and algebraic computing. The project should lead to progress in matrix algorithms and challenge solving in cryptology, and should provide new insights into high performance programming and library design problems (J.-C. Faugère [contact], L. Perret, G. Renault, M. Safey El Din).

- **ANR Grant GeoLMI: Geometry of Linear Matrix Inequalities (2011-2015).** GeoLMI project aims at developing an algebraic and geometric study of linear matrix inequalities (LMI) for systems control theory. It is an interdisciplinary project at the border between information sciences (systems control), pure mathematics (algebraic geometry) and applied mathematics (optimisation). The project focuses on the geometry of determinantal varieties, on decision problems involving positive polynomials, on computational algorithms for algebraic geometry, on computational algorithms for semi-definite programming, and on applications of algebraic geometry techniques in systems control theory, namely for robust control of linear systems and polynomial optimal control (Participants: J.-C. Faugère, M. Safey El Din [contact], E. Tsigaridas).

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. A3

Type: PEOPLE

Instrument: Career Integration Grant

Duration: May 2013 - April 2017

Coordinator: Jean-Charles Faugère

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

Inria contact: Elias Tsigaridas

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

8.2.2. Collaborations in European Programs, except FP7 & H2020

Program: ICT COST Action IC1403

Project acronym : CRYPTACUS)

Project title: Cryptanalysis of ubiquitous computing systems

Duration: 12/2014 – 12/2018

Coordinator: Prof 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.

Program: COST Action IC1306

Project acronym : CryptoAction

Project title: Cryptography for Secure Digital Interaction

Duration: 04/2014 – 04/2018

Coordinator: Dr. Claudio ORLANDI

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

8.3. International Initiatives

8.3.1. Inria International Labs

8.3.1.1. Inria@SiliconValley

See https://project.inria.fr/siliconvalley/fr/

Associate Team involved in the International Lab:

GOAL

Title: Geometry and Optimization with ALgebraic methods.

International Partner (Institution - Laboratory - Researcher):

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

Start year: 2015

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

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

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

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

The kickoff workshop was held at UC Berkeley in May 2015, see https://math.berkeley.edu/~bernd/GOALworkshop.html.

Both Carlos Améndola Cerón and Kaies Kubjas visited the team one month through the associated team.

8.3.1.2. Sino-European Laboratory of Informatics, Automation and Applied Mathematics (LIAMA)

See http://liama.ia.ac.cn/.

Associate Team involved in the International Lab:

ECCA

Title: Exact/Certifed Computation with Algebraic Systems

International Partner (Institution - Laboratory - Researcher):

KLMM – Chinese Academy of Sciences, Lihong Zhi.

Start year: 2012

See also: http://liama.ia.ac.cn/research/liama-projects/current/265-ecca-project-description-and-achievements.html

Exact/Certifed Computation with Algebraic Systems (ECCA) is a project run within the LIAMA Consortium as a cooperation project between CNRS/Inria/LIP6, KLMM, SKLOIS and LMIB. The main scientific objective of this project is to study and compute the solutions of nonlinear algebraic systems and their structures and properties with target applications to computational geometry, algebraic cryptanalysis, global optimization, and algebraic biology.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Carlos Améndola Cerón

Date: Sept. 2015

Institution: Technische Universität Berlin, Germany

Kaie Kubjas

Date: Oct. 2015

Institution: Aalto Science Institute, Finland

Cordian Riener

Date: May 2015

Institution: Aalto Science Institute, Finland

Igor Shparlinski

Date: Sept. 2015

Institution: The University of New South Wales, Australia

Rekha Thomas

Date: Feb. 2015

Institution: University of Washington, USA.

8.4.1.1. Internships

Matías Bender

Date: Sep 2014 - Feb 2015

Institution: Universidad de Buenos Aires (Argentina)

Supervisor: Jean-Charles Faugère

Jérôme Govinden

Date: Feb. 2015 - Sept. 2015

Institution: UPMC

Supervisors: Jean-Charles Faugère, Ludovic Perret

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. General chair, scientific chair

Guénaël Renault and Emmanuel Prouff were both General Co-chairs of CHES 2015.

9.1.1.2. Member of the organizing committees

Dongming Wang was involved in the organization of the following conferences

- Fourth International Seminar on Program Verification, Automated Debugging and Symbolic Computation (PAS 2015) (Beijing, China, October 21-23, 2015);
- Dagstuhl Seminar 15471: Symbolic Computation and Satisfiability Checking ($(SC)^2$ 2015) (Dagstuhl, Germany, November 15-20, 2015);
- International Seminar on Geometric Computation (GC 2015) (Nanning, China, February 2-4, 2015).

9.1.2. Scientific events selection

9.1.2.1. Chair of conference program committees

Dongming Wang was Program Co-chair of the following conferences

- Fourth International Seminar on Program Verification, Automated Debugging and Symbolic Computation (PAS 2015) (Beijing, China, October 21-23, 2015);
- Dagstuhl Seminar 15471: Symbolic Computation and Satisfiability Checking ($(SC)^2$ 2015) (Dagstuhl, Germany, November 15-20, 2015);
- International Seminar on Geometric Computation (GC 2015) (Nanning, China, February 2-4, 2015).

9.1.2.2. Member of the conference program committees

Jean-Charles Faugère was member of the program committees of the following conferences

- PKC 2015
- Eurocrypt 2016

Ludovic Perret was member of the program committees of the following conferences

- The 7th International Workshop on Parallel Symbolic Computation (PASCO'15)
- The 41th International Symposium on Symbolic and Algebraic Computation (ISSAC'16)

Emmanuel Prouff was member of the program committees of the following conferences

- Workshop on Cryptographic Hardware and Embedded Systems (CHES 2015);
- 14th Smart Card Research and Advanced Application Conference (CARDIS 2015);
- 6th International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE);
- Indocrypt 2015.

Guénaël Renault was member of the program committees of the following conferences

- International Symposium on Symbolic and Algebraic Computation (ISSAC 2015)

Mohab Safey El Din was was member of the program committees of the following conference

- International Conference on Mathematical Aspects of Computer and Information Sciences (MACIS) 2015;

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

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

9.1.3. Journal

9.1.3.1. Member of the editorial boards

Ludovic Perret is Member of the Editorial Board of Designs, Codes and Cryptography.

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

Dongming Wang has the following editorial activities:

- Editor-in-Chief and Managing Editor for the journal
  Mathematics in Computer Science (published by Birkhäuser/Springer, Basel).
- Executive Associate Editor-in-Chief for the journal

SCIENCE CHINA Information Sciences (published by Science China Press, Beijing and Springer, Berlin).

- Member of the Editorial Boards for the
  - Journal of Symbolic Computation (published by Academic Press/Elsevier, London),
  - Frontiers of Computer Science (published by Higher Education Press, Beijing and Springer, Berlin),
  - Texts and Monographs in Symbolic Computation (published by Springer, Wien New York),
- Member of the International Advisory Board for the Communications of JSSAC (Japan Society for Symbolic and Algebraic Computation) (published by JSSAC).

9.1.4. Invited talks

Jean-Charles Faugère was invited speaker at

Workshop on "Grobner bases techniques for post-quantum cryptography", March 27, 2015 Washington (USA)

Workshop on Algebra, Geometry and Proofs in Symbolic Computation Thematic Program on Computer Algebra, Fields Inst. Toronto, Dec. 2015.

Sixth International Conference on Mathematical Aspects of Computer and Information Sciences (MACIS) Nov 11–13, 2015 Zuse Institute Berlin (ZIB), Germany.

Journées Nationales de Calcul Formel (3 hours lecture) Oct 2015, Cluny France

Daniel Lazard was special invited talk at Effective Methods in Algebraic Geometry 2015 - Università di Trento, Trento, June 2015.

Emmanuel Prouff was invited talk at Workshop on Constructive Side-Channel Analysis and Secure Design 2015, Mövenpick Hotel, Berlin, Apr. 2015.

Mohab Safey El Din was invited speaker at

Workshop on Algebra, Geometry and Proofs in Symbolic Computation Thematic Program on Computer Algebra, Fields Inst. Toronto, Dec. 2015.

Workshop on Linear Computer Algebra and Symbolic-Numeric Computation, Thematic Program on Computer Algebra, Fields Inst. Toronto, Oct. 2015.

Workshop Algebraic Vision, TU Berlin, October 2015.

Dagstuhl seminar on Complexity of Symbolic and Numeric Procedures, Dagstuhl, Germany, June 2015.

Czech workshop on applied mathematics in engineering Prague, Czech, February, 2015.

Mohab Safey El Din was also invited to give talks at

Minisymposium on Maximum Likelihood Degrees and Critical Points, SIAM Conference on Applied Algebraic Geometry, Daejoon, Aug. 2015, South-Korea.

Minisymposium on Real algebraic geometry and Optimization, SIAM Conference on Applied Algebraic Geometry, Daejoon, Aug. 2015, South-Korea.

Minisymposium on Polynomial Optimization and Moments, SIAM Conference on Applied Algebraic Geometry, Daejoon, Aug. 2015, South-Korea.

Elias Tsigaridas was invited speaker at

Workshop on Algebra, Geometry and Proofs in Symbolic Computation Thematic Program on Computer Algebra, Fields Inst. Toronto, Dec. 2015.

Structured Matrices Days 2015 June 4–5, 2015 XLIM-DMI, Université de Limoges, France.

Computer Algebra in Scientific Computing (CASC) September 14–18, 2015 RWTH Aachen University, Aachen, Germany.

9.1.5. Scientific expertise

Guénaël Renault had the following scientific expertise activities :

member of jury de selection du concours CR2 Inria Saclay

participating to the panel for research proposals selection in the field of theoretical computer science, Finland Academy.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Jérémy Berthomieu had the following teaching activities:

Master : Modeling and problems numerical and symbolic solving through MAPLE and MATLAB software, 52 hours, M1, Université Pierre-et-Marie-Curie, France

Master : In charge of Basics of Algebraic Algorithms, 70 hours, M1, Université Pierre-et-Marie-Curie, France

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

Licence : Numerical Algorithmic, 6 hours, L3, Université Pierre-et-Marie-Curie, France

Licence : Representations and Numerical Methods, 40 hours, L2, Université Pierre-et-Marie-Curie, France

Licence : Projects supervision, 20 hours, L2, Université Pierre-et-Marie-Curie, France

Jean-Charles Faugère had the following teaching activities:

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

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

Ludovic Perret had the following teaching activities amounting to around 220 hours:

Master : Polynomial Systems solving, M2, MPRI

Master : In charge of Introduction to Security, M1, Université Pierre-et-Marie-Curie, France

Master : In charge of Complexity, M1, Université Pierre-et-Marie-Curie, France

Licence : Introduction to Algorithmic, L2, Université Pierre-et-Marie-Curie, France

Licence : In charge of the Computer Science – Applied Mathematics Program (PIMA) in Licence, L2, Université Pierre-et-Marie-Curie, France

Licence : Project supervision, L2, Université Pierre-et-Marie-Curie, France

Guénaël Renault had the following teaching activities:

Master : In charge of the Security, Reliability and Numerical Efficiency Program in Master, 45 hours, M1 and M2, Université Pierre-et-Marie-Curie, France

Master : In charge of Advanced and Applied Cryptology, 70 hours, M2, Université Pierre-et-Marie-Curie, France

Master : In charge of Security and Side-channels, 10 hours, M2, Université Pierre-et-Marie-Curie, France

Master : In charge of Threats and Attacks Modeling, 40 hours, M1, Université Pierre-et-Marie-Curie, France

Master : Pro/Research internships supervision, 40 hours, M2, Université Pierre-et-Marie-Curie, France

Master : Projects supervision, 20 hours, M1, Université Pierre-et-Marie-Curie, France

Licence : In charge of Introduction to Cryptology, 30 hours, L3, Université Pierre-et-Marie-Curie, France

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

Mohab Safey El Din had the following teaching activities:

Master : In charge of Modeling and problems numerical and symbolic solving through MAPLE and MATLAB software, 18 hours, M1, Université Pierre-et-Marie-Curie, France

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

Master: In charge of Fundamental Algorithms in Real Algebraic Geometry, 22,5 hours, M2, ENS de Lyon, France

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

Licence : In charge of the Computer Science – Applied Mathematics Program (PIMA) in Licence, L2 and L3, Université Pierre-et-Marie-Curie, France

Mohab Safey El Din gave also a course at the "Ecole Jeunes Chercheurs 2015" of GDR IM.

9.2.2. Supervision

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

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

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

PhD : Simone Naldi, Exact algorithms for determinantal varieties and semidefinite programming, Univ. Toulouse, defended in Sept. 2015, Didier Henrion and Mohab Safey El Din

PhD in progress : Adrian Thillard, Countermeasures to side-channel attacks and secure multi-party computation, Damien Vergnaud, Emmanuel Prouff

PhD : Fréderic Urvoy de Portzamparc, Algebraic and physical security based on error-correcting codes, Université Pierre-et-Marie-Curie, defended in Apr. 2015, Jean-Charles Faugère and Ludovic Perret

PhD in progress : Thibaut Verron, Gröbner bases and structured polynomial systems, started in Sept. 2012, Jean-Charles Faugère and Mohab Safey El Din

PhD : Rina Zeitoun, Algebraic methods for the analysis of the security of cryptographic algorithms implementations, Université Pierre-et-Marie-Curie, defended in July 2015, Jean-Charles Faugère and Guénaël Renault

9.2.3. Juries

Jean-Charles Faugère was:

reviewer and member of the PhD committee of Tristan Vaccon;

member of the PhD committee of Simone Naldi;

member of the PhD committee of Frédéric de Portzamparc;

member of the PhD committee of Simone Naldi;

Ludovic Perret was:

member of the PhD committee of Frédéric de Portzamparc;

Emmanuel Prouff was:

member of the PhD committee of Luke Maher;

member of the PhD committee of Mathieu Carbone;

member of the PhD committee of Praveen Vadnala;

member of the PhD committee of Sonia Belaid;

member of the PhD committee of Sylvain Ruhault;

member of the PhD committee of Vincent Grosso;

member of the PhD committee of Annelie Heuser as reviewer;

member of the PhD committee of Kevin Layat.

Guénaël Renault was:

member of the PhD committee of Rina Zeitoun;

member of mid-term evaluation committee of Nicolas Bruneau;

Mohab Safey El Din was:

member of the PhD committee of Simone Naldi;

member of the PhD committee of Frédéric Urvoy de Portzamparc;

Elias Tsigaridas was

member of the PhD committee of Aaron Herman;

member of the mid-term evaluation committee of Mario Cornejo-Ramirez;

9.3. Popularization

Mohab Safey El Din gave a course at the “Ecole Jeunes Chercheurs 2015” of GDR IM and wrote for it a book chapter [21].

10. Bibliography

Publications of the year

Articles in International Peer-Reviewed Journals

[1] M. ALBRECHT, C. CID, J.-C. FAUGÈRE, R. FITZPATRICK, L. PERRET. *On the complexity of the BKW algorithm on LWE*, in "Designs, Codes and Cryptography", February 2015, vol. 74, n° 2, 26 p. [*DOI :* 10.1007/s10623-013-9864-x], https://hal.inria.fr/hal-00921517

[2] M. BARDET, J.-C. FAUGÈRE, B. SALVY. *On the complexity of the F5 Gröbner basis algorithm*, in "Journal of Symbolic Computation", September 2015, vol. 70, pp. 49–70 [*DOI :* 10.1016/j.jsc.2014.09.025], https://hal.inria.fr/hal-01064519

[3] J. BERTHOMIEU, J.-C. FAUGÈRE, L. PERRET. *Polynomial-Time Algorithms for Quadratic Isomorphism of Polynomials: The Regular Case*, in "Journal of Complexity", August 2015, vol. 31, n° 4, pp. 590–616 [*DOI :* 10.1016/j.jco.2015.04.001], https://hal.inria.fr/hal-00846041

[4] J.-C. FAUGÈRE, A. OTMANI, L. PERRET, F. DE PORTZAMPARC, J.-P. TILLICH. *Folding Alternant and Goppa Codes with Non-Trivial Automorphism Groups*, in "IEEE Transactions on Information Theory", 2015, vol. 62, n° 1, pp. 184 - 198 [*DOI :* 10.1109/TIT.2015.2493539], https://hal.inria.fr/hal-01244609

[5] J.-C. FAUGÈRE, A. OTMANI, L. PERRET, F. DE PORTZAMPARC, J.-P. TILLICH. *Structural Cryptanalysis of McEliece Schemes with Compact Keys*, in "Designs, Codes and Cryptography", January 2015, 26 p. , https://hal.inria.fr/hal-00964265

[6] J.-C. FAUGÈRE, M. SAFEY EL DIN, T. VERRON. *On the complexity of computing Gröbner bases for weighted homogeneous systems*, in "Journal of Symbolic Computation", 2016 [*DOI :* 10.1016/j.jsc.2015.12.001], https://hal.inria.fr/hal-01097316

[7] D. HENRION, S. NALDI, M. SAFEY EL DIN. *Real root finding for determinants of linear matrices*, in "Journal of Symbolic Computation", May 2016, vol. 74, pp. 205-238 [*DOI :* 10.1016/j.jsc.2015.06.010], https://hal.archives-ouvertes.fr/hal-01077888

[8] V. Y. PAN, E. TSIGARIDAS. *Accelerated Approximation of the Complex Roots and Factors of a Univariate Polynomial*, in "Theoretical Computer Science", 2015, https://hal.inria.fr/hal-01105267

[9] V. Y. PAN, E. TSIGARIDAS. *Nearly optimal computations with structured matrices*, in "Theoretical Computer Science", 2015, https://hal.inria.fr/hal-01105263

[10] V. Y. PAN, E. TSIGARIDAS. *Nearly Optimal Refinement of Real Roots of a Univariate Polynomial*, in "Journal of Symbolic Computation", 2015, vol. 74, pp. 181–204 [*DOI :* 10.1016/J.JSC.2015.06.009], https://hal.inria.fr/hal-00960896

International Conferences with Proceedings

[11] I. BANNWARTH, M. SAFEY EL DIN. *Probabilistic Algorithm for Computing the Dimension of Real Algebraic Sets*, in "Proceedings of the 40th International Symposium on Symbolic and Algebraic Computation", Bath, United Kingdom, ACM, July 2015 [*DOI :* 10.1145/2755996.2756670], https://hal.archives-ouvertes.fr/hal-01152751

[12] J. BERTHOMIEU, B. BOYER, J.-C. FAUGÈRE. *Linear Algebra for Computing Gröbner Bases of Linear Recursive Multidimensional Sequences*, in "40th International Symposium on Symbolic and Algebraic Computation", Bath, United Kingdom, July 2015, pp. 61–68 [*DOI :* 10.1145/2755996.2756673], https://hal.inria.fr/hal-01237861

[13] B. BÉRARD, S. HADDAD, C. PICARONNY, M. SAFEY EL DIN, M. SASSOLAS. *Polynomial Interrupt Timed Automata*, in "The 9th Workshop on Reachability Problems (RP'15)", Warsaw, Poland, Lecture Notes in Computer Science, Springer, September 2015, vol. 9328, pp. 20-32 [*DOI :* 10.1007/978-3-319-24537-9_3], https://hal.archives-ouvertes.fr/hal-01222572

[14] M. CONDE PENA, J.-C. FAUGÈRE, L. PERRET. *Algebraic Cryptanalysis of a Quantum Money Scheme The Noise-Free Case*, in "IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC'15)", Maryland, United States, March 2015, https://hal.inria.fr/hal-01098223

[15] J.-S. CORON, J.-C. FAUGÈRE, G. RENAULT, R. ZEITOUN. *Factoring $N = p^r q^s$ for Large r and s*, in "RSA Conference Cryptographers' Track", San Francisco, United States, Topics in Cryptology – CT-RSA 2016, February 2016, https://hal.inria.fr/hal-01250302

[16] J.-C. FAUGÈRE, D. GLIGOROSKI, L. PERRET, S. SIMONA, E. THOMAE. *A Polynomial-Time Key-Recovery Attack on MQQ Cryptosystems*, in "IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC'15)", Maryland, United States, March 2015, https://hal.inria.fr/hal-01074194

[17] F. GUO, M. SAFEY EL DIN, W. CHU, L. ZHI. *Optimizing a Parametric Linear Function over a Non-compact Real Algebraic Variety*, in "The 2015 ACM on International Symposium on Symbolic and Algebraic Computation", Bath, United Kingdom, ACM, July 2015, pp. 205-212 [*DOI :* 10.1145/2755996.2756666], https://hal.inria.fr/hal-01237920

[18] D. HENRION, S. NALDI, M. SAFEY EL DIN. *Real root finding for rank defects in linear Hankel matrices*, in "International Symposium on Symbolic and Algebraic Computation (ISSAC)", Bath, United Kingdom, July 2015, pp. 221-228, https://hal.archives-ouvertes.fr/hal-01114378

[19] A. HERMAN, E. TSIGARIDAS. *Bounds for the Condition Number of Polynomials Systems with Integer Coefficients*, in "CASC", Aachen, Germany, V. P. GERDT, W. KOEPF, W. M. SEILER, E. V. VOROZHTSOV (editors), 2015, vol. 9301, pp. 210–219 [*DOI :* 10.1007/978-3-319-24021-3_16], https://hal.inria.fr/hal-01248389

[20] V. VITSE, A. WALLET. *Improved Sieving on Algebraic Curves*, in "LATINCRYPT 2015, 4th International Conference on Cryptology and Information Security in Latin America", Guadalajara, Mexico, K. LAUTER, F. RODRÍGUEZ-HENRÍQUEZ (editors), Lecture Notes in Computer Science, August 2015, vol. 9230, pp. 295-307 [*DOI :* 10.1007/978-3-319-22174-8_16], http://hal.upmc.fr/hal-01203086

Scientific Books (or Scientific Book chapters)

[21] M. SAFEY EL DIN. *Algorithmes efficaces en géométrie algébrique réelle*, in "Informatique Mathématique Une photographie en 2015", CNRS Editions, 2015, https://hal.inria.fr/hal-01237922

Other Publications

[22] J. BERTHOMIEU, B. BOYER, J.-C. FAUGÈRE. *Linear Algebra for Computing Gröbner Bases of Linear Recurrent Multidimensional Sequences*, December 2015, working paper or preprint, https://hal.inria.fr/hal-01253934

[23] I. EMIRIS, B. MOURRAIN, E. TSIGARIDAS. *Separation bounds for polynomial systems*, December 2015, working paper or preprint, https://hal.inria.fr/hal-01105276

[24] D. HENRION, S. NALDI, M. SAFEY EL DIN. *Exact algorithms for linear matrix inequalities*, August 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01184320

[25] D. HENRION, S. NALDI, M. SAFEY EL DIN. *Real root finding for low rank linear matrices*, June 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01159210

[26] D. LAZARD. *Mobile 4R and 5R loops*, March 2015, Soumis à Mechanism and Machine Theory, https://hal.inria.fr/hal-01130254

[27] V. Y. PAN, E. TSIGARIDAS, Z. LIANG. *Simple and Efficient Real Root-finding for a Univariate Polynomial*, January 2015, working paper or preprint, https://hal.inria.fr/hal-01105309

[28] A. STRZEBONSKI, E. TSIGARIDAS. *Univariate real root isolation in an extension field and applications*, 2015, working paper or preprint, https://hal.inria.fr/hal-01248390