IN PARTNERSHIP WITH:
CNRS

Université Pierre et Marie Curie (Paris 6)

Activity Report 2016

Project-Team POLSYS

Polynomial Systems

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

RESEARCH CENTER
Paris

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Project-Team POLSYS

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

Keywords:

Computer Science and Digital Science:

2.4. - Verification, 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
7.3. - Optimization
7.5. - Geometry, Topology
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 [Délégation Inria, Senior Researcher, Univ. Bourgogne, Professor, until Aug. 2016, HDR]
Elias Tsigaridas [Inria, Researcher]

Faculty Members

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

Engineer

Jérôme Govinden [SATT-LUTECH, until Mar. 2016]

PhD Students

Ivan Bannwarth [UPMC]
Matías Bender [Inria]
Ulrick Severin [Dassault Aviation, until Aug. 2016]
Thibaut Verron [UPMC, until Sep. 2016]
Alexandre Wallet [Inria, until Dec. 2016]

Visiting Scientist

Christian Eder [Technische Universität Kaiserslautern, Germany, regularly]

Administrative Assistants

Georgette Bonpapa [UPMC]
Laurence Bourcier [Inria]
Virginie Collette [Inria]
Irphane Khan [UPMC]
Nelly Maloisel [Inria]

Others

Daniel Lazard [UPMC, Professor, Émérite, HDR]
Emmanuel Prouff [ANSSI, Safran Identity and Security, Associate Member, HDR]
Dongming Wang [CNRS, Senior Researcher, Associate Member, HDR]
Sènan Dossa [ENS Lyon, Internship, from May 2016 until Sep. 2016]
Vincent Guisse [Min. de l'Éducation Nationale, Internship, from Apr. 2016 until Jul. 2016]
Ramon Ronzon [École polytechnique, Internship, from Mar. 2016 until Sep. 2016]

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.

3.3. Solving Systems over the Reals and Applications.

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

[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.

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 a variant of the Wiedemann algorithm. Hence, our goal is also to obtain a dedicated high performance library for transforming (i.e. change ordering) Gröbner bases.

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

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

Participants: Jean-Charles Faugère, Ludovic Perret, Guénaël Renault, 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*.

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.

[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.

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

The goal of the RISQ project is to prepare the security industry to the upcoming shift of classical cryptography to quantum-safe cryptography. The RISQ project is a massive effort at the French level to embrace the quantum-safe revolution. The project gather 15 partners : ANSSI, C&S, CEA, Crypto Experts, EADS, ENS Lyon, ENS Paris, Gemalto, Orange, PCQC, POLSYS (Inria de Paris), Université de Rennes, Secure IC, Thales CS, and Université de Versailles.

The RISQ project is certainly the biggest (in term of number of partners, as well as funding) industrial project ever organized in quantum-safe cryptography. RISQ is one of few projects accepted in the “Grands Défis du Numérique” which is managed by BPI France, and will be funded thanks to the PIA.

POLSYS actively participated to gather the partners of RISQ, and in defining the proposal. POLSYS will lead the academic effort in RISQ.

Jointly with LAAS (D. Henrion, S. Naldi), we have released a new MAPLE library SPECTRA for finding a real point $x = (x_1, ..., x_n)$ such that the symmetric matrix $A(x) = A_0 + A_1\, x_1 + \cdots + A_n\, x_n$ is positive semidefinite using exact arithmetic (see http://homepages.laas.fr/henrion/software/spectra/).

Our open source C library SLV has been officially released this year with a presentation at ISSAC. It aims at solating and approximating the real roots of univariate polynomials with integer coefficients (see http://www-polsys.lip6.fr/~elias/soft.html)

4.1.1. Awards

Matías Bender received the Distinguished Student Author Award of ISSAC2016 for his paper [22] written with J.-Ch. FAUGÈRE, L. PERRET and E. TSIGARIDAS.

BEST PAPER AWARD:

[22]
M. R. BENDER, J.-C. FAUGÈRE, L. PERRET, E. TSIGARIDAS. *A Superfast Randomized Algorithm to Decompose Binary Forms*, in "ISSAC ’16 - 41st International Symposium on Symbolic and Algebraic Computation", Waterloo, Canada, ACM, July 2016, pp. 79-86 [*DOI :* 10.1145/2930889.2930896], https://hal.inria.fr/hal-01363545

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

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

5.3. 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/Software/FGb/

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/Software/index.html

5.5. HFEBoost

FUNCTIONAL DESCRIPTION

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

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

5.6. RAGlib

Real Algebraic Geometry library
FUNCTIONAL DESCRIPTION

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

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

5.7. SLV

FUNCTIONAL DESCRIPTION

SLV is a software package in C that provides routines for isolating (and subsequently refine) the real roots of univariate polynomials with integer or rational coefficients based on subdivision algorithms and on the continued fraction expansion of real numbers. Special attention is given so that the package can handle polynomials that have degree several thousands and size of coefficients hundrends of Megabytes. Currently the code consists of $\sim 5\,000$ lines.

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

5.8. SPECTRA

Semidefinite Programming solved Exactly with Computational Tools of Real Algebra
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 Grobner bases and provides either certified numerical approximations of the solutions or exact representations of them.

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

6. New Results

6.1. Fundamental algorithms and structured polynomial systems

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

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

In the extended version [6], we investigate this problem and design several algorithms for computing such a Gröbner basis of an ideal of relations using linear algebra techniques. The first one performs a lot of table queries and is analogous to a change of variables on the ideal of relations.

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

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

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

6.1.2. Guessing Linear Recurrence Relations of Sequence Tuples and P-recursive Sequences with Linear Algebra

Given several n-dimensional sequences, we first present in [23] an algorithm for computing the Gröbner basis of their module of linear recurrence relations.

A P-recursive sequence $(u_{\mathbf{i}})_{\mathbf{i}\in\mathbb{N}^n}$ satisfies linear recurrence relations with polynomial coefficients in $\mathbf{i}$, as defined by Stanley in 1980. Calling directly the aforementioned algorithm on the tuple of sequences $\left((\mathbf{i}^{\mathbf{j}}\, u_{\mathbf{i}})_{\mathbf{i}\in\mathbb{N}^n}\right)_{\mathbf{j}}$ for retrieving the relations yields redundant relations. Since the module of relations of a P-recursive sequence also has an extra structure of a 0-dimensional right ideal of an Ore algebra, we design a more efficient algorithm that takes advantage of this extra structure for computing the relations.

Finally, we show how to incorporate Gröbner bases computations in an Ore algebra $\mathbb{K}\langle t_1, ..., t_n, x_1, ..., x_n\rangle$, with commutators $x_k\, x_\ell - x_\ell\, x_k = t_k\, t_\ell - t_\ell\, t_k = t_k\, x_\ell - x_\ell\, t_k = 0$ for $k \neq \ell$ and $t_k\, x_k - x_k\, t_k = x_k$, into the algorithm designed for P-recursive sequences. This allows us to compute faster the Gröbner basis of the ideal spanned by the first relations, such as in 2D/3D-space walks examples.

6.1.3. On the Connection Between Ritt Characteristic Sets and Buchberger-Gröbner Bases

For any polynomial ideal I, let the minimal triangular set contained in the reduced Buchberger–Gröbner basis of I with respect to the purely lexicographical term order be called the W-characteristic set of I. In [18], we establish a strong connection between Ritt's characteristic sets and Buchberger's Gröbner bases of polynomial ideals by showing that the W-characteristic set C of I is a Ritt characteristic set of I whenever C is an ascending set, and a Ritt characteristic set of I can always be computed from C with simple pseudo-division when C is regular. We also prove that under certain variable ordering, either the W-characteristic set of I is normal, or irregularity occurs for the jth, but not the $(j+1)$th, elimination ideal of I for some j. In the latter case, we provide explicit pseudo-divisibility relations, which lead to nontrivial factorizations of certain polynomials in the Buchberger–Gröbner basis and thus reveal the structure of such polynomials. The pseudo-divisibility relations may be used to devise an algorithm to decompose arbitrary polynomial sets into normal triangular sets based on Buchberger–Gröbner bases computation.

6.1.4. 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 $W = (w_1, \cdots, w_n)$, W-homogeneous polynomials are polynomials which are homogeneous w.r.t the weighted degree $\deg_W\left(X_1^{\alpha_1}, \cdots, X_n^{\alpha_n}\right) = \sum w_i\alpha_i$.

Gröbner bases for weighted homogeneous systems can be computed by adapting existing algorithms for homogeneous systems to the weighted homogeneous case. In [12], we show that in this case, the complexity estimate for Algorithm F5 $\left(\binom{n+d_{\max}-1}{d_{\max}}^{\omega}\right)$ can be divided by a factor $\left(\prod w_i\right)^{\omega}$. 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 $\left(\prod w_i\right)^{\omega}$. Under genericity assumptions, for zero-dimensional weighted homogeneous systems of W-degree $(d_1, \cdots, d_n)$, 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 F5 is bounded by the weighted Macaulay bound $\sum (d_i - w_i) + w_n$, 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.

6.1.5. A Superfast Randomized Algorithm to Decompose Binary Forms

Symmetric Tensor Decomposition is a major problem that arises in areas such as signal processing, statistics, data analysis and computational neuroscience. It is equivalent to a homogeneous polynomial in n variables of degree D as a sum of Dth powers of linear forms, using the minimal number of summands. This minimal number is called the rank of the polynomial/tensor. We consider the decomposition of binary forms, that corresponds to the decomposition of symmetric tensors of dimension 2 and order D. This problem has its roots in Invariant Theory, where the decompositions are known as canonical forms. As part of that theory, different algorithms were proposed for the binary forms. In recent years, those algorithms were extended for the general symmetric tensor decomposition problem. We present in [22] a new randomized algorithm that enhances the previous approaches with results from structured linear algebra and techniques from linear recurrent sequences. It achieves a softly linear arithmetic complexity bound. To the best of our knowledge, the previously known algorithms have quadratic complexity bounds.

6.1.6. On the Bit Complexity of Solving Bilinear Polynomial Systems

In [29] we bound the Boolean complexity of computing isolating hyperboxes for all complex roots of systems of bilinear polynomials. The resultant of such systems admits a family of determinantal Sylvester-type formulas, which we make explicit by means of homological complexes. The computation of the determinant of the resultant matrix is a bottleneck for the overall complexity. We exploit the quasi-Toeplitz structure to reduce the problem to efficient matrix-vector products, corresponding to multivariate polynomial multiplication. For zero-dimensional systems, we arrive at a primitive element and a rational univariate representation of the roots. The overall bit complexity of our probabilistic algorithm is $\widetilde{O}_B(n^4D^4 + n^2D^4\tau)$, where n is the number of variables, D equals the bilinear Bézout bound, and τ is the maximum coefficient bitsize. In addition, a careful infinitesimal symbolic perturbation of the system allows us to treat degenerate and positive dimensional systems, thus making our algorithms and complexity analysis applicable to the general case.

6.2. Solving Systems over the Reals and Applications

6.2.1. Exact algorithms for linear matrix inequalities

Let $A(x) = A_0 + x_1A_1 + ... + x_nA_n$ be a linear matrix, or pencil, generated by given symmetric matrices $A_0, A_1, ..., A_n$ of size m with rational entries. The set of real vectors x such that the pencil is positive semidefinite is a convex semi-algebraic set called spectrahedron, described by a linear matrix inequality (LMI). In [13], we design an exact algorithm that, up to genericity assumptions on the input matrices, computes an exact algebraic representation of at least one point in the spectrahedron, or decides that it is empty. The algorithm does not assume the existence of an interior point, and the computed point minimizes the rank of the pencil on the spectrahedron. The degree d of the algebraic representation of the point coincides experimentally with the algebraic degree of a generic semidefinite program associated to the pencil. We provide explicit bounds for the complexity of our algorithm, proving that the maximum number of arithmetic operations that are performed is essentially quadratic in a multilinear Bézout bound of d. When m (resp. n) is fixed, such a bound, and hence the complexity, is polynomial in n (resp. m). We conclude by providing results of experiments showing practical improvements with respect to state-of-the-art computer algebra algorithms.

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. In [14], we focus 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 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. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets

A roadmap for a semi-algebraic set S is a curve which has a non-empty and connected intersection with all connected components of S. Hence, this kind of object, introduced by Canny, can be used to answer connectivity queries (with applications, for instance, to motion planning) but has also become of central importance in effective real algebraic geometry, since it is used in higher-level algorithms. In [15], we provide a probabilistic algorithm which computes roadmaps for smooth and bounded real algebraic sets. Its output size and running time are polynomial in $(nD)^{n\log(d)}$, where D is the maximum of the degrees of the input polynomials, d is the dimension of the set under consideration and n is the number of variables. More precisely, the running time of the algorithm is essentially subquadratic in the output size. Even under our assumptions, it is the first roadmap algorithm with output size and running time polynomial in $(nD)^{n\log(d)}$.

6.2.4. Determinantal sets, singularities and application to optimal control in medical imagery

Control theory has recently been involved in the field of nuclear magnetic resonance imagery. The goal is to control the magnetic field optimally in order to improve the contrast between two biological matters on the pictures. Geometric optimal control leads us here to analyze mero-morphic vector fields depending upon physical parameters, and having their singularities defined by a determinantal variety. The involved matrix has polynomial entries with respect to both the state variables and the parameters. Taking into account the physical constraints of the problem, one needs to classify, with respect to the parameters, the number of real singularities lying in some prescribed semi-algebraic set. In [24], we develop a dedicated algorithm for real root classification of the singularities of the rank defects of a polynomial matrix, cut with a given semi-algebraic set. The algorithm works under some genericity assumptions which are easy to check. These assumptions are not so restrictive and are satisfied in the aforementioned application. As more general strategies for real root classification do, our algorithm needs to compute the critical loci of some maps, intersections with the boundary of the semi-algebraic domain, etc. In order to compute these objects, the determinantal structure is exploited through a stratification by the rank of the polynomial matrix. This speeds up the computations by a factor 100. Furthermore, our implementation is able to solve the application in medical imagery, which was out of reach of more general algorithms for real root classification. For instance, computational results show that the contrast problem where one of the matters is water is partitioned into three distinct classes.

6.2.5. Optimal Control of an Ensemble of Bloch Equations with Applications in MRI

The optimal control of an ensemble of Bloch equations describing the evolution of an ensemble of spins is the mathematical model used in Nuclear Resonance Imaging and the associated costs lead to consider Mayer optimal control problems. The Maximum Principle allows to parameterize the optimal control and the dynamics is analyzed in the framework of geometric optimal control. This leads to numerical implementations or suboptimal controls using averaging principle as presented in [25].

6.2.6. Critical Point Computations on Smooth Varieties: Degree and Complexity bounds

Let $V \subset \mathbb{C}^n$ be an equidimensional algebraic set and g be an n-variate polynomial with rational coefficients. Computing the critical points of the map that evaluates g at the points of V is a cornerstone of several algorithms in real algebraic geometry and optimization. Under the assumption that the critical locus is finite and that the projective closure of V is smooth, we provide in [31] sharp upper bounds on the degree of the critical locus which depend only on $\deg(g)$ and the degrees of the generic polar varieties associated to V. Hence, in some special cases where the degrees of the generic polar varieties do not reach the worst-case bounds, this implies that the number of critical points of the evaluation map of g is less than the currently known degree bounds. We show that, given a lifting fiber of V, a slight variant of an algorithm due to Bank,

Giusti, Heintz, Lecerf, Matera and Solernó computes these critical points in time which is quadratic in this bound up to logarithmic factors, linear in the complexity of evaluating the input system and polynomial in the number of variables and the maximum degree of the input polynomials.

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

6.3.1. Structural Cryptanalysis of McEliece Schemes with Compact Key.

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. We show in [11] 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 hardest 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. We mention that some parameters that have been proposed in the literature remain out of reach of the methods given here. weakness arising from Goppa codes with QM or QD symmetries. Indeed, the security of such schemes is 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

6.3.2. 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 in [10], 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 no symmetry anymore. This result is obtained thanks to an 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. Lastly, 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.

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

D. Boneh, G. Durfee, and N. Howgrave-Graham 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 [27], 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 equal to a product of k factors of prime powers $p_i^{r_i}$; 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.

6.3.4. *On the p-adic stability of the FGLM algorithm*

Nowadays, many strategies to solve polynomial systems use the computation of a Gröbner basis for the graded reverse lexicographical ordering, followed by a change of ordering algorithm to obtain a Gröbner basis for the lexicographical ordering. The change of ordering algorithm is crucial for these strategies. In [33], we study the p-adic stability of the main change of ordering algorithm, FGLM. We show that FGLM is stable and give explicit upper bound on the loss of precision occuring in its execution. The variant of FGLM designed to pass from the grevlex ordering to a Gröbner basis in shape position is also stable. Our study relies on the application of Smith Normal Form computations for linear algebra.

6.3.5. *Binary Permutation Polynomial Inversion and Application to Obfuscation Techniques*

Whether it is for constant obfusation, opaque predicate or equation obfuscation, Mixed Boolean-Arithmetic (MBA) expressions are a powerful tool providing concrete ways to achieve obfuscation. Recent results introduced ways to mix such a tool with permutation polynomials modulo 2^n in order to make the obfuscation technique more resilient to SMT solvers. However, because of limitations regarding the inversion of such permutations, the set of permutation polynomials presented suffers some restrictions. Those restrictions allow several methods of arithmetic simplification, decreasing the effectiveness of the technique at hiding information. In [19], we present general methods for permutation polynomials inversion. These methods allow us to remove some of the restrictions presented in the literature, making simplification attacks less effective. We discuss complexity and limits of these methods, and conclude that not only current simplification attacks may not be as effective as we thought, but they are still many uses of polynomial permutations in obfuscation that are yet to be explored.

6.3.6. *Horizontal Side-Channel Attacks and Countermeasures on the ISW Masking Scheme*

A common countermeasure against side-channel attacks consists in using the masking scheme originally introduced by Ishai, Sahai and Wagner (ISW) at Crypto 2003, and further generalized by Rivain and Prouff at CHES 2010. The countermeasure is provably secure in the probing model, and it was showed by Duc, Dziembowski and Faust at Eurocrypt 2014 that the proof can be extended to the more realistic noisy leakage model. However the extension only applies if the leakage noise increases at least linearly with the masking order n, which is not necessarily possible in practice. In [20], we investigate the security of an implementation when the previous condition is not satisfied, for example when the masking order n increases for a constant noise. We exhibit two (template) horizontal side-channel attacks against the Rivain-Prouff's secure multiplication scheme and we analyze their efficiency thanks to several simulations and experiments. Eventually, we describe a variant of Rivain-Prouff's multiplication that is still provably secure in the original ISW model, and also heuristically secure against our new attacks.

6.3.7. *Faster Evaluation of SBoxes via Common Shares*

In [28], we describe a new technique for improving the efficiency of the masking countermeasure against side-channel attacks. Our technique is based on using common shares between secret variables, in order to reduce the number of finite field multiplications. Our algorithms are proven secure in the ISW probing model with $n > t + 1$ shares against t probes. For AES, we get an equivalent of 2.8 non-linear multiplications for every SBox evaluation, instead of 4 in the Rivain-Prouff countermeasure. We obtain similar improvements for other block-ciphers. Our technique is easy to implement and performs relatively well in practice, with roughly a 20% speed-up compared to existing algorithms.

6.3.8. Information Extraction in the Presence of Masking with Kernel Discriminant Analysis

To reduce the memory and timing complexity of the Side-Channel Attacks (SCA), dimensionality reduction techniques are usually applied to the measurements. They aim to detect the so-called Points of Interest (PoIs), which are time samples which (jointly) depend on some sensitive information (e.g. secret key sub-parts), and exploit them to extract information. The extraction is done through the use of functions which combine the measurement time samples. Examples of combining functions are the linear combinations provided by the Principal Component Analysis or the Linear Discriminant Analysis. When a masking countermeasure is properly implemented to thwart SCAs, the selection of PoIs is known to be a hard task: almost all existing methods have a combinatorial complexity explosion, since they require an exhaustive search among all possible d-tuples of points. In this paper we propose an efficient method for informative feature extraction in presence of masking countermeasure. This method, called Kernel Discriminant Analysis, consists in completing the Linear Discriminant Analysis with a so-called kernel trick, in order to efficiently perform it over the set of all possible d-tuples of points without growing in complexity with d. We identify and analyse the issues related to the application of such a method. Afterwards, its performances are compared to those of the Projection Pursuit (PP) tool for PoI selection up to a 4th-order context. Experiments show that the Kernel Discriminant Analysis remains effective and efficient for high-order attacks, leading to a valuable alternative to the PP in constrained contexts where the increase of the order d does not imply a growth of the profiling datasets.

6.3.9. Polynomial Evaluation and Side Channel Analysis

Side Channel Analysis (SCA) is a class of attacks that exploits leakage of information from a cryptographic implementation during execution. To thwart it, masking is a common countermeasure. The principle is to randomly split every sensitive intermediate variable occurring in the computation into several shares and the number of shares, called the masking order, plays the role of a security parameter. The main issue while applying masking to protect a block cipher implementation is to specify an efficient scheme to secure the S-box computations. Several masking schemes, applicable for arbitrary orders, have been recently introduced. Most of them follow a similar approach originally introduced in the paper of Carlet et al published at FSE 2012; the S-box to protect is viewed as a polynomial and strategies are investigated which minimize the number of field multiplications which are not squarings. The paper [32] aims at presenting all these works in a comprehensive way. The methods are discussed, their differences and similarities are identified and the remaining open problems are listed.

6.3.10. Redefining the Transparency Order

In [7], we consider the multi-bit Differential Power Analysis (DPA) in the Hamming weight model. In this regard, we revisit the definition of Transparency Order (TO) from the work of Prouff (FSE 2005) and find that the definition has certain limitations. Although this work has been quite well referred in the literature, surprisingly, these limitations remained unexplored for almost a decade. We analyse the definition from scratch, modify it and finally provide a definition with better insight that can theoretically capture DPA in Hamming weight model for hardware implementation with precharge logic. At the end, we confront the notion of (revised) transparency order with attack simulations in order to study to what extent the low transparency order of an s-box impacts the efficiency of a side channel attack against its processing.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Grants with Industry

Until the mid 2000's, multivariate cryptography was developing very rapidly, producing many interesting and versatile public-key schemes. However, many of them were soon successfully cryptanalysed (a lot have been done in this group). As a consequence, the confidence in multivariate cryptography cryptosystems declined. It seems that there have emerged new important reasons for renewal of the interest in a new generation

of multivariate schemes. In the past two years, the algorithms for solving the Discrete Logarithm Problem over small characteristic fields underwent an extraordinary development. This clearly illustrates the risk to not consider alternatives to classical assumptions based on number theory. In parallel, two of the most important standardization bodies in the world, NIST and ETSI have recently started initiatives for developing cryptographic standards not based on number theory, with a particular focus on primitives resistant to quantum algorithms. An objective here is then to focus on the design of multivariate schemes.

The team is 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 Ministry of Defense. The experiment gathered a total of hundred participants from various operational units. This is a first milestone in the maturation project whose goal is to create a start-up.

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).
- **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).

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: COST

Project acronym: CryptoAction

Project title: Cryptography for Secure Digital Interaction

Duration: 04 2014 - 04 2018

Coordinator: Claudio ORLANDI

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

Program: COST

Project acronym: CRYPTACUS

Project title: Cryptanalysis of ubiquitous computing systems

Duration: 12 2014 - 12 2018

Coordinator: Gildas AVOINE

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

8.3. International Initiatives

8.3.1. Inria International Labs

8.3.1.1. GOAL

Title: Geometry and Optimization with ALgebraic methods.

International Partner (Institution - Laboratory - Researcher):

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

Start year: 2015

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

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

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

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

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Carlos Améndola Cerón

Date: May 2016

Institution: Technische Universität Berlin, Germany

Christoph Koutschan

Date: Nov. 2016

Institution: Österreichische Akademie der Wissenschaften, Linz

Didier Henrion

Date: Nov. 2016

Institution: LAAS, CNRS

Simone Naldi

Date: Nov. 2016

Institution: TU Univ. Dortmund, Germany.

Ioannis Psarros

Date: May. 2016

Institution: University of Athens, Greece.

8.4.1.1. Internships

Vincent Guisse

Date: Apr. 2016 - Jul. 2016

Institution: Université Paris – Diderot

Supervisor: Jean-Charles Faugère, Jérémy Berthomieu

Ramon Ronzon

Date: Mar. 2016 - Sep. 2016

Institution: École polytechnique

Supervisor: Jean-Charles Faugère, Ludovic Perret

Sènan Dossa

Date: Mar. 2016 - Sep. 2016

Institution: ENS Lyon

Supervisor: Jean-Charles Faugère, Ludovic Perret

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Member of the organizing committees

Dongming Wang was involved in the organization of the following conferences

- Special Session on Software of Polynomial Systems at the 5th International Congress on Mathematical Software (ICMS 2016) (Berlin, Germany, July 11-14, 2016).

9.1.2. Scientific events selection

9.1.2.1. Member of the conference program committees

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

- Conference on Cryptographic Hardware and Embedded Systems 2016 (CHES 2016) (Santa Barbara, CA, USA, Aug. 17-19, 2016);
- Smart Card Research and Advanced Application Conference (CARDIS 2016) (Cannes, France, Nov. 7-9, 2016);
- International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2016) (Graz, Austria, Apr. 14-15);
- 23rd ACM Conference on Computer and Communications Security (ACM CCS 2016) (Vienna, Austria, Oct. 24-28).

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

- 11th International Workshop on Automated Deduction in Geometry (ADG 2016) (Strasbourg, France, June 27-29, 2016);
- 7th International Symposium on Symbolic Computation in Software Science (SCSS 2016) (Tokyo, Japan, March 28-31, 2016).

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

- Computer Algebra in Scientific Computing (CASC 2016), Sept 2016 Bucharest, Romania.

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.

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

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

Emmanuel Prouff was invited speaker at

- EUROCRYPT 2016 (invited tutorial), Vienna, Austria, on Securing Cryptography Implementations in Embedded Systems.
- SPACE 2016 (invited speaker), Hyderabad, India on Breaking Cryptographic Implementations Using Deep Learning Techniques.

Mohab Safey El Din was invited speaker at

- the SMAI-MODE session on semi-algebraic optimization, Toulouse, March 2016, France.
- the AIM Workshop on Algebraic Vision which was held at the American Institute of Mathematics, San Jose, May 2016, USA.
- the NCSU seminar on Symbolic Computation, Raleigh, May 2016, USA.
- the PGMO session on Semi-Definite Programming, Palaiseau, October 2016, France.

Ludovic Perret was invited speaker at 17th World Conference on Information Security Applications (WISA 2016, August, Korea).

Elias Tsigaridas was invited speaker at

- the Department Seminar Series, of the Computer Science Department of the University of Liverpool, Apr 2016, UK.
- the Seminar of RICAM, University of Linz, Austria (Dec. 2016)

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, 34 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

Master : Projects supervision, 8 hours, L2, Université Pierre-et-Marie-Curie, France

Licence : Introduction to Algorithmics, 49 hours, L3, Université Pierre-et-Marie-Curie, France

Licence : Representations and Numerical Methods, 41 hours, L2, Université Pierre-et-Marie-Curie, France

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

Jean-Charles Faugère had the following teaching activities:

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

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

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, 36 hours, M1, Université Pierre-et-Marie-Curie, France

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

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

Master : In charge of the Security, Reliability and Numerical Efficiency Program in Master, 12 hours, M1 and M2, Université Pierre-et-Marie-Curie, France

Master : Introduction to Security, 10 hours, M1, Université Pierre-et-Marie-Curie, 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

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 in progress : Clayton Eduardo Lente da Silva, Planar discontinuous dynamical system, Universidade Estadual Paulista (São José do Rio Preto), started in Sep. 2013, Paulo Ricardo da Silva and Alain Jacquemard

HdR : Ludovic Perret, Université Pierre-et-Marie-Curie, defended in Dec. 2016

HdR : Guénaël Renault, Université Pierre-et-Marie-Curie, defended in Dec. 2016

PhD : Thársis Souza Silva, Relay Systems, Universidade Federal de Goiás, Goiânia, defended in May 2016, Ronaldo Alves Garcia and Alain Jacquemard

PhD : Adrian Thillard, Countermeasures to Side-Channel Attacks and Secure- Multi-Party Computation, ENS Paris, defended in Dec. 2016 Damien Vergnaud and Emmanuel Prouff

PhD : Thibaut Verron, Gröbner bases and structured polynomial systems, Université Pierre-et-Marie-Curie, defended in Sept. 2016, Jean-Charles Faugère and Mohab Safey El Din

PhD : Alexandre Wallet, The point decomposition problem in Jacobian varieties, Université Pierre-et-Marie-Curie, defended in Dec. 2016, Jean-Charles Faugère

9.2.3. Juries

Jean-Charles Faugère was examiner in the PhD committees of C. Chenavier, V. Neiger, T. Verron and A. Wallet and in the HDR committees of L. Perret and G. Renault.

Alain Jacquemard was examiner in the PhD committee of T.S. Silva.

Emmanuel Prouff was reviewer of the PhD theses of A. Battistello and D. Martin. He was examiner in the PhD committee of A. Battistello, D. Martin and A. Thillard and in the HDR committees of G. Renault.

Mohab Safey El Din was examiner in the PhD committees of T. Verron and A. Wallet and in the HDR committees of L. Perret and G. Renault.

9.3. Popularization

J.-C. Faugère and L. Perret wrote a paper “Le grand défi du post-quantique” for MISC (HS 13, April 2016).

10. Bibliography

Major publications by the team in recent years

[1] M. R. BENDER, J.-C. FAUGÈRE, L. PERRET, E. TSIGARIDAS. *A Superfast Randomized Algorithm to Decompose Binary Forms*, in "ISSAC '16 - 41st International Symposium on Symbolic and Algebraic Computation", Waterloo, Canada, ACM, July 2016, pp. 79-86 [*DOI :* 10.1145/2930889.2930896], https://hal.inria.fr/hal-01363545

Publications of the year

Doctoral Dissertations and Habilitation Theses

[2] L. PERRET. *Gröbner bases techniques in Quantum-Safe Cryptography*, UPMC - Paris 6 Sorbonne Universités, December 2016, Habilitation à diriger des recherches, https://tel.archives-ouvertes.fr/tel-01417808

[3] G. RENAULT. *Contribution à la Résolution Algébrique et Applications en Cryptologie*, UPMC - Paris 6 Sorbonne Universités, December 2016, Habilitation à diriger des recherches, https://hal.inria.fr/tel-01416242

[4] T. VERRON. *Regularisation of Gröbner basis computations for weighted and determinantal systems, and an application to medical imagery*, Université Pierre et Marie Curie, September 2016, https://tel.archives-ouvertes.fr/tel-01404406

[5] A. WALLET. *The point decomposition problem in Jacobian varieties* , Université Pierre & Marie Curie - Paris 6, November 2016, https://tel.archives-ouvertes.fr/tel-01407675

Articles in International Peer-Reviewed Journals

[6] J. BERTHOMIEU, B. BOYER, J.-C. FAUGÈRE. *Linear Algebra for Computing Gröbner Bases of Linear Recursive Multidimensional Sequences*, in "Journal of Symbolic Computation", 2016, 48 p. [*DOI :* 10.1016/J.JSC.2016.11.005], https://hal.inria.fr/hal-01253934

[7] K. CHAKRABORTY, S. SARKAR, S. MAITRA, B. MAZUMDAR, D. MUKHOPADHYAY, E. PROUFF. *Redefining the transparency order*, in "Designs, Codes and Cryptography", 2016 [*DOI :* 10.1007/s10623-016-0250-3], https://hal.archives-ouvertes.fr/hal-01399584

[8] C. EDER, J.-C. FAUGÈRE. *A survey on signature-based algorithms for computing Gröbner basis computations*, in "Journal of Symbolic Computation", 2016, pp. 1-75 [*DOI :* 10.1016/J.JSC.2016.07.031], https://hal.inria.fr/hal-00974810

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

[10] 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", 2016, vol. 62, n° 1, pp. 184 - 198 [*DOI :* 10.1109/TIT.2015.2493539], https://hal.inria.fr/hal-01244609

[11] 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", April 2016, vol. 79, n° 1, pp. 87-112 [*DOI :* 10.1007/s10623-015-0036-z], https://hal.inria.fr/hal-00964265

[12] 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

[13] D. HENRION, S. NALDI, M. SAFEY EL DIN. *Exact algorithms for linear matrix inequalities*, in "SIAM Journal on Optimization", September 2016, vol. 26, n° 4, pp. 2512–2539 [*DOI :* 10.1137/15M1036543], https://hal.archives-ouvertes.fr/hal-01184320

[14] 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

[15] M. SAFEY EL DIN, E. SCHOST. *A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets*, in "Journal of the ACM", 2016, Major revision, accepted for publication to Journal of the ACM, https://hal.inria.fr/hal-00849057

[16] A. STRZEBONSKI, E. TSIGARIDAS. *Univariate real root isolation over a single logarithmic extension of real algebraic numbers*, in "Springer Proceedings in Mathematics & Statistics", 2017, Ilias S. Kotsireas and Edgar Martí´nez-Moro, https://hal.inria.fr/hal-01001820

[17] E. TSIGARIDAS. *SLV: a software for real root isolation*, in "ACM Communications in Computer Algebra", November 2016, vol. 50, n° 3, pp. 117 - 120 [*DOI :* 10.1145/3015306.3015317], https://hal.inria.fr/hal-01422209

[18] D. WANG. *On the Connection Between Ritt Characteristic Sets and Buchberger–Gröbner Bases*, in "Mathematics in Computer Science", 2016, vol. 10, n° 4, pp. 479–492 [*DOI :* 10.1007/s11786-016-0279-8], https://hal.inria.fr/hal-01399579

International Conferences with Proceedings

[19] L. BARTHELEMY, N. EYROLLES, G. RENAULT, R. ROBLIN. *Binary Permutation Polynomial Inversion and Application to Obfuscation Techniques*, in "2nd International Workshop on Software PROtection", Vienna, Austria, ACM, October 2016 [*DOI :* 10.1145/2995306.2995310], https://hal.inria.fr/hal-01388108

[20] A. BATTISTELLO, J.-S. CORON, E. PROUFF, R. ZEITOUN. *Horizontal Side-Channel Attacks and Countermeasures on the ISW Masking Scheme*, in "18th Conference on Cryptographic Hardware and Embedded Systems (CHES 2016)", Santa Barbara, CA, United States, Cryptographic Hardware and Embedded Systems – CHES 2016, Springer, August 2016, vol. 9813, pp. 23 - 39 [*DOI :* 10.1007/978-3-662-53140-2_2], https://hal.archives-ouvertes.fr/hal-01399577

[21] S. BELAID, F. BENHAMOUDA, A. PASSELÈGUE, E. PROUFF, A. THILLARD, D. VERGNAUD. *Randomness Complexity of Private Circuits for Multiplication*, in "EUROCRYPT 2016", Vienna, Austria, May 2016, pp. 616-648 [*DOI :* 10.1007/978-3-662-49896-5_22], https://hal.archives-ouvertes.fr/hal-01324823

[22] *Best Paper*
M. R. BENDER, J.-C. FAUGÈRE, L. PERRET, E. TSIGARIDAS. *A Superfast Randomized Algorithm to Decompose Binary Forms*, in "ISSAC '16 - 41st International Symposium on Symbolic and Algebraic Computation", Waterloo, Canada, ACM, July 2016, pp. 79-86 [*DOI :* 10.1145/2930889.2930896], https://hal.inria.fr/hal-01363545.

[23] J. BERTHOMIEU, J.-C. FAUGÈRE. *Guessing Linear Recurrence Relations of Sequence Tuples and P-recursive Sequences with Linear Algebra*, in "41st International Symposium on Symbolic and Algebraic Computation", Waterloo, ON, Canada, July 2016, pp. 95-102 [*DOI :* 10.1145/2930889.2930926], https://hal.inria.fr/hal-01314266

[24] B. BONNARD, J.-C. FAUGÈRE, A. JACQUEMARD, M. SAFEY EL DIN, T. VERRON. *Determinantal sets, singularities and application to optimal control in medical imagery*, in "International symposium on symbolic and algebraic computations", Waterloo, Canada, ACM, July 2016, pp. 103-110 [*DOI :* 10.1145/2930889.2930916], https://hal.inria.fr/hal-01307073

[25] B. BONNARD, A. JACQUEMARD, J. ROUOT. *Optimal Control of an Ensemble of Bloch Equations with Applications in MRI*, in "55th IEEE Conference on Decision and Control - CDC", Las Vegas, United States, December 2016, https://hal.inria.fr/hal-01287290

[26] B. BOYER, C. EDER, J.-C. FAUGÈRE, S. LACHARTRE, F. MARTANI. *GBLA – Gröbner Basis Linear Algebra Package*, in "41st International Symposium on Symbolic and Algebraic Computation", Waterloo, ON, Canada, July 2016, pp. 135-142 [*DOI :* 10.1145/2930889.2930914], https://hal.inria.fr/hal-01276346

[27] 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 [*DOI :* 10.1007/978-3-319-29485-8_26], https://hal.inria.fr/hal-01250302

[28] J.-S. CORON, A. GREUET, E. PROUFF, R. ZEITOUN. *Faster Evaluation of SBoxes via Common Shares*, in "18th International Conference on Cryptographic Hardware and Embedded Systems (CHES 2016)", Santa Barbara, CA, United States, Cryptographic Hardware and Embedded Systems – CHES 2016, Springer, August 2016, vol. 9813, pp. 498 - 514 [*DOI :* 10.1007/978-3-662-53140-2_24], https://hal.archives-ouvertes.fr/hal-01399578

[29] I. Z. EMIRIS, A. MANTZAFLARIS, E. TSIGARIDAS. *On the Bit Complexity of Solving Bilinear Polynomial Systems*, in "ISSAC '16 - 41st International Symposium on Symbolic and Algebraic Computation", Waterloo, Canada, ACM, July 2016, pp. 215-222 [*DOI :* 10.1145/2930889.2930919], https://hal.inria.fr/hal-01401134

[30] J.-C. FAUGÈRE, P.-J. SPAENLEHAUER, J. SVARTZ. *Computing Small Certificates of Inconsistency of Quadratic Fewnomial Systems*, in "International Symposium on Symbolic and Algebraic Computation (ISSAC 2016)", Waterloo, Canada, ACM, July 2016, pp. 223-230 [*DOI :* 10.1145/2930889.2930927], https://hal.inria.fr/hal-01314651

[31] M. SAFEY EL DIN, P.-J. SPAENLEHAUER. *Critical Point Computations on Smooth Varieties: Degree and Complexity bounds*, in "International Symposium on Symbolic and Algebraic Computation (ISSAC)", Waterloo, Canada, July 2016, pp. 183–190 [*DOI :* 10.1145/2930889.2930929], https://hal.inria.fr/hal-01312750

Scientific Books (or Scientific Book chapters)

[32] C. CARLET, E. PROUFF. *Polynomial Evaluation and Side Channel Analysis*, in "The New Codebreakers", Lecture Notes in Computer Science, Springer, 2016, vol. 9100, pp. 315 - 341 [*DOI :* 10.1007/978-3-662-49301-4_20], https://hal.archives-ouvertes.fr/hal-01399573

Other Publications

[33] G. RENAULT, T. VACCON. *On the p-adic stability of the FGLM algorithm*, 2016, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01266071

[34] M. SAFEY EL DIN, E. SCHOST. *Bit complexity for multi-homogeneous polynomial system solving Application to polynomial minimization*, May 2016, working paper or preprint, https://hal.inria.fr/hal-01319729