Activity Report 2018

Team OURAGAN

OUtils de Résolution Algébriques pour la Géométrie et ses ApplicatioNs

Inria teams are typically groups of researchers working on the definition of a common project, and objectives, with the goal to arrive at the creation of a project-team. Such project-teams may include other partners (universities or research institutions).

RESEARCH CENTER
Paris

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Team OURAGAN

Creation of the Team: 2012 January 01

Keywords:

Computer Science and Digital Science:

A4.3. - Cryptography
A4.3.1. - Public key cryptography
A4.3.2. - Secret key cryptography
A4.3.3. - Cryptographic protocols
A4.3.4. - Quantum Cryptography
A7.1. - Algorithms
A7.1.4. - Quantum algorithms
A8.1. - Discrete mathematics, combinatorics
A8.3. - Geometry, Topology
A8.4. - Computer Algebra
A8.5. - Number theory
A8.10. - Computer arithmetic

Other Research Topics and Application Domains:

B5.6. - Robotic systems
B9.5.1. - Computer science
B9.5.2. - Mathematics

1. Team, Visitors, External Collaborators

Research Scientists

Fabrice Rouillier [Team leader, Inria, Senior Researcher, HDR]
Razvan Barbulescu [CNRS, Researcher]

Faculty Members

Elisha Falbel [Sorbonne Université, Professor, HDR]
Antonin Guilloux [Sorbonne Université, Associate Professor, HDR]
Antoine Joux [Sorbonne Université, Professor, HDR]
Pierre-Vincent Koseleff [Sorbonne Université, Associate Professor, HDR]

Post-Doctoral Fellows

Anand Kumar Naranayan [Sorbonne Université]
Irene Pasquinelli [Sorbonne Université]

PhD Students

Thomas Espitau [Sorbonne Université]
Mahya Mehrabdollahei [Inria, from Oct 2018]
Natalia Kharchenko [Sorbonne Université]
Sudarshan Shinde [Sorbonne Université]
Robin Timsit [Sorbonne Université]

Administrative Assistant

Laurence Bourcier [Inria]

2. Overall Objectives

2.1. Overall Objectives

OURAGAN proposes to focus on the transfer of computational algebraic methods to some related fields (computational geometry, topology, number theory, etc.) and some carefully chosen application domains (robotics, control theory, evaluation of the security of cryptographic systems, etc.), which implies working equally on the use (modeling, know - how) and on the development of new algorithms. The latest breakthrough developments and applications where algebraic methods are currently decisive remain few and very targeted. We wish to contribute to increase the impact of these methods but also the number of domains where the use of computational algebraic methods represent a significant added value. This transfer-oriented positioning does not imply to stop working on the algorithms, it simply sets the priorities.

An original aspect of the OURAGAN proposal is to blend into an environment of fundamental mathematics, at the Institut de Mathématiques de Jussieu – Paris Rive Gauche (IMJ-PRG CNRS 7586), and to be cross-functional to several teams (Algebraic Analysis, Complex Analysis and Geometry, Number Theory to name only the main ones), which will be our first source of transfer of computational know-how. The success of this coupling allows to maintain a strong theoretical basis and to measure objectively our transfer activity in the direction of mathematicians (in geometry, topology, number theory, etc.) and to consolidate the presence of Inria in scientific areas among the most theoretical.

We propose two general directions with four particular targets:

- Number Theory
  - Algorithmic Number Theory
- Topology in small dimension
  - Character varieties
  - Knot theory
  - Computational geometry

These actions come, of course, in addition to the study and development of a common set of core elements of

- Basic theory and algorithms in algebra and geometry [Led by Antoine Joux and Fabrice Rouillier].

This core activity is the invention and study of fundamental algebraic algorithms and objects that can be grouped into 2 categories: algorithms designed to operate on finite fields and algorithms running on fields of characteristic 0; with 2 types of computational strategies: the exactness and the use of approximate arithmetic (but with exact results). This mix also installs joint studies between the various axes and is an originality of the project-team. For example many kinds of arithmetic tools around algebraic numbers have to face to similar theoretical problems such as finding a good representation for a number field; almost all problems related to the resolution of algebraic systems will reduce to the study of varieties in small dimension and in particular, most of the time, to the effective computation of the topology of curves and surfaces, or the certified drawing of non algebraic function over an algebraic variety.

The tools and objects developed for research on algorithmic number theory as well as in computational geometry apply quite directly on some selected connected challenging subjects:

- Security of cryptographic systems
- Control theory
- Robotics

These applications will serve for the evaluation of the general tools we develop when used in a different context, in particular their capability to tackle state of the art problems.

2.2. Scientific ground

2.2.1. Basic computable objects and algorithms

The basic computable objects and algorithms we study, use, optimize or develop are among the most classical ones in computer algebra and are studied by many people around the world: they mainly focus on basic computer arithmetic, linear algebra, lattices and polynomial system solving.

Our approach for tackling these basic problems, whose solution is important for the work of the whole team, is three-fold. First, for some selected problems, we do propose and develop general algorithms (isolation of real roots of univariate polynomials, parametrizations of solutions of zero-dimensional polynomial systems, solutions of parametric equations, etc.). Second, for a selection of well-known problems, we propose different computational strategies (for example the use of approximate arithmetic to speed up LLL algorithm or root isolators, still certifying the final result). Last, we propose specialized variants of known algorithms optimized for a given problem (for example, dedicated solvers for degenerated bivariate polynomials to be used in the computation of the topology of plane curves).

In the context of OURAGAN, it is important to avoid reinventing the wheel and to re-use wherever possible existing objects and algorithms. The main effort being focused on finding good formulations/modelizations for an efficient use. However, on demand, we will propose implementations at many different levels. For example, for our ongoing work on hybrid strategies for LLL, mixing interval arithmetics and basic linear algebra operations, we have replaced our general reliable multiprecision interval artihmetic package (MPFI [1]) by a dedicated one and managed to save an important factor.

In the activity of OURAGAN, many key objects or algorithms around the resolution of algebraic systems are developed within the team, such as the resolution of polynomials in one variable with real coefficients [77], [66], rational parameterizations of solutions of zero-dimensional systems with rational coefficients [76], [34] or discriminant varieties for solving systems depending on parameters [73].

For our studies in number theory and applications to the security of cryptographic systems, our team works on three categories of basic algorithms: discrete logarithm computations [64] (for example to make progress on the computation of class groups in number fields [56]), network reductions by means of LLL variants [45] and obviously various computations in linear algebra, for example dedicated to *almost sparse* matrices [65].

These two directions of development are linked at several levels. For example, working with number fields, in particular finding good representations of number fields, lead to the same computational problems as working with roots of polynomial systems by means of triangular systems (towers of number fields) or rational parameterizations (unique number field). Making any progress in one direction will probably have direct consequences for almost all the problems we want to tackle.

Several strategies are also shared between these directions such as the use of approximate arithmetic to speed up certified computations. Sometimes these can also lead to improvement for a different purpose (for example computations over the rationals, deeply used in geometry can often be parallelized combining computations in finite fields together with fast Chinese remaindering and modular evaluations).

As single highlighted example of this sharing of tools and strategies, the use of approximate arithmetic [75] is common to the work on LLL [45] (use in the evaluation of the security of cryptographic systems), resolutions of real-world algebraic systems [66] (used in our applications in robotics and control theory), computations of signs of trigonometric expressions used in knot theory [12] or to certified evaluations of dilogarithm functions on an algebraic variety for the computation of volumes of representations in our work in topology [52].

2.2.2. Algorithmic Number Theory

The frontiers between computable objects, algorithms (above section), computational number theory and applications to security of cryptographic systems are very porous. This union of research fields is mainly driven by the algorithmic improvement to solve presumably hard problems relevant to cryptography, such as computation of discrete logarithms, resolution of hard subset-sum problems, decoding of random binary codes

[1] https://gforge.inria.fr/projects/mpfi/

and search for close and short vectors in lattices. While factorization and discrete logarithm problems have a long history in cryptography, the recent post-quantum cryptosystems introduce a new variety of presumably hard problems/objects/algorithms with cryptographic relevance: the shortest vector problem (SVP), the closest vector problem (CVP) or the computation of isogenies between elliptic curves, especially in the supersingular case.

Solving the discrete logarithm problem in finite fields is a key question for the security of Diffie-Hellman based crypto and was the focus of a lot of academic research over the past 40 years. It is one of the expertise domain in the OURAGAN team.

Members of OURAGAN started working on the topic of discrete logarithms around 1998, with several computation records that were announced on the NMBRTHRY mailing list. In large characteristic, especially for the case of prime fields, the best current method is the number field sieve (NFS) algorithm. In particular, they published the first NFS based record computation [63]. Despite huge practical improvements, the prime field case algorithm hasn't really changed since that first record. Around the same time, we also presented small characteristic computation record based on simplifications of the Function Field Sieve (FFS) algorithm [62].

In 2006, important changes occurred concerning the FFS and NFS algorithms, indeed, while the algorithms only covered the extreme case of constant characteristic and constant extension degree, two papers extended their ranges of applicability to all finite fields. At the same time, this permitted a big simplification of the FFS, removing the need for function fields.

Starting from 2012, new results appeared in small characteristic. Initially based on a simplification of the 2006 result, they quickly blossomed into the Frobenial representation methods, with quasi-polynomial time complexity [28], [64], [57]. Recent progress were also made in larger characteristic [30], [29], [27], [26].

An interesting side-effect of this research was the need to revisit the key sizes of pairing-based cryptography. This type of cryptography is also a topic of interest for OURAGAN. In particular, it was introduced in 2000 [61]. Recent re-evaluation of the necessary key size [26], making use of the overview of the possible discrete logarithm constructions are discussed [25].

The computations of *class groups in number fields* has strong links with the computations of discrete logarithms or factorizations using the NFS (number field sieve) strategy which as the name suggests is based on the use of number fields. Roughly speaking, the NFS algorithm uses two number fields and the strategy consists in choosing number fields with small sized coefficients in their definition polynomials. On the contrary, in class group computations, there is a single number field, which is clearly a simplification, but this field is given as input by some fixed definition polynomial. Obviously, the degree of this polynomial as well as the size of its coefficients are both influencing the complexity of the computations so that finding other polynomials representing the same class group but with a better characterization (degree or coefficient's sizes) is a mathematical problem with direct practical consequences. We proposed a method to address the problem in [56], but many issues remain open.

Computing generators of principal ideals of cyclotomic fields is also strongly related to the computation of class groups in number fields. Ideals in cyclotomic fields are used in a number of recent public-key cryptosystems. Among the difficult problems that ensure the safety of these systems, there is one that consists in finding a small generator, if it exists, of an ideal. The case of cyclotomic fields is considered in [33].

We also use the computations of class numbers to search for examples and counter-examples for mathematical conjectures. For example a study of cyclic cubic fields [26] allowed to progress in the study of Greenberg's conjecture [2].

Another consecrated problem in algorithmic number theory is smoothness testing, i.e. given an integer, decide if all its prime factors are smaller than a given bound. The only subexponential algorithm for this is H. Lenstra's elliptic curve method. Many of the families of elliptic curves here were found (according to the authors) by

[2] R. Greenberg, « On the Iwasawa invariants of totally real number fields », American J. of Math., vol. 98, 1976, p. 263-284.

ad-hoc methods. We introduced a new point of view which allows to make rapidly a finite list of families which are guaranteed to contain the good families for the elliptic curve method of factorization [31].

2.2.3. Topology in small dimension

2.2.3.1. Character varieties

There is a tradition of using computations and software to study and understand the topology of small dimensional manifolds, going back at least to Thurston's works (and before him, Riley's pionering work). The underlying philosophy of these tools is to build combinatorial models of manifolds (for example, the torus is often described as a square with an identification of the sides). For dimension 2, 3, 4, this approach is relevant and effective. In the team OURAGAN, we focus on the dimension 3, where the manifolds are modelized by a finite numbers of tetrahedra with identification of the faces. The software SnapPy [3] implements this strategy and is regularly used as a starting point in our work. Along the same philosophy of implementation, we can also cite Regina [4]. A specific trait of SnapPy is that it focuses on hyperbolic structures on the 3-dimensional manifolds. This setting is the object of a huge amount of theoretical work that were used to speed up computations. For example, some Newton methods were implemented without certification for solving a system of equations, but the theoretical knowledge of the uniqueness of the solution made this implementation efficient enough for the target applications. In recent years, in part under the influence of our team [5], more attention has been given to certified computations and now this is implemented in SnapPy.

This philosophy (modelization of manifolds by quite simple combinatoric models to compute such complicated objects as representations of the fundamental group) was applied in a pioneering work of Falbel[5] when he begins to look for another type of geometry on 3-dimensional manifolds (called CR-spherical geometry). From a computational point of view, this change of objectives was a jump in the unknown: the theoretical justification for the computations were missing, and the number of variables of the systems were multiplied by four. So instead of a relatively small system that could be tackled by Newton methods and numerical approximations, we had to deal with/study (were in front of) relatively big systems (the smallest example being 8 variables of degree 6) with no a priori description of the solutions. This input from OURAGAN was needed and proved to be useful.

Still, the computable objects that appear from the theoretical study are very often outside the reach of automated computations and are to be handled case by case. A few experts around the world have been tackling this kind of computations (Dunfield, Goerner, Heusener, Porti, Tillman, Zickert) and the main current achievement is the *Ptolemy module* [6] for SnapPy.

From these early computational needs, topology in small dimension has historically been the source of collaboration with the IMJ-PRG laboratory. At the beginning, the goal was essentially to provide computational tools for finding geometric structures in triangulated 3-dimensional varieties. Triangulated varieties can be topologically encoded by a collection of tetrahedra with gluing constraints (this can be called a triangulation or mesh, but it is not an approximation of the variety by simple structures, rather a combinatorial model). Imposing a geometric structure on this combinatorial object defines a number of constraints that we can translate into an algebraic system that we then have to solve to study geometric structures of the initial variety, for example in relying on solutions to study representations of the fundamental group of the variety. For these studies, a large part of the computable objects or algorithms we develop are required, from the algorithms for univariate polynomials to systems depending on parameters. It should be noted that most of the computational work lies in the modeling of problems [32] (see [4]) that have strictly no chance to be solved by blindly running the most powerful black boxes: we usually deal here with systems that have 24 to 64 variables, depend on 4 to 8 parameters and with degrees exceeding 10 in each variable. With an ANR [7] funding on the subject, the progress that we did [48](see [4]) were (much) more significant than expected. In particular, we have introduced new

[3] https://www.math.uic.edu/t3m/SnapPy/
[4] https://regina-normal.github.io
[5] as part of the CURVE project
[6] https://www.math.uic.edu/t3m/SnapPy/ptolemy.html
[7] ANR project Structures Géométriques et Triangulations

computable objects with an immediate theoretical meaning (let us say rather with a theoretical link established with the usual objects of the domain), namely, the so-called *deformation variety*.

Recent developments around Mahler measure [24] lead to the study of new computable objects at a cross-road between geometry and number theory.

2.2.3.2. Knot theory

Knot theory is a wide area of mathematics. We are interested in polynomial representations of long knots, that is to say polynomial embeddings $\mathbf{R} \to \mathbf{R}^3 \subset \mathbf{S}^3$. Every knot admits a polynomial representation and a natural question is to determine explicit parameterizations, minimal degree parameterizations. On the other hand we are interested to determine what is the knot of a given polynomial smooth embedding $\mathbf{R} \to \mathbf{R}^3$. These questions involve real algebraic curves. Two-bridge knots (or rational knots) are particularly studied because they are much easier to study. The first 26 knots (except 8_5) are two-bridge knots. It is proved that every knot is a Chebyshev knot [67], that is to say can be parameterized by a Chebyshev curve $(T_a(t), T_b(t), T_c(t+\varphi))$ where $T_n(t) = \cos(n \arccos t)$ is the n-th Chebyshev polynomial of the first kind. Chebyshev knots are polynomial analogues of Lissajous knots that have been studied by Jones, Hoste, Lamm...

Our activity in Knot theory is a bridge between our work in computational geometry (topology and drawing of real space curves) and our work on topology in small dimensions (varieties defined as a knot complement). It was first established that any knot can be parameterized by Chebyshev polynomials, then we have studied the properties of harmonic nodes [69] which then opened the way to effective computations. We were able to give an exhaustive, minimal and certified list of Chebyshev parameterizations of the first rational knots, using blind computations [70]. On the other hand, we propose the identification of Chebyshev knot diagrams ([12]) by developing new certified algorithms for computing trigonometric expressions [71], which was also the subject of Tran Cuong's PhD thesis at UPMC [78]. These works share many tools with our action in visualization and computational geometry.

We made use of Chebyshev polynomials so as Fibonacci polynomials which are families of orthogonal polynomials. Considering the Alexander-Conway polynomials as continuant polynomials in the Fibonacci basis, we were able to give a partial answer to Hoste's conjecture on the roots of Alexander polynomials of alternating knots [68].

We study the lexicographic degree of the two-bridge knots, that is to say the minimal (multi)degree of a polynomial representation of a N-crossing two-bridge knot. We show that this degree is $(3, b, c)$ with $b + c = 3N$. We have determined the lexicographic degree of the first 362 first two-bridge knots with 12 crossings or fewer [39].Minimal degrees are available [8]. These results make use of the braid theoretical approach developped by Y. Orevkov to study real plane curves and the use of real pseudoholomorphic curves ([2]), the slide isotopies on trigonal diagrams, namely those that never increase the number of crossings [38].

2.2.3.3. Visualization and Computational Geometry

The drawing of algebraic curves and surfaces is a critical action in OURAGAN since it is a key ingredient in numerous developments. For example, a certified plot of a discriminant variety could be the only admissible answer that can be proposed for engineering problems that need the resolution of parametric algebraic systems: this variety (and the connected components of its counter part) defines a partition of the parameter's space in regions above which the solutions are numerically stable and topologically simple.

For our action in Algorithmic Geometry, we are associated with the GAMBLE EPI (Inria Nancy Grand Est) with the aim of developing computational techniques for the study, plotting and topology of real algebraic curves and surfaces. The work involves the development of effective methods of resolution of algebraic systems with 2 or 3 variables (see [1] for example) which are basic engines for computing the topology [74], [43] / or plotting.

[8] https://webusers.imj-prg.fr/~pierre-vincent.koseleff/knots/2bk-lexdeg.html

3. Research Program

3.1. Basic computable objects and algorithms

The development of basic computable objects is somehow *on demand* and depends on all the other directions. However, some critical computations are already known to be bottlenecks and are sources of constant efforts.

Computations with algebraic numbers appear in almost all our activities: when working with number fields in our work in algorithmic number theory as well as in all the computations that involve the use of solutions of zero-dimensional systems of polynomial equations. Among the identified problems: finding good representations for single number fields (optimizing the size and degree of the defining polynomials), finding good representations for towers or products of number fields (typically working with a tower or finding a unique good extension), efficiently computing in practice with number fields (using certified approximation vs working with the formal description based on polynomial arithmetics). Strong efforts are currently done in the understanding of the various strategies by means of tight theoretical complexity studies [43], [72], [35] and many other efforts will be required to find the right representation for the right problem in practice. For example, for isolating critical points of plane algebraic curves, it is still unclear (at least the theoretical complexity cannot help) that an intermediate formal parameterization is more efficient than a triangular decomposition of the system and it is still unclear that these intermediate computations could be dominated in time by the certified final approximation of the roots.

3.2. Algorithmic Number Theory

Concerning algorithmic number theory, the main problems we will be considering in the coming years are the following:

- *Number fields.* We will continue working on the problems of class groups and generators. In particular, the existence and accessibility of *good* defining polynomials for a fixed number field remain very largely open. The impact of better polynomials on the algorithmic performance is a very important parameter, which makes this problem essential.
- *Lattice reduction.* Despite a great amount of work in the past 35 years on the LLL algorithm and its successors, many open problems remain. We will continue the study of the use of interval arithmetic in this field and the analysis of variants of LLL along the lines of the *Potential*-LLL which provides improved reduction comparable to BKZ with a small block size but has better performance.
- *Elliptic curves and Drinfeld modules.* The study of elliptic curves is a very fruitful area of number theory with many applications in crypto and algorithms. Drinfeld modules are “cousins” of elliptic curves which have been less explored in the algorithm context. However, some recent advances [44] have used them to provide some fast sophisticated factoring algorithms. As a consequence, it is natural to include these objects in our research directions.

3.3. Topology in small dimension

3.3.1. Character varieties

The brute force approach to computable objects from topology of small dimension will not allow any significant progress. As explained above, the systems that arise from these problems are simply outside the range of doable computations. We still continue the work in this direction by a four-fold approach, with all three directions deeply inter-related. First, we focus on a couple of especially meaningful (for the applications) cases, in particular the 3-dimensional manifold called Whitehead link complement. At this point, we are able to make steps in the computation and describe part of the solutions [48], [55]; we hope to be able to complete the computation using every piece of information to simplify the system. Second, we continue the theoretical work to understand more properties of these systems [46]. These properties may prove how useful for the mathematical understanding is the resolution of such systems - or at least the extraction of

meaningful information. This approach is for example carried on by Falbel and his work on configuration of flags [49], [51]. Third, we position ourselves as experts in the know-how of this kind of computations and natural interlocutors for colleagues coming up with a question on such a computable object [53], [55]. This also allows us to push forward the kind of computation we actually do and make progress in the direction of the second point. We are credible interlocutors because our team has the blend of theoretical knowledge and computational capabilities that grants effective resolutions of the problems we are presented. And last, we use the knowledge already acquired to pursue our theoretical study of the CR-spherical geometry [42], [50], [47].

Another direction of work is the help to the community in experimental mathematics on new objects. It involves downsizing the system we are looking at (for example by going back to systems coming from hyperbolic geometry and not CR-spherical geometry) and get the most out of what we can compute, by studying new objects. An example of this research direction is the work of Guilloux around the volume function on deformation varieties. This is a real-analytic function defined on the varieties we specialized in computing. Being able to do effective computations with this function led first to a conjecture [52]. Then, theoretical discussions around this conjecture led to a paper on a new approach to the Mahler measure of some 2-variables polynomials [54]. In turn, this last paper gave a formula for the Mahler measure in terms of a function akin to the volume function applied at points in an algebraic variety whose moduli of coordinates are 1. The OURAGAN team has the expertise to compute all the objects appearing in this formula, opening the way to another area of application. This area is deeply linked with number theory as well as topology of small dimension. It requires all the tools at disposition within OURAGAN.

3.3.2. Knot theory

We will carry on the exhaustive search for the lexicographic degrees for the rational knots. They correspond to trigonal space curves: computations in the braid group B_3, explicit parametrization of trigonal curves corresponding to "dessins d'enfants", etc. The problem seems much more harder when looking for more general knots.

On the other hand, a natural direction would be: given an explicit polynomial space curve, determine the under/over nature of the crossings when projecting, draw it and determine the known knot [9] it is isotopic to.

3.3.3. Vizualisation and Computational Geometry

As mentioned above, the drawing of algebraic curves and surfaces is a critical action in OURAGAN since it is a key ingredient in numerous developments. In some cases, one will need a fully certified study of the variety for deciding existence of solutions (for example a region in a robot's parameter's space with solutions to the DKP above or deciding if some variety crosses the unit polydisk for some stability problems in control-theory), in some other cases just a partial but certified approximation of a surface (path planning in robotics, evaluation of non algebraic functions over an algebraic variety for volumes of knot complements in the study of character varieties).

On the one hand, we will contribute to general tools like ISOTOP [10] under the supervision of the GAMBLE project-team and, on the other hand, we will propose ad-hoc solutions by gluing some of our basic tools (problems of high degrees in robust control theory). The priority is to provide a first software that implements methods that fit as most as possible the very last complexity results we got on several (theoretical) algorithms for the computation of the topology of plane curves.

A particular effort will be devoted to the resolution of overconstraint bivariate systems which are useful for the studies of singular points and to polynomials systems in 3 variables in the same spirit : avoid the use of Gröbner basis and propose a new algorithm with a state-of-the-art complexity and with a good practical behavior.

[9] for example the first rational knots are listed at https://team.inria.fr/ouragan/knots
[10] https://isotop.gamble.loria.fr

In parallel, one will have to carefully study the drawing of graphs of non algebraic functions over algebraic complex surfaces for providing several tools which are useful for mathematicians working on topology in small dimension (a well known example is the drawing of amoebia, a way of representing a complex curve on a sheet of paper).

4. Application Domains

4.1. Security of cryptographic systems

The study of the security of asymmetric cryptographic systems comes as an application of the work carried out in algorithmic number theory and revolves around the development and the use of a small number of general purpose algorithms (lattice reduction, class groups in number fields, discrete logarithms in finite fields, ...). For example, the computation of generators of principal ideals of cyclotomic fields can be seen as one of these applications since these are used in a number of recent public key cryptosystems.

The cryptographic community is currently very actively assessing the threat coming for the development of quantum computers. Indeed, such computers would permit tremendous progresses on many number theoretic problems such as factoring or discrete logarithm computations and would put the security of current cryptosystem under a major risk. For this reason, there is a large global research effort dedicated to finding alternative methods of securing data. In particular, the US standardization agency called NIST has recently launched a standardization process around this issue. In this context, OURAGAN is part of the competition and has submitted a candidate, also published in [13]. This method is based on number-theoretic ideas involving a new presumably difficult problem concerning the Hamming distance of integers modulo large numbers of Mersenne.

4.2. Robotics

Algebraic computations have tremendously been used in Robotics, especially in kinematics, since the last quarter of the 20th century. For example, one can cite different proofs for the 40 possible solutions to the direct kinematics problem for steward platforms and companion experiments based on Gröbner basis computations. On the one hand, hard general kinematics problems involve too many variables for pure algebraic methods to be used in place of existing numerical or semi-numerical methods everywhere and everytime, and on the other hand, for some quite large classes, global algebraic studies allow to propose exhaustive classifications that cannot be reached by other methods.

Robotics is a long-standing collaborative work with LS2N (Laboratory of Numerical Sciences of Nantes). Work has recently focused on the offline study of mechanisms, mostly parallel, their singularities or at least some types of singularities (cuspidals robots: cusps in the workspace).

For most parallel or serial manipulators, pose variables and joints variables are linked by algebraic equations and thus lie an algebraic variety. The two-kinematics problems (the direct kinematics problem - DKP- and the inverse kinematics problem - IKP) consist in studying the preimage of the projection of this algebraic variety onto a subset of unknowns. Solving the DKP remains to computing the possible positions for a given set of joint variables values while solving the IKP remains to computing the possible joints variables values for a given position. Algebraic methods have been deeply used in several situations for studying parallel and serial mechanisms, but finally their use stays quite confidential in the design process. Cylindrical Algebraic Decomposition coupled with variable's eliminations by means of Gröbner based computations can be used to model the workspace, the joint space and the computation of singularities. On the one hand, such methods suffer immediately when increasing the number of parameters or when working with imprecise data. On the other hand, when the problem can be handled, they might provide full and exhaustive classifications. The tools we use in that context [41] [40] ([58], [60], [59]) depend mainly on the resolution of parameter-based systems and therefore of study-dependent curves or flat algebraic surfaces (2 or 3 parameters), thus joining our thematic *Algorithmic Geometry*.

4.3. Control theory

Many problems in control theory have been studied using general exact polynomial solvers in the past. One can cite the famous Routh-Hurwitz criterion (late 19th century) for the stability of a linear time invariant (LTI) control system and its relation with Sturm sequences and Cauchy index. However most of the strategies used were involving mostly tools for univariate polynomials and then tried to tackle multivariate problems recursively with respect to the variables. More recent work are using a mix of symbolic/numeric strategies, using semi-definite programming for classes of optimization problems or homotopy methods for some algebraic problems, but still very few practical experiments are currently involving certified algebraic using general solvers for polynomial equations.

Our work in control theory is a recent activity and it is done in collaboration with a group of specialists, the GAIA team, Inria Lille-Nord Europe. We started with a well-known problem, the study of the stability of differential delay systems and multidimensional systems with an important observation: with a correct modelization, some recent algebraic methods, derived from our work in algorithmic geometry and shared with applications in robotics, now allow some previously impossible computations and lead to a better understanding of the problems to be solved [37], [36]. The field is porous to computer algebra since one finds for a long time algebraic criteria of all kinds but the technology seems blocked on a recursive use of one-variable methods, whereas our approach involves the direct processing of problems into a larger number of variables or variants.

The structural stability of n-D discrete linear systems (with $n \geq 2$) is a good source of problems of several kinds ranging from solving univariate polynomials to studying algebraic systems depending on parameters. For example, we have shown that the standard characterization of the structural stability of a multivariate rational transfer function (namely, the denominator of the transfer function does not have solutions in the unit polydisc of $\mathbb{C}^n$) is equivalent to deciding whether or not a certain system of polynomial equations has real solutions. The use state-of-the-art computer algebra algorithms to check this last condition, and thus the structural stability of multidimensional systems has been validated in several situations from toy examples with parameters to state-of-the-art examples involving the resolution of bivariate systems.

5. Highlights of the Year

5.1. Highlights of the Year

- In [24], Antonin Guilloux and Julien Marché propose a closed formula for the Mahler measure of a class of bivariate polynomials with rational coefficients (exact polynomials). This class of polynomials contains A-polynomials of knot complements and the authors express the Mahler Measure of a volume function defined on the vanishing set of the polynomial.

  As computing Mahler measures is a well known challenge in number theory and as computing volumes of knots complements is a critical objective for our research on character varieties, this result make an original bridge between our two main research directions.
- A key encapsulation message named Mersenne-756839 has been submitted at the NIST call for standard on Post-Quantum Cryptography. This submission is a complement to the article [13] presented in three invited lectures by Antoine Joux (JFLI (UMI CNRS) / Tokyo university , Nanyang Technological University, LATtice Crypto and Algorithms conference).
- Our agreement with WATERLOO MAPLE INC. has been reviewed for a two years term in 2018. Out next objective is the diffusion of our new solver for univariate polynomials with real coefficients.

6. New Software and Platforms

6.1. ISOTOP

Topology and geometry of planar algebraic curves

KEYWORDS: Topology - Curve plotting - Geometric computing
FUNCTIONAL DESCRIPTION: Isotop is a Maple software for computing the topology of an algebraic plane curve, that is, for computing an arrangement of polylines isotopic to the input curve. This problem is a necessary key step for computing arrangements of algebraic curves and has also applications for curve plotting. This software has been developed since 2007 in collaboration with F. Rouillier from Inria Paris - Rocquencourt.
NEWS OF THE YEAR: In 2018, an engineer from Inria Nancy (Benjamin Dexheimer) finished the implementation of the web server to improve the diffusion of our software.

- Participants: Luis Penaranda, Marc Pouget and Sylvain Lazard
- Contact: Marc Pouget
- Publications: Rational Univariate Representations of Bivariate Systems and Applications - Separating Linear Forms for Bivariate Systems - On The Topology of Planar Algebraic Curves - New bivariate system solver and topology of algebraic curves - Improved algorithm for computing separating linear forms for bivariate systems - Solving bivariate systems using Rational Univariate Representations - On the topology of planar algebraic curves - On the topology of real algebraic plane curves - Bivariate triangular decompositions in the presence of asymptotes - Separating linear forms and Rational Univariate Representations of bivariate systems
- URL: https://isotop.gamble.loria.fr/

6.2. RS

FUNCTIONAL DESCRIPTION: Real Roots isolation for algebraic systems with rational coefficients with a finite number of Complex Roots

- Participant: Fabrice Rouillier
- Contact: Fabrice Rouillier
- URL: https://team.inria.fr/ouragan/software/

6.3. A NewDsc

A New Descartes
KEYWORD: Scientific computing
FUNCTIONAL DESCRIPTION: Computations of the real roots of univariate polynomials with rational coefficients.

- Authors: Fabrice Rouillier, Alexander Kobel and Michael Sagraloff
- Partner: Max Planck Institute for Software Systems
- Contact: Fabrice Rouillier
- URL: https://anewdsc.mpi-inf.mpg.de

6.4. SIROPA

KEYWORDS: Robotics - Kinematics
FUNCTIONAL DESCRIPTION: Library of functions for certified computations of the properties of articulated mechanisms, particularly the study of their singularities

- Authors: Damien Chablat, Fabrice Rouillier, Guillaume Moroz and Philippe Wenger
- Partner: LS2N
- Contact: Guillaume Moroz
- URL: http://siropa.gforge.inria.fr/

6.5. MPFI

KEYWORD: Arithmetic

FUNCTIONAL DESCRIPTION: MPFI is a C library based on MPFR and GMP for multi precision floating point arithmetic.

- Contact: Fabrice Rouillier
- URL: http://mpfi.gforge.inria.fr

7. New Results

7.1. On $SL(3,\mathbb{C})$-representations of the Whitehead link group

In [9], we describe a family of representations in $SL(3,\mathbb{C})$ of the fundamental group π of the Whitehead link complement. These representations are obtained by considering pairs of regular order three elements in $SL(3,\mathbb{C})$ and can be seen as factorising through a quotient of π defined by a certain exceptional Dehn surgery on the Whitehead link. Our main result is that these representations form an algebraic component of the $SL(3,\mathbb{C})$-character variety of π.

7.2. A simplified approach to rigorous degree 2 elimination in discrete logarithm algorithms

In [10], we revisit the ZigZag strategy of Granger, Kleinjung and Zumbrägel. In particular, we provide a new algorithm and proof for the so-called degree 2 elimination step. This allows us to provide a stronger theorem concerning discrete logarithm computations in small characteristic fields $F_{q^{k_0 k}}$ with k close to q and k_0 a small integer. As in the aforementioned paper, we rely on the existence of two polynomials h_0 and h_1 of degree 2 providing a convenient representation of the finite field $F_{q^{k_0 k}}$.

7.3. Computing Chebyshev knot diagrams

A Chebyshev curve $\mathcal{C}(a,b,c,\phi)$ has a parametrization of the form $x(t) = T_a(t); \quad y(t) = T_b(t); z(t) = T_c(t+\phi)$, where a, b, c are integers, $T_n(t)$ is the Chebyshev polynomial of degree n and $\phi \in \mathbb{R}$. When $\mathcal{C}(a,b,c,\phi)$ is nonsingular, it defines a polynomial knot. In [12], we determine all possible knot diagrams when ϕ varies. Let a, b, c be integers, a is odd, $(a,b) = 1$, we show that one can list all possible knots $\mathcal{C}(a,b,c,\phi)$ in $O(n^2)$ bit operations, with $n = abc$.

7.4. Programmable projective measurement with linear optics

In [8] present a scheme for a universal device which can be programmed by quantum states to perform a chosen projective measurement, and its implementation in linear optics. In particular, our scheme takes a single input system (the input register), and M-1 systems all in a state psi (the program registers), whose role is to encode the measurement direction, and approximates the projective measurement with respect to the state psi on the input system. Importantly the scheme is entirely independent of the measurement basis choice psi. This is done optimally in M, if we demand the input state psi always returns the appropriate outcome, and limits to the ideal projective measurement with M. The size of the linear optical circuit we propose scales as M log M , and requires O(M log M) classical side processing. Our scheme can be viewed as an extension of the swap test to the instance where one state is supplied many times.

7.5. Updating key size estimations for pairings

Recent progress on NFS imposed a new estimation of the security of pairings. In [6], we study the best attacks against some of the most popular pairings. It allows us to propose new pairing-friendly curves of 128 bits and 192 bits of security.

7.6. How to Securely Compute with Noisy Leakage in Quasilinear Complexity

Since their introduction in the late 90's, side-channel attacks have been considered as a major threat against cryptographic implementations. This threat has raised the need for formal leakage models in which the security of implementations can be proved. At Eurocrypt 2013, Prouff and Rivain introduced the noisy leakage model which has been argued to soundly capture the physical reality of power and electromagnetic leakages. In their work, they also provide the first formal security proof for a masking scheme in the noisy leakage model. However their work has two important limitations: (i) the security proof relies on the existence of a leak-free component, (ii) the tolerated amount of information in the leakage (aka leakage rate) is of $O(1/n)$ where n is the number of shares in the underlying masking scheme. The first limitation was nicely tackled by Duc, Dziembowski and Faust one year later (Eurocrypt 2014). Their main contribution was to show a security reduction from the noisy leakage model to the conceptually simpler random- probing model. They were then able to prove the security of the well-known Ishai-Sahai-Wagner scheme (Crypto 2003) in the noisy leakage model. The second limitation was addressed last year in a paper by Andrychowicz, Dziembowski and Faust (Eurocrypt 2016). The proposed construction achieves security in the strong adaptive probing model with a leakage rate of $O(1/logn)$ at the cost of a $O(n^2logn)$ complexity. we argue that their result can be translated into the noisy leakage model with a leakage rate of $O(1)$ by using secret sharing based on algebraic geometric codes. They further argue that the efficiency of their construction can be improved by a linear factor using packed secret sharing but no details are provided.

In [14], we show how to compute in the presence of noisy leakage with a leakage rate up to $\widetilde{O}(1)$ in complexity $\widetilde{O}(n)$. They use a polynomial encoding allowing quasilinear multiplication based on the fast Number Theoretic Transform (NTT). They first show that the scheme is secure in the random-probing model with leakage rate $O(1/logn)$. Using the reduction by Duc et al. this result can be translated in the noisy leakage model with a $O(1/|F|^2logn)$ leakage rate. However, as in the work of Andrychowicz et al. , our construction also requires $|F| = O(n)$. In order to bypass this issue, we refine the granularity of our computation by considering the noisy leakage model on logical instructions that work on constant-size machine words. we provide a generic security reduction from the noisy leakage model at the logical-instruction level to the random-probing model at the arithmetic level. This reduction allows to prove the security of the construction in the noisy leakage model with leakage rate $\widetilde{O}(1)$).

7.7. A New Public-Key Cryptosystem via Mersenne Numbers

In [13], we propose a new public-key cryptosystem whose security is based on the computational intractability of the following problem: Given a Mersenne number $p = 2^n - 1$ where n is a prime, a positive integer h , and two n -bit integers T,R , find two n -bit integers F,G each of Hamming weight at most h such that T = F ·R+G modulo p , under the promise that they exist.

7.8. Workspace, Joint space and Singularities of a family of Delta-Like Robot

In [11], we describe the workspace, the joint space and the singularities of a family of delta-like parallel robots by using algebraic tools. The different func- tions of SIROPA library are introduced, which is used to induce an estimation about the complexity in representing the singularities in the workspace and the joint space. A Gröbner based elimination is used to compute the singularities of the manipulator and a Cylindrical Algebraic Decomposition algorithm is used to study the workspace and the joint space. From these algebraic objects, they propose some certified three-dimensional plotting describing the shape of works- pace and of the joint space which will help the engineers or researchers to decide the most suited configuration of the manipulator they should use for a given task. Also, the different parameters associated with the complexity of the serial and parallel singularities are tabulated, which further enhance the selection of the different configuration of the manipulator by comparing the complexity of the singularity equations.

7.9. Certified Non-conservative Tests for the Structural Stability of Discrete Multidimensional Systems

In [7], we present new computer algebra based methods for testing the structural stability of n-D discrete linear systems (with $n \geq 2$). More precisely, they show that the standard characterization of the structural stability of a multivariate rational transfer function (namely, the denominator of the transfer function does not have solutions in the unit polydisc of $\mathbb{C}^n$) is equivalent to the fact that a certain system of polynomials does not have real solutions. We then use state-of-the-art computer algebra algorithms to check this last condition, and thus the structural stability of multidimensional systems.

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

The objective of our Agrement with WATERLOO MAPLE INC. is to promote software developments to which we actively contribute.

On the one hand, WMI provides man power, software licenses, technical support (development, documentation and testing) for an inclusion of our developments in their commercial products. On the other hand, OURAGAN offers perpetual licenses for the use of the concerned source code.

As past results of this agreement one can cite our C-Library *RS* for the computations of the real solutions zero-dimensional systems or also our collaborative development around the Maple package *DV* for solving parametric systems of equations.

For this term, the agreement covers algorithms developed in areas including but not limited to: 1) solving of systems of polynomial equations, 2) validated numerical polynomial root finding, 3) computational geometry, 4) curves and surfaces topology, 5) parametric algebraic systems, 6) cylindrical algebraic decompositions, 7) robotics applications.

In particular, it covers our collaborative work with some of our partners, especially the Gamble Project-Team - Inria Nancy Grand Est.

9. Partnerships and Cooperations

9.1. European Initiatives

9.1.1. FP7 & H2020 Projects

Program:H2020-EU.1.1. - EXCELLENT SCIENCE - European Research Council (ERC)

Project acronym: Almacrypt

Project title: Algorithmic and Mathematical Cryptology

Duration: 01/2016 - 12/2010

Coordinator: Antoine Joux

Abstract: Cryptology is a foundation of information security in the digital world. Today's internet is protected by a form of cryptography based on complexity theoretic hardness assumptions. Ideally, they should be strong to ensure security and versatile to offer a wide range of functionalities and allow efficient implementations. However, these assumptions are largely untested and internet security could be built on sand. The main ambition of Almacrypt is to remedy this issue by challenging the assumptions through an advanced algorithmic analysis. In particular, this proposal questions the two pillars of public-key encryption: factoring and discrete logarithms. Recently, the PI contributed to show that in some cases, the discrete logarithm problem is considerably weaker

than previously assumed. A main objective is to ponder the security of other cases of the discrete logarithm problem, including elliptic curves, and of factoring. We will study the generalization of the recent techniques and search for new algorithmic options with comparable or better efficiency. We will also study hardness assumptions based on codes and subset-sum, two candidates for post-quantum cryptography. We will consider the applicability of recent algorithmic and mathematical techniques to the resolution of the corresponding putative hard problems, refine the analysis of the algorithms and design new algorithm tools. Cryptology is not limited to the above assumptions: other hard problems have been proposed to aim at post-quantum security and/or to offer extra functionalities. Should the security of these other assumptions become critical, they would be added to Almacrypt's scope. They could also serve to demonstrate other applications of our algorithmic progress. In addition to its scientific goal, Almacrypt also aims at seeding a strengthened research community dedicated to algorithmic and mathematical cryptology.

9.2. International Initiatives

9.2.1. Inria International Labs

9.2.1.1. Informal International Partners

- CQT Singapour (UMI CNRS Majulab)
- UFPA - Para -Brésil (José Miguel Veloso)
- Institut Joseph Fourier - Université Grenoble Alpes (Martin Deraux, V. Vitse et Pierre Will)
- Max-Planck-Institut für Informatik - Saarbrücken - Germany (Michael Sagraloff)
- Holon Institute of Technology, Israel (Jeremy Kaminsky)

9.3. International Research Visitors

9.3.1. Visits of International Scientists

- Jeremy Kaminsky (Holon Institute of Technology, Israel). 3-months visitor in Ouragan and École Polytechnique (MAX) and École des Mines. Chateaubriand Fellow. Subjects: Control Theory, Algebraic Geometry and Computer Vision.

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Organizing Committees

- Antonin Guilloux is a Co-organizer of the International conference Dynamics of Groups Actions (Cetraro, may 2019) [11]
- Antoine Joux co-organized the Sprint Summer School *Post-Scryptum* [12]
- Antoine-Joux co-organized *Crypto in the quantum age (STIAS)* [13]

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

- Antoine Joux was Program Chair of Africacrypt [14]

[11] http://dynamicsgroupactions.imj-prg.fr/fr/68-2/
[12] https://postscryptum.lip6.fr
[13] http://stias.ac.za/events/workshop-on-cryptography-in-the-quantum-age
[14] http://africacrypt2018.aui.ma/commitees.php

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- Elisha Falbel is a member of the editorial board of *São Paulo Journal of Mathematical Sciences - Springer*
- Antoine Joux is a member of the editorial board of *Designs, Codes and Cryptography*
- Fabrice Rouillier is a member of the editorial board of *Journal of Symbolic Computation*

10.1.3.2. Reviewer - Reviewing Activities

- Antonin Guilloux is reviewer in several journals, including Duke Math Journal.
- Razvan Barbulescu is reviewer for several cryptology conferences including Eurocrypt and WAIFI.

10.1.4. Invited Talks

- Razvan Barbulescu, Cryptography and algorithmic number theory, june 2018, Caen
- Elisha Falbel, Colloquium Heidelberg, June 2018 -Heidelberg -Alemagne
- Elisha Falbel, Representation varieties and geometric structures in low dimensions , July 2018 - Warwick-UK
- Elisha Falbel, Modern Trends in Differential Geometry, July 2018, Sao Paulo- Brazil
- Antonin Guilloux, Computation in Geometric Topology, December 2017 - Warwick - UK.
- Antonin Guilloux, Mahler Measure and values of L-functions, August 2018 - Copenhagen - Denmark.
- Antoine Joux, JFLI (UMI CNRS) / Tokyo university, May 2018, Tokyo https://jfliwp.prod.lamp.cnrs.fr/2018/04/13/jfli-seminar-on-the-mersenne-cryptosystem/
- Antoine Joux, Invited Lecture at the conference *Lattice crypto and algorithms*, May 2018, Bertinoro, Italy
- Antoine Joux, The Mersenne Cryptosystem, Nanyang University, June 2018, Singapore

10.1.5. Research Administration

- Fabrice Rouillier is a member of the scientific commitee of the Indo French Centre for Applied Mathematics

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Elisha Falbel : courses in Algebra and Analysis, L1 , Sorbonne Université.

Elisha Falbel : Course in Probabiltés, L3, Polytech

Elisha Falbel : Introduction aux surfaces de Riemann, M1, Sorbonne Université.

Antonin Guilloux: Courses in General Mathematics, L1, Sorbonne Université.

Antonin Guilloux: Chair of the Mathematics in L1 at Sorbonne Université; Lead of the renewing of the mathematical courses in L1 at Sorbonne Université for 2019.

Antonin Guilloux: Course in Hyperbolic geometry and character varieties, M2, Sorbonne Université.

Antoine Joux : Course on Techniques in Cryptography and Cryptanalysis, M2, Parisian Master of Research in Computer Science.

Pierre-Vincent Koseleff : Course on Applied Algebra, L3 for undergraduate students (6th semester), Sorbonne Université.

Pierre-Vincent Koseleff : Préparation à l'agrégation de Mathématiques, M2. General Chair and teacher. Sorbonne Université.

Fabrice Rouillier : Course in Algebraic Computations, M1, 24h, Sorbonne Université.

Fabrice Rouillier : Course in "Agrégation Option - C", M2, 31 heures,Sorbonne Université.

Razvan Barbulescu : part of the Course at MPRI Arithmetic algorithms for cryptology 6h

Razvan Barbulescu : 3 projects of cryptology in Python

Razvan Barbulescu : exercice sessions for Algorithmic and complexity 30h

10.2.2. Supervision

PhD in progress : Thomas Espitau, 09/2016, directed by Antoine Joux

PhD in progress : Natalia Kharchenko, 09/2016, directed by Antoine Joux

PhD in progress : Mahya Mehrabdollahei, 09/2018, directed by Antonin Guilloux and Fabrice Rouillier

PhD in progress : Sudarshan Shinde, 09/2016, directed by Razvan Barbulescu and Pierre-Vincent Koseleff

PhD in progress : Robin Timsit, 09/2015, directed by Elisha Falbel

10.2.3. Juries

- Fabrice Rouillier was reviewer of the PhD of Ruben Becker (Universität des Saarlandes)
- Antonin Guilloux, jury of the PhD thesis of Alexandre Bellis - Etude Topologique du Flot Horocyclique Le cas des surfaces Géométriquement Infnies - Supervisor: Françoise Dal'Bo.

10.3. Popularization

10.3.1. Internal or external Inria responsibilities

- Razvan Barbulescu is *chargé médiation* at IMJ-PRG
- Razvan Barbulescu is a member of the steering commitee of the association *Animath* [15]
- Fabrice Rouillier is *chargé de mission médiation* at Inria Paris
- Fabrice Rouillier is a member of the editorial board of *Interstices*
- Fabrice Rouillier is the president of the association *Animath*

10.3.2. Interventions

- Razvan Barbulescu co-organizes the *Alkindi* [16] competition on crytography (50000 participants)

11. Bibliography

Major publications by the team in recent years

[1] Y. BOUZIDI, S. LAZARD, G. MOROZ, M. POUGET, F. ROUILLIER, M. SAGRALOFF. *Solving bivariate systems using Rational Univariate Representations*, in "Journal of Complexity", 2016, vol. 37, pp. 34–75 [*DOI :* 10.1016/J.JCO.2016.07.002], https://hal.inria.fr/hal-01342211

[2] E. BRUGALLÉ, P.-V. KOSELEFF, D. PECKER. *On the lexicographic degree of two-bridge knots*, in "Journal Of Knot Theory And Its Ramifications (JKTR)", June 2016, vol. 25, n° 7, 14p., 21 figs [*DOI :* 10.1142/S0218216516500449], https://hal.archives-ouvertes.fr/hal-01084472

[3] E. FALBEL, A. GUILLOUX. *Dimension of character varieties for 3-manifolds*, in "Proceedings of the American Mathematical Society", 2016 [*DOI :* 10.1090/PROC/13394], https://hal.archives-ouvertes.fr/hal-01370284

[15] http://www.animath.fr
[16] http://concours-alkindi.fr/

[4] E. FALBEL, A. GUILLOUX, P.-V. KOSELEFF, F. ROUILLIER, M. THISTLETHWAITE. *Character Varieties For SL(3,C): The Figure Eight Knot*, in "Experimental Mathematics", 2016, vol. 25, n° 2, 17 p. [*DOI :* 10.1080/10586458.2015.1068249], https://hal.inria.fr/hal-01362208

[5] E. FALBEL, J. WANG. *Branched spherical CR structures on the complement of the figure-eight knot*, in "Michigan Mathematical Journal", 2014, vol. 63, pp. 635-667, https://hal.archives-ouvertes.fr/hal-01374789

Publications of the year

Articles in International Peer-Reviewed Journals

[6] R. BARBULESCU, S. DUQUESNE. *Updating key size estimations for pairings*, in "Journal of Cryptology", 2018, https://hal.archives-ouvertes.fr/hal-01534101

[7] Y. M. BOUZIDI, A. QUADRAT, F. ROUILLIER. *Certified Non-conservative Tests for the Structural Stability of Discrete Multidimensional Systems*, in "Multidimensional Systems and Signal Processing", June 2018, https://hal.inria.fr/hal-01951765

[8] U. CHABAUD, E. DIAMANTI, D. MARKHAM, E. KASHEFI, A. JOUX. *Optimal quantum-programmable projective measurement with linear optics*, in "Physical Review A", December 2018, https://arxiv.org/abs/1805.02546 - 11 pages, 7 figures [*DOI :* 10.1103/PHYSREVA.98.062318], https://hal.sorbonne-universite.fr/hal-01931757

[9] A. GUILLOUX, P. WILL. *On SL(3,C)-representations of the Whitehead link group*, in "Geometriae Dedicata", 2018, https://arxiv.org/abs/1607.01536 [*DOI :* 10.1007/S10711-018-0404-8], https://hal.archives-ouvertes.fr/hal-01370289

[10] F. GÖLOĞLU, A. JOUX. *A simplified approach to rigorous degree 2 elimination in discrete logarithm algorithms*, in "Mathematics of Computation", 2018, 1 p. , https://hal.archives-ouvertes.fr/hal-01960765

[11] R. JHA, D. CHABLAT, L. BARON, F. ROUILLIER, G. MOROZ. *Workspace, Joint space and Singularities of a family of Delta-Like Robot*, in "Mechanism and Machine Theory", September 2018, vol. 127, pp. 73-95 [*DOI :* 10.1016/J.MECHMACHTHEORY.2018.05.004], https://hal.archives-ouvertes.fr/hal-01796066

[12] P.-V. KOSELEFF, D. PECKER, F. ROUILLIER, C. TRAN. *Computing Chebyshev knot diagrams*, in "Journal of Symbolic Computation", 2018, vol. 86, 21 p. , https://arxiv.org/abs/1512.07766 [*DOI :* 10.1016/J.JSC.2017.04.001], https://hal.inria.fr/hal-01232181

Scientific Books (or Scientific Book chapters)

[13] D. AGGARWAL, A. JOUX, A. PRAKASH, M. SANTHA. *A New Public-Key Cryptosystem via Mersenne Numbers*, in "Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III", Springer, 2018, pp. 459-482, https://hal.archives-ouvertes.fr/hal-01960756

[14] D. GOUDARZI, A. JOUX, M. RIVAIN. *How to Securely Compute with Noisy Leakage in Quasilinear Complexity*, in "Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part II", Springer, October 2018, pp. 547-574, https://hal.archives-ouvertes.fr/hal-01960745

[15] A. GUILLOUX, S. LANFRANCHI, É. VARCIN. *Mussolini et les mots de la race*, in "La pensée de la race en Italie : du romantisme au fascisme", A. ARAMINI, E. BOVO (editors), Cahiers de la MSHE Ledoux. Archives de l'imaginaire social, Presses universitaires de Franche-Comté, May 2018, pp. 169-184, https://hal.archives-ouvertes.fr/hal-01768471

Other Publications

[16] D. M. ALMEIDA, E. E. FALBEL. *Fat sub-Riemannian symmetric spaces: the nilpotent case*, May 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01791316

[17] R. BARBULESCU, S. SHINDE. *A complete classification of ECM-friendly families using modular curves*, June 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01822144

[18] E. BRUGALLÉ, P.-V. KOSELEFF, D. PECKER. *The lexicographic degree of the first two-bridge knots*, September 2018, https://arxiv.org/abs/1501.06393 - 30 p., 58 fig., 6 tables, https://hal.archives-ouvertes.fr/hal-01108678

[19] D. N. DIATTA, S. DIATTA, F. ROUILLIER, M.-F. ROY, M. SAGRALOFF. *Bounds for polynomials on algebraic numbers and application to curve topology*, October 2018, https://arxiv.org/abs/1807.10622 - working paper or preprint, https://hal.inria.fr/hal-01891417

[20] E. FALBEL, A. GUILLOUX, P. WILL. *Hilbert metric, beyond convexity*, 2018, https://arxiv.org/abs/1804.05317 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-01768400

[21] E. FALBEL, M. MACULAN, G. SARFATTI. *Configurations of flags in orbits of real forms*, April 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01779459

[22] E. FALBEL, J. VELOSO. *Flag structures on real 3-manifolds*, April 2018, https://arxiv.org/abs/1804.11096 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-01778582

[23] A. GUILLOUX, I. KIM. *Deformation space of discrete groups of SU(2,1) in quaternionic hyperbolic plane*, March 2018, https://arxiv.org/abs/1803.05231 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-01736953

[24] A. GUILLOUX, J. MARCHÉ. *Volume function and Mahler measure of exact polynomials*, April 2018, https://arxiv.org/abs/1804.01395 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-01758986

References in notes

[25] R. BARBULESCU. *A brief history of pairings*, in "International Workshop on the Arithmetic of Finite Fields WAIFI 2016", Gand, Belgium, Arithmetic of Finite Fields – WAIFI 2016, Springer, July 2016, vol. 10064, https://hal.archives-ouvertes.fr/hal-01363444

[26] R. BARBULESCU, S. DUQUESNE. *Updating key size estimations for pairings*, in "Journal of Cryptology", December 2018, vol. published online, to appear in print, https://hal.archives-ouvertes.fr/hal-01534101

[27] R. BARBULESCU, P. GAUDRY, A. GUILLEVIC, F. MORAIN. *Improving NFS for the discrete logarithm problem in non-prime finite fields*, in "Eurocrypt 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques", Sofia, Bulgaria, M. FISCHLIN, E. OSWALD (editors),

Advances in Cryptology – EUROCRYPT 2015, April 2015, vol. 9056, pp. 129-155 [*DOI :* 10.1007/978-3-662-46800-5_6], https://hal.inria.fr/hal-01112879

[28] R. BARBULESCU, P. GAUDRY, A. JOUX, E. THOMÉ. *A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic*, in "Eurocrypt 2014", Copenhagen, Denmark, P. Q. NGUYEN, E. OSWALD (editors), Advances in Cryptology - EUROCRYPT 2014, Springer, May 2014, vol. 8441, pp. 1-16 [*DOI :* 10.1007/978-3-642-55220-5_1], https://hal.inria.fr/hal-00835446

[29] R. BARBULESCU, P. GAUDRY, T. KLEINJUNG. *The Tower Number Field Sieve*, in "ASIACRYPT 2015", Auckland, New Zealand, T. IWATA, J. H. CHEON (editors), Advances in cryptology-Asiacrypt 2015, Springer, November 2015, vol. 9453, pp. 31-58, https://hal.archives-ouvertes.fr/hal-01155635

[30] R. BARBULESCU, C. PIERROT. *The Multiple Number Field Sieve for Medium and High Characteristic Finite Fields*, in "LMS Journal of Computation and Mathematics", 2014, vol. 17, pp. 230–246 [*DOI :* 10.1112/S1461157014000369], https://hal.inria.fr/hal-00952610

[31] R. BARBULESCU, S. SHINDE. *A complete classification of ECM-friendly families using modular curves*, June 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01822144

[32] N. BERGERON, E. FALBEL, A. GUILLOUX. *Tetrahedra of flags, volume and homology of SL(3)*, in "Geometry & Topology Monographs", 2014, vol. 18 [*DOI :* 10.2140/GT.2014.18.1911], https://hal.archives-ouvertes.fr/hal-01370258

[33] J.-F. BIASSE, T. ESPITAU, P.-A. FOUQUE, A. GÉLIN, P. KIRCHNER. *Computing generator in cyclotomic integer rings*, in "36th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2017)", Paris, France, Lecture Notes in Computer Science, April 2017, vol. 10210, pp. 60-88 [*DOI :* 10.1007/978-3-319-56620-7_3], https://hal.archives-ouvertes.fr/hal-01518438

[34] Y. BOUZIDI, S. LAZARD, G. MOROZ, M. POUGET, F. ROUILLIER. *Improved algorithm for computing separating linear forms for bivariate systems*, in "ISSAC - 39th International Symposium on Symbolic and Algebraic Computation", Kobe, Japan, July 2014, https://hal.inria.fr/hal-00992634

[35] Y. BOUZIDI, S. LAZARD, G. MOROZ, M. POUGET, F. ROUILLIER, M. SAGRALOFF. *Solving bivariate systems using Rational Univariate Representations*, in "Journal of Complexity", 2016, vol. 37, pp. 34–75 [*DOI :* 10.1016/J.JCO.2016.07.002], https://hal.inria.fr/hal-01342211

[36] Y. BOUZIDI, A. QUADRAT, F. ROUILLIER. *Certified Non-conservative Tests for the Structural Stability of Multidimensional Systems*, August 2017, 31 p. , To appear in Multidimensional Systems and Signal Processing, https://link.springer.com/article/10.1007/s11045-018-0596-y, https://hal.inria.fr/hal-01571230

[37] Y. BOUZIDI, F. ROUILLIER. *Certified Algorithms for proving the structural stability of two dimensional systems possibly with parameters*, in "MNTS 2016 - 22nd International Symposium on Mathematical Theory of Networks and Systems", Minneapolis, United States, Proceedings of the 22nd International Symposium on Mathematical Theory of Networks and Systems, July 2016, https://hal.inria.fr/hal-01366202

[38] E. BRUGALLÉ, P.-V. KOSELEFF, D. PECKER. *Untangling trigonal diagrams*, in "Journal Of Knot Theory And Its Ramifications (JKTR)", June 2016, vol. 25, n^{O} 7, 10p., 24 figs [*DOI :* 10.1142/S0218216516500437], https://hal.archives-ouvertes.fr/hal-01084463

[39] E. BRUGALLÉ, P.-V. KOSELEFF, D. PECKER. *The lexicographic degree of the first two-bridge knots*, September 2018, 30 p., 58 fig., 6 tables, submitted, https://hal.archives-ouvertes.fr/hal-01108678

[40] D. CHABLAT, R. JHA, F. ROUILLIER, G. MOROZ. *Non-singular assembly mode changing trajectories in the workspace for the 3-RPS parallel robot*, in "14th International Symposium on Advances in Robot Kinematics", Ljubljana, Slovenia, June 2014, pp. 149 - 159, https://hal.archives-ouvertes.fr/hal-00956325

[41] D. CHABLAT, R. JHA, F. ROUILLIER, G. MOROZ. *Workspace and joint space analysis of the 3-RPS parallel robot*, in "ASME 2013 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference", Buffalo, United States, August 2014, vol. Volume 5A, pp. 1-10, https://hal.archives-ouvertes.fr/hal-01006614

[42] M. DERAUX, E. FALBEL. *Complex hyperbolic geometry of the figure eight knot*, in "Geometry and Topology", February 2015, vol. 19, pp. 237–293 [*DOI :* 10.2140/GT.2015.19.237], https://hal.archives-ouvertes.fr/hal-00805427

[43] D. N. DIATTA, S. DIATTA, F. ROUILLIER, M.-F. ROY, M. SAGRALOFF. *Bounds for polynomials on algebraic numbers and application to curve topology*, October 2018, working paper or preprint, https://hal.inria.fr/hal-01891417

[44] J. DOLISKANI, A. K. NARAYANAN, É. SCHOST. *Drinfeld Modules with Complex Multiplication, Hasse Invariants and Factoring Polynomials over Finite Fields*, in "CoRR", 2017, vol. abs/1712.00669, http://arxiv.org/abs/1712.00669

[45] T. ESPITAU, A. JOUX. *Adaptive precision LLL and Potential-LLL reductions with Interval arithmetic*, in "IACR Cryptology ePrint Archive", 2016, vol. 2016, 528 p. , http://eprint.iacr.org/2016/528

[46] E. FALBEL, A. GUILLOUX. *Dimension of character varieties for 3-manifolds*, in "Proceedings of the American Mathematical Society", 2016 [*DOI :* 10.1090/PROC/13394], https://hal.archives-ouvertes.fr/hal-01370284

[47] E. FALBEL, A. GUILLOUX, P. WILL. *Hilbert metric, beyond convexity*, 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01768400

[48] E. FALBEL, P.-V. KOSELEFF, F. ROUILLIER. *Representations of fundamental groups of 3-manifolds into PGL(3,C): Exact computations in low complexity*, in "Geometriae Dedicata", August 2015, vol. 177, n^{o} 1, 52 p. [*DOI :* 10.1007/S10711-014-9987-X], https://hal.inria.fr/hal-00908843

[49] E. FALBEL, M. MACULAN, G. SARFATTI. *Configurations of flags in orbits of real forms*, April 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01779459

[50] E. FALBEL, R. SANTOS THEBALDI. *A Flag structure on a cusped hyperbolic 3-manifold with unipotent holonomy*, in "Pacific Journal of Mathematics", 2015, vol. 278, n^{o} 1, pp. 51-78, https://hal.archives-ouvertes.fr/hal-00958255

[51] E. FALBEL, J. VELOSO. *Flag structures on real 3-manifolds*, April 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01778582

[52] A. GUILLOUX. *Volume of representations and birationality of peripheral holonomy*, in "Experimental Mathematics", May 2017, https://hal.archives-ouvertes.fr/hal-01370287

[53] A. GUILLOUX, I. KIM. *Deformation space of discrete groups of SU(2,1) in quaternionic hyperbolic plane*, March 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01736953

[54] A. GUILLOUX, J. MARCHÉ. *Volume function and Mahler measure of exact polynomials*, April 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01758986

[55] A. GUILLOUX, P. WILL. *On SL(3,C)-representations of the Whitehead link group*, 2018, To appear in Geom. Ded., https://hal.archives-ouvertes.fr/hal-01370289

[56] A. GÉLIN, A. JOUX. *Reducing number field defining polynomials: an application to class group computations*, in "Algorithmic Number Theory Symposium XII", Kaiserslautern, Germany, LMS Journal of Computation and Mathematics, August 2016, vol. 19, n^{o} A, pp. 315–331 [*DOI :* 10.1112/S1461157016000255], https://hal.archives-ouvertes.fr/hal-01362144

[57] F. GÖLOĞLU, A. JOUX. *A Simplified Approach to Rigorous Degree 2 Elimination in Discrete Logarithm Algorithms*, in "IACR Cryptology ePrint Archive", 2018, vol. 2018, 430 p. , https://eprint.iacr.org/2018/430

[58] R. JHA, D. CHABLAT, L. BARON, F. ROUILLIER, G. MOROZ. *Workspace, Joint space and Singularities of a family of Delta-Like Robot*, in "Mechanism and Machine Theory", September 2018, vol. 127, pp. 73-95 [*DOI :* 10.1016/J.MECHMACHTHEORY.2018.05.004], https://hal.archives-ouvertes.fr/hal-01796066

[59] R. JHA, D. CHABLAT, F. ROUILLIER, G. MOROZ. *An algebraic method to check the singularity-free paths for parallel robots*, in "International Design Engineering Technical Conferences & Computers and Information in Engineering Conference", Boston, United States, ASME, August 2015, https://hal.archives-ouvertes.fr/hal-01142989

[60] R. JHA, D. CHABLAT, F. ROUILLIER, G. MOROZ. *Workspace and Singularity analysis of a Delta like family robot*, in "4th IFTOMM International Symposium on Robotics and Mechatronics", Poitiers, France, June 2015, https://hal.archives-ouvertes.fr/hal-01142465

[61] A. JOUX. *A one round protocol for tripartite Diffie-Hellman*, in "J. Cryptology", 2004, vol. 17, n^{o} 4, pp. 263–276

[62] A. JOUX, R. LERCIER. *The function field sieve is quite special*, in "Algorithmic Number Theory-ANTS V", Lecture Notes in Computer Science, Springer, 2002, vol. 2369, pp. 431-445

[63] A. JOUX, R. LERCIER. *Improvements to the general number field sieve for discrete logarithms in prime fields. A comparison with the gaussian integer method*, in "Math. Comput.", 2003, vol. 72, n^{o} 242, pp. 953-967

[64] A. JOUX, C. PIERROT. *Improving the Polynomial time Precomputation of Frobenius Representation Discrete Logarithm Algorithms - Simplified Setting for Small Characteristic Finite Fields*, in "20th International Conference on the Theory and Application of Cryptology and Information Security", Kaoshiung, Taiwan, Lecture Notes in Computer Science, Springer Berlin Heidelberg, December 2014, vol. 8873, pp. 378-397 [*DOI :* 10.1007/978-3-662-45611-8_20], https://hal.archives-ouvertes.fr/hal-01213649

[65] A. JOUX, C. PIERROT. *Nearly Sparse Linear Algebra and application to Discrete Logarithms Computations*, in "Contemporary Developments in Finite Fields and Applications ", 2016 [*DOI :* 10.1142/9789814719261_0008], https://hal.inria.fr/hal-01154879

[66] A. KOBEL, F. ROUILLIER, M. SAGRALOFF. *Computing Real Roots of Real Polynomials ... and now For Real!*, in " ISSAC '16 Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation", Waterloo, Canada, ISSAC '16 Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation, July 2016, 7 p. [*DOI :* 10.1145/2930889.2930937], https://hal.inria.fr/hal-01363955

[67] P.-V. KOSELEFF, D. PECKER. *Chebyshev Knots*, in "Journal of Knot Theory and Its Ramifications", April 2011, vol. 20, n^{o} 4, pp. 575-593 [*DOI :* 10.1142/S0218216511009364], https://hal.archives-ouvertes.fr/hal-00344501

[68] P.-V. KOSELEFF, D. PECKER. *On Alexander–Conway polynomials of two-bridge links*, in "Journal of Symbolic Computation", May 2015, vol. Volume 68, n^{o} 2, pp. 215-229, 15p [*DOI :* 10.1016/J.JSC.2014.09.011], https://hal.archives-ouvertes.fr/hal-00538729

[69] P.-V. KOSELEFF, D. PECKER. *Harmonic Knots*, in "Journal Of Knot Theory And Its Ramifications (JKTR)", 2016, vol. 25, n^{o} 13, 18 p. , 18 p., 30 fig. [*DOI :* 10.1142/S0218216516500747], https://hal.archives-ouvertes.fr/hal-00680746

[70] P.-V. KOSELEFF, D. PECKER, F. ROUILLIER. *The first rational Chebyshev knots*, in "Journal of Symbolic Computation", December 2010, vol. 45, n^{o} 12, pp. 1341-1358 [*DOI :* 10.1016/J.JSC.2010.06.014], https://hal.archives-ouvertes.fr/hal-00429510

[71] P.-V. KOSELEFF, F. ROUILLIER, C. TRAN. *On the sign of a trigonometric expression*, in "ISSAC ' 15", Bath, United Kingdom, Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation, July 2015 [*DOI :* 10.1145/2755996.2756664], https://hal.inria.fr/hal-01200820

[72] S. LAZARD, M. POUGET, F. ROUILLIER. *Bivariate triangular decompositions in the presence of asymptotes*, in "Journal of Symbolic Computation", 2017, vol. 82, pp. 123 - 133 [*DOI :* 10.1016/J.JSC.2017.01.004], https://hal.inria.fr/hal-01468796

[73] D. LAZARD, F. ROUILLIER. *Solving Parametric Polynomial Systems*, in "Journal of Symbolic Computation", June 2007, vol. 42, pp. 636-667

[74] D. NIANG DIATTA, F. ROUILLIER, M.-F. ROY. *On the computation of the topology of plane curves*, in "International Symposium on Symbolic and Algebraic Computation", Kobe, Japan, K. NABESHIMA (editor), ACM Press, July 2014, pp. 130-137 [*DOI :* 10.1145/2608628.2608670], https://hal.archives-ouvertes.fr/hal-00935728

[75] N. REVOL, F. ROUILLIER. *Motivations for an arbitrary precision interval arithmetic and the MPFI library*, in "Reliable Computing", August 2005, vol. 11, n^{o} 4, pp. 275-290 [*DOI :* 10.1007/S11155-005-6891-Y], https://hal.inria.fr/inria-00544998

[76] F. ROUILLIER. *Solving zero-dimensional systems through the rational univariate representation*, in "Journal of Applicable Algebra in Engineering, Communication and Computing", 1999, vol. 9, n^{o} 5, pp. 433–461

[77] F. ROUILLIER, P. ZIMMERMANN. *Efficient Isolation of Polynomial Real Roots*, in "Journal of Computational and Applied Mathematics", 2003, vol. 162, n^{o} 1, pp. 33–50

[78] C. TRAN. *Symbolic computing with the basis of Chebyshev's monic polynomials*, Université Pierre et Marie Curie - Paris VI, October 2015, https://tel.archives-ouvertes.fr/tel-01273287