IN PARTNERSHIP WITH:
CNRS

Ecole normale supérieure de Lyon

Université Claude Bernard (Lyon 1)

Activity Report 2019

Project-Team ARIC

Arithmetic and Computing

IN COLLABORATION WITH: Laboratoire de l'Informatique du Parallélisme (LIP)

RESEARCH CENTER
Grenoble - Rhône-Alpes

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Project-Team ARIC

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

Keywords:

Computer Science and Digital Science:

A1.1. - Architectures
A2.4. - Formal method for verification, reliability, certification
A4. - Security and privacy
A7. - Theory of computation
A8. - Mathematics of computing

Other Research Topics and Application Domains:

B9.5. - Sciences
B9.10. - Privacy

1. Team, Visitors, External Collaborators

Research Scientists

Bruno Salvy [Team leader, Inria, Senior Researcher]
Nicolas Brisebarre [CNRS, Researcher, HDR]
Claude-Pierre Jeannerod [Inria, Researcher]
Vincent Lefèvre [Inria, Researcher]
Benoît Libert [CNRS, Senior Researcher, HDR]
Jean-Michel Muller [CNRS, Senior Researcher, HDR]
Alain Passelègue [Inria, Researcher]
Nathalie Revol [Inria, Researcher]
Warwick Tucker [Inria, International Chair, Advanced Research Position]
Gilles Villard [CNRS, Senior Researcher, HDR]

Faculty Members

Guillaume Hanrot [École Normale Supérieure de Lyon, Professor, HDR]
Fabien Laguillaumie [Univ Claude Bernard, Professor, HDR]
Nicolas Louvet [Univ Claude Bernard, Associate Professor]
Damien Stehlé [École Normale Supérieure de Lyon, Professor, HDR]

Post-Doctoral Fellows

Chitchanok Chuengsatiansup [Inria, Post-Doctoral Fellow, until May 2019]
Alonso Gonzalez [École Normale Supérieure de Lyon, Post-Doctoral Fellow]
Dingding Jia [École Normale Supérieure de Lyon, Post-Doctoral Fellow, from Aug 2019]
Elena Kirshanova [École Normale Supérieure de Lyon, Post-Doctoral Fellow, until Jun 2019]
Changmin Lee [Univ de Lyon, Post-Doctoral Fellow]
Hervé Tale Kalachi [Inria, Post-Doctoral Fellow, from Apr 2019]
Anastasiia Volkova Lozanova [Inria, Post-Doctoral Fellow, until Feb 2019]

PhD Students

Florent Bréhard [École Normale Supérieure de Lyon, PhD Student, until Aug 2019]
Qian Chen [École normale supérieure de Rennes, PhD Student, until Aug 2019]
Adel Hamdi [Orange Labs, PhD Student, granted by CIFRE]
Huyen Nguyen [École Normale Supérieure de Lyon, PhD Student]
Alice Pellet–Mary [École Normale Supérieure de Lyon, PhD Student, until Oct 2019]

Miruna Rosca [Bitdefender, PhD Student]
Radu Titiu [Bitdefender, PhD Student]
Ida Tucker [École Normale Supérieure de Lyon, PhD Student]

Technical staff

Rikki Amit Inder Deo [Inria, Engineer, from Nov 2019]
Joris Picot [École Normale Supérieure de Lyon, part-time Engineer]

Administrative Assistants

Nelly Amsellem [École Normale Supérieure de Lyon, Administrative Assistant, until Sep 2019]
Virginie Bouyer [École Normale Supérieure de Lyon, Administrative Assistant, from Oct 2019]
Octavie Paris [École Normale Supérieure de Lyon, Administrative Assistant, from May 2019]

2. Overall Objectives

2.1. Overall Objectives

A major challenge in modeling and scientific computing is the simultaneous mastery of hardware capabilities, software design, and mathematical algorithms for the efficiency and reliability of the computation. In this context, the overall objective of AriC is to improve computing at large, in terms of performance, efficiency, and reliability. We work on the fine structure of floating-point arithmetic, on controlled approximation schemes, on algebraic algorithms and on new cryptographic applications, most of these themes being pursued in their interactions. Our approach combines fundamental studies, practical performance and qualitative aspects, with a shared strategy going from high-level problem specifications and standardization actions, to computer arithmetic and the lowest-level details of implementations.

This makes AriC the right place for drawing the following lines of action:

- Design and integration of new methods and tools for mathematical program specification, certification, security, and guarantees on numerical results. Some main ingredients here are: the interleaving of formal proofs, computer arithmetic and computer algebra; error analysis and computation of certified error bounds; the study of the relationship between performance and numerical quality; and on the cryptography aspects, focus on the practicality of existing protocols and design of more powerful lattice-based primitives.
- Generalization of a hybrid symbolic-numeric trend, and interplay between arithmetic for both improving and controlling numerical approaches (symbolic $\rightarrow$ numeric), and accelerating exact solutions (symbolic $\longleftarrow$ numeric). This trend, especially in the symbolic computation community, has acquired a strategic role for the future of scientific computing. The integration in AriC of computer arithmetic, reliable computing, and algebraic computing, is expected to lead to a deeper understanding of the problem and novel solutions.
- Mathematical and algorithmic foundations of computing. We address algorithmic complexity and fundamental aspects of approximation, polynomial and matrix algebra, and lattice-based cryptography. Practical questions concern the design of high performance and reliable computing kernels, thanks to optimized computer arithmetic operators and an improved adequacy between arithmetic bricks and higher level ones.

According to the application domains that we target and our main fields of expertise, these lines of actions are declined in three themes with specific objectives.

- **Efficient approximation methods (§3.1).** Here lies the question of interleaving formal proofs, computer arithmetic and computer algebra, for significantly extending the range of functions whose reliable evaluation can be optimized.
- **Lattices: algorithms and cryptography (§3.2).** Long term goals are to go beyond the current design paradigm in basis reduction, and to demonstrate the superiority of lattice-based cryptography over contemporary public-key cryptographic approaches.

- **Algebraic computing and high performance kernels (§3.3).** The problem is to keep the algorithm and software designs in line with the scales of computational capabilities and application needs, by simultaneously working on the structural and the computer arithmetic levels.

3. Research Program

3.1. Efficient and certified approximation methods

3.1.1. Safe numerical approximations

The last twenty years have seen the advent of computer-aided proofs in mathematics and this trend is getting more and more important. They request: fast and stable numerical computations; numerical results with a guarantee on the error; formal proofs of these computations or computations with a proof assistant. One of our main long-term objectives is to develop a platform where one can study a computational problem on all (or any) of these three levels of rigor. At this stage, most of the necessary routines are not easily available (or do not even exist) and one needs to develop *ad hoc* tools to complete the proof. We plan to provide more and more algorithms and routines to address such questions. Possible applications lie in the study of mathematical conjectures where exact mathematical results are required (e.g., stability of dynamical systems); or in more applied questions, such as the automatic generation of efficient and reliable numerical software for function evaluation. On a complementary viewpoint, numerical safety is also critical in robust space mission design, where guidance and control algorithms become more complex in the context of increased satellite autonomy. We will pursue our collaboration with specialists of that area whose questions bring us interesting focus on relevant issues.

3.1.2. Floating-point computing

Floating-point arithmetic is currently undergoing a major evolution, in particular with the recent advent of a greater diversity of available precisions on a same system (from 8 to 128 bits) and of coarser-grained floating-point hardware instructions. This new arithmetic landscape raises important issues at the various levels of computing, that we will address along the following three directions.

3.1.2.1. Floating-point algorithms, properties, and standardization

One of our targets is the design of building blocks of computing (e.g., algorithms for the basic operations and functions, and algorithms for complex or double-word arithmetic). Establishing properties of these building blocks (e.g., the absence of "spurious" underflows/overflows) is also important. The IEEE 754 standard on floating-point arithmetic (whose next version, a rather minor revision, will be released soon) will have to undergo a major revision within a few years: first because advances in technology or new needs make some of its features obsolete, and because new features need standardization. We aim at playing a leading role in the preparation of the next standard.

3.1.2.2. Error bounds

We will pursue our studies in rounding error analysis, in particular for the "low precision–high dimension" regime, where traditional analyses become ineffective and where improved bounds are thus most needed. For this, the structure of both the data and the errors themselves will have to be exploited. We will also investigate the impact of mixed-precision and coarser-grained instructions (such as small matrix products) on accuracy analyses.

3.1.2.3. High performance kernels

Most directions in the team are concerned with optimized and high performance implementations. We will pursue our efforts concerning the implementation of well optimized floating-point kernels, with an emphasis on numerical quality, and taking into account the current evolution in computer architectures (the increasing width of SIMD registers, and the availability of low precision formats). We will focus on computing kernels used within other axes in the team such as, for example, extended precision linear algebra routines within the FPLLL and HPLLL libraries.

3.2. Lattices: algorithms and cryptology

We intend to strengthen our assessment of the cryptographic relevance of problems over lattices, and to broaden our studies in two main (complementary) directions: hardness foundations and advanced functionalities.

3.2.1. Hardness foundations

Recent advances in cryptography have broaden the scope of encryption functionalities (e.g., encryption schemes allowing to compute over encrypted data or to delegate partial decryption keys). While simple variants (e.g., identity-based encryption) are already practical, the more advanced ones still lack efficiency. Towards reaching practicality, we plan to investigate simpler constructions of the fundamental building blocks (e.g., pseudorandom functions) involved in these advanced protocols. We aim at simplifying known constructions based on standard hardness assumptions, but also at identifying new sources of hardness from which simple constructions that are naturally suited for the aforementioned advanced applications could be obtained (e.g., constructions that minimize critical complexity measures such as the depth of evaluation). Understanding the core source of hardness of today's standard hard algorithmic problems is an interesting direction as it could lead to new hardness assumptions (e.g., tweaked version of standard ones) from which we could derive much more efficient constructions. Furthermore, it could open the way to completely different constructions of advanced primitives based on new hardness assumptions.

3.2.2. Cryptanalysis

Lattice-based cryptography has come much closer to maturity in the recent past. In particular, NIST has started a standardization process for post-quantum cryptography, and lattice-based proposals are numerous and competitive. This dramatically increases the need for cryptanalysis: Do the underlying hard problems suffer from structural weaknesses? Are some of the problems used easy to solve, e.g., asymptotically? Are the chosen concrete parameters meaningful for concrete cryptanalysis? In particular, how secure would they be if all the known algorithms and implementations thereof were pushed to their limits? How would these concrete performances change in case (full-fledged) quantum computers get built?

On another front, the cryptographic functionalities reachable under lattice hardness assumptions seem to get closer to an intrinsic ceiling. For instance, to obtain cryptographic multilinear maps, functional encryption and indistinguishability obfuscation, new assumptions have been introduced. They often have a lattice flavour, but are far from standard. Assessing the validity of these assumptions will be one of our priorities in the mid-term.

3.2.3. Advanced cryptographic primitives

In the design of cryptographic schemes, we will pursue our investigations on functional encryption. Despite recent advances, efficient solutions are only available for restricted function families. Indeed, solutions for general functions are either way too inefficient for pratical use or they rely on uncertain security foundations like the existence of circuit obfuscators (or both). We will explore constructions based on well-studied hardness assumptions and which are closer to being usable in real-life applications. In the case of specific functionalities, we will aim at more efficient realizations satisfying stronger security notions.

Another direction we will explore is multi-party computation via a new approach exploiting the rich structure of class groups of quadratic fields. We already showed that such groups have a positive impact in this field by designing new efficient encryption switching protocols from the additively homomorphic encryption we introduced earlier. We want to go deeper in this direction that raises interesting questions such as how to design efficient zero-knowledge proofs for groups of unknown order, how to exploit their structure in the context of 2-party cryptography (such as two-party signing) or how to extend to the multi-party setting.

In the context of the PROMETHEUS H2020 project, we will keep seeking to develop new quantum-resistant privacy-preserving cryptographic primitives (group signatures, anonymous credentials, e-cash systems, etc). This includes the design of more efficient zero-knowledge proof systems that can interact with lattice-based cryptographic primitives.

3.3. Algebraic computing and high performance kernels

The connections between algorithms for structured matrices and for polynomial matrices will continue to be developed, since they have proved to bring progress to fundamental questions with applications throughout computer algebra. The new fast algorithm for the bivariate resultant opens an exciting area of research which should produce improvements to a variety of questions related to polynomial elimination. Obviously, we expect to produce results in that area.

For definite summation and integration, we now have fast algorithms for single integrals of general functions and sequences and for multiple integrals of rational functions. The long-term objective of that part of computer algebra is an efficient and general algorithm for multiple definite integration and summation of general functions and sequences. This is the direction we will take, starting with single definite sums of general functions and sequences (leading in particular to a faster variant of Zeilberger's algorithm). We also plan to investigate geometric issues related to the presence of apparent singularities and how they seem to play a role in the complexity of the current algorithms.

4. Application Domains

4.1. Floating-point and Validated Numerics

Our expertise on validated numerics is useful to analyze and improve, and guarantee the quality of numerical results in a wide range of applications including:

- scientific simulation;
- global optimization;
- control theory.

Much of our work, in particular the development of correctly rounded elementary functions, is critical to the

- reproducibility of floating-point computations.

4.2. Cryptography, Cryptology, Communication Theory

Lattice reduction algorithms have direct applications in

- public-key cryptography;
- diophantine equations;
- communications theory.

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

Florent Bréhard, jointly with Mioara Joldes and Jean-Bernard Lasserre (CNRS LAAS) received the Distinguished paper award at ISSAC 2019 for *On Moment Problems with Holonomic Functions*.

Alice Pellet-Mary was an awardee of the L'Oréal-Unesco scholarship for Women and Science.

BEST PAPER AWARD:

[16]
F. BRÉHARD, M. JOLDES, J.-B. LASSERRE. *On Moment Problems with Holonomic Functions*, in "ISSAC 2019 - 44th International Symposium on Symbolic and Algebraic Computation", Pékin, China, July 2019, pp. 66-73, https://hal.archives-ouvertes.fr/hal-02006645

6. New Software and Platforms

6.1. FPLLL

KEYWORDS: Euclidean Lattices - Computer algebra system (CAS) - Cryptography

SCIENTIFIC DESCRIPTION: The fplll library is used or has been adapted to be integrated within several mathematical computation systems such as Magma, Sage, and PariGP. It is also used for cryptanalytic purposes, to test the resistance of cryptographic primitives.

FUNCTIONAL DESCRIPTION: fplll contains implementations of several lattice algorithms. The implementation relies on floating-point orthogonalization, and LLL is central to the code, hence the name.

It includes implementations of floating-point LLL reduction algorithms, offering different speed/guarantees ratios. It contains a 'wrapper' choosing the estimated best sequence of variants in order to provide a guaranteed output as fast as possible. In the case of the wrapper, the succession of variants is oblivious to the user.

It includes an implementation of the BKZ reduction algorithm, including the BKZ-2.0 improvements (extreme enumeration pruning, pre-processing of blocks, early termination). Additionally, Slide reduction and self dual BKZ are supported.

It also includes a floating-point implementation of the Kannan-Fincke-Pohst algorithm that finds a shortest non-zero lattice vector. For the same task, the GaussSieve algorithm is also available in fplll. Finally, it contains a variant of the enumeration algorithm that computes a lattice vector closest to a given vector belonging to the real span of the lattice.

- Author: Damien Stehlé
- Contact: Damien Stehlé
- URL: https://github.com/fplll/fplll

6.2. Gfun

generating functions package

KEYWORD: Symbolic computation

FUNCTIONAL DESCRIPTION: Gfun is a Maple package for the manipulation of linear recurrence or differential equations. It provides tools for guessing a sequence or a series from its first terms, for manipulating rigorously solutions of linear differential or recurrence equations, using the equation as a data-structure.

- Contact: Bruno Salvy
- URL: http://perso.ens-lyon.fr/bruno.salvy/software/the-gfun-package/

6.3. GNU-MPFR

KEYWORDS: Multiple-Precision - Floating-point - Correct Rounding

FUNCTIONAL DESCRIPTION: GNU MPFR is an efficient arbitrary-precision floating-point library with well-defined semantics (copying the good ideas from the IEEE 754 standard), in particular correct rounding in 5 rounding modes. It provides about 80 mathematical functions, in addition to utility functions (assignments, conversions...). Special data (Not a Number, infinities, signed zeros) are handled like in the IEEE 754 standard. GNU MPFR is based on the mpn and mpz layers of the GMP library.

- Participants: Guillaume Hanrot, Paul Zimmermann, Philippe Théveny and Vincent Lefèvre
- Contact: Vincent Lefèvre
- Publications: Correctly Rounded Arbitrary-Precision Floating-Point Summation - Optimized Binary64 and Binary128 Arithmetic with GNU MPFR - Évaluation rapide de fonctions hypergéométriques - Arbitrary Precision Error Analysis for computing $\zeta(s)$ with the Cohen-Olivier algorithm: Complete description of the real case and preliminary report on the general case - MPFR: A Multiple-Precision Binary Floating-Point Library with Correct Rounding. - The Generic Multiple-Precision Floating-Point Addition With Exact Rounding (as in the MPFR Library)
- URL: https://www.mpfr.org/

6.4. Sipe

KEYWORDS: Floating-point - Correct Rounding

FUNCTIONAL DESCRIPTION: Sipe is a mini-library in the form of a C header file, to perform radix-2 floating-point computations in very low precisions with correct rounding, either to nearest or toward zero. The goal of such a tool is to do proofs of algorithms/properties or computations of tight error bounds in these precisions by exhaustive tests, in order to try to generalize them to higher precisions. The currently supported operations are addition, subtraction, multiplication (possibly with the error term), fused multiply-add/subtract (FMA/FMS), and miscellaneous comparisons and conversions. Sipe provides two implementations of these operations, with the same API and the same behavior: one based on integer arithmetic, and a new one based on floating-point arithmetic.

- Participant: Vincent Lefèvre
- Contact: Vincent Lefèvre
- Publications: SIPE: Small Integer Plus Exponent - Sipe: a Mini-Library for Very Low Precision Computations with Correct Rounding
- URL: https://www.vinc17.net/research/sipe/

6.5. LinBox

KEYWORD: Exact linear algebra

FUNCTIONAL DESCRIPTION: LinBox is an open-source C++ template library for exact, high-performance linear algebra computations. It is considered as the reference library for numerous computations (such as linear system solving, rank, characteristic polynomial, Smith normal forms,...) over finite fields and integers with dense, sparse, and structured matrices.

- Participants: Clément Pernet and Thierry Gautier
- Contact: Clément Pernet
- URL: http://linalg.org/

6.6. HPLLL

KEYWORDS: Euclidean Lattices - Computer algebra system (CAS)

FUNCTIONAL DESCRIPTION: Software library for linear algebra and Euclidean lattice problems

- Contact: Gilles Villard
- URL: http://perso.ens-lyon.fr/gilles.villard/hplll/

7. New Results

7.1. Efficient approximation methods

7.1.1. Exchange algorithm for evaluation and approximation error-optimized polynomials

Machine implementation of mathematical functions often relies on polynomial approximations. The particularity is that rounding errors occur both when representing the polynomial coefficients on a finite number of bits, and when evaluating it in finite precision. Hence, for finding the best polynomial (for a given fixed degree, norm and interval), one has to consider both types of errors: approximation and evaluation. While efficient algorithms were already developed for taking into account the approximation error, the evaluation part is usually a posteriori handled, in an ad-hoc manner. In [15], we formulate a semi-infinite linear optimization problem whose solution is the best polynomial with respect to the supremum norm of the sum of both errors. This problem is then solved with an iterative exchange algorithm, which can be seen as an extension of the well-known Remez algorithm. A discussion and comparison of the obtained results on different examples are finally presented.

7.1.2. On Moment Problems with Holonomic Functions

Many reconstruction algorithms from moments of algebraic data were developed in optimization, analysis or statistics. Lasserre and Putinar proposed an exact reconstruction algorithm for the algebraic support of the Lebesgue measure, or of measures with density equal to the exponential of a known polynomial. Their approach relies on linear recurrences for the moments, obtained using Stokes theorem. In [16], we extend this study to measures with holonomic densities and support with real algebraic boundary. In the framework of holonomic distributions (i.e. they satisfy a holonomic system of linear partial or ordinary differential equations with polynomial coefficients), an alternate method to creative telescoping is proposed for computing linear recurrences for the moments. When the coefficients of a polynomial vanishing on the support boundary are given as parameters, the obtained recurrences have the advantage of staying linear with respect to them. This property allows for an efficient reconstruction method. Given a finite number of numerically computed moments for a measure with holonomic density, and assuming a real algebraic boundary for the support, we propose an algorithm for solving the inverse problem of obtaining both the coefficients of a polynomial vanishing on the boundary and those of the polynomials involved in the holonomic operators which annihilate the density.

7.1.3. A certificate-based approach to formally verified approximations

In [17], we present a library to verify rigorous approximations of univariate functions on real numbers, with the Coq proof assistant. Based on interval arithmetic, this library also implements a technique of validation a posteriori based on the Banach fixed-point theorem. We illustrate this technique on the case of operations of division and square root. This library features a collection of abstract structures that organize the specification of rigorous approximations, and modularize the related proofs. Finally, we provide an implementation of verified Chebyshev approximations, and we discuss a few examples of computations.

7.2. Floating-point and validated numerics

7.2.1. Error analysis of some operations involved in the Cooley-Tukey Fast Fourier Transform

We are interested in [4] in obtaining error bounds for the classical Cooley-Tukey FFT algorithm in floating-point arithmetic, for the 2-norm as well as for the infinity norm. For that purpose we also give some results on the relative error of the complex multiplication by a root of unity, and on the largest value that can take the real or imaginary part of one term of the FFT of a vector x, assuming that all terms of x have real and imaginary parts less than some value b.

7.2.2. Algorithms for triple-word arithmetic

Triple-word arithmetic consists in representing high-precision numbers as the unevaluated sum of three floating-point numbers (with “nonoverlapping” constraints that are explicited in the paper). We introduce and analyze in [7] various algorithms for manipulating triple-word numbers: rounding a triple-word number to a floating-point number, adding, multiplying, dividing, and computing square-roots of triple-word numbers, etc. We compare our algorithms, implemented in the Campary library, with other solutions of comparable accuracy. It turns out that our new algorithms are significantly faster than what one would obtain by just using the usual floating-point expansion algorithms in the special case of expansions of length 3.

7.2.3. Accurate Complex Multiplication in Floating-Point Arithmetic

We deal in [24] with accurate complex multiplication in binary floating-point arithmetic, with an emphasis on the case where one of the operands in a “double-word” number. We provide an algorithm that returns a complex product with normwise relative error bound close to the best possible one, i.e., the rounding unit u.

7.2.4. Semi-automatic implementation of the complementary error function

The normal and complementary error functions are ubiquitous special functions for any mathematical library. They have a wide range of applications. Practical applications call for customized implementations that have strict accuracy requirements. Accurate numerical implementation of these functions is, however, non-trivial. In particular, the complementary error function erfc for large positive arguments heavily suffers from cancellation, which is largely due to its asymptotic behavior. We provide a semi-automatic code generator for the erfc function which is parameterized by the user-given bound on the relative error. Our solution, presented in [31], exploits the asymptotic expression of erfc and leverages the automatic code generator Metalibm that provides accurate polynomial approximations. A fine-grained a priori error analysis provides a libm developer with the required accuracy for each step of the evaluation. In critical parts, we exploit double-word arithmetic to achieve implementations that are fast, yet accurate up to 50 bits, even for large input arguments. We demonstrate that for high required accuracies the automatically generated code has performance comparable to that of the standard libm and for lower ones our code demonstrated roughly 25% speedup.

7.2.5. Posits: the good, the bad and the ugly

Many properties of the IEEE-754 floating-point number system are taken for granted in modern computers and are deeply embedded in compilers and low-level softare routines such as elementary functions or BLAS. In [32] we review such properties on the recently proposed Posit number system. Some are still true. Some are no longer true, but sensible work-arounds are possible, and even represent exciting challenge for the community. Some, in particular the loss of scale invariance for accuracy, are extremely dangerous if Posits are to replace floating point completely. This study helps framing where Posits are better than floating-point, where they are worse, and what tools are missing in the Posit landscape. For general-purpose computing, using Posits as a storage format only could be a way to reap their benefits without loosing those of classical floating-point. The hardware cost of this alternative is studied.

7.2.6. The relative accuracy of $(x+y)*(x-y)$

We consider in [8] the relative accuracy of evaluating $(x+y)(x-y)$ in IEEE floating-point arithmetic, when x and y are two floating-point numbers and rounding is to nearest. This expression can be used for example as an efficient cancellation-free alternative to x^2-y^2 and is well known to have low relative error, namely, at most about $3u$ with u denoting the unit roundoff. In this paper we complement this traditional analysis with a finer-grained one, aimed at improving and assessing the quality of that bound. Specifically, we show that if the tie-breaking rule is *to away* then the bound $3u$ is asymptotically optimal. In contrast, if the tie-breaking rule is *to even*, we show that asymptotically optimal bounds are now $2.25u$ for base two and $2u$ for larger bases, such as base ten. In each case, asymptotic optimality is obtained by the explicit construction of a certificate, that is, some floating-point input (x, y) parametrized by u and such that the error of the associated result is equivalent to the error bound as $u \to 0$. We conclude with comments on how $(x+y)(x-y)$ compares with x^2 in the presence of floating-point arithmetic, in particular showing cases where the computed value of $(x+y)(x-y)$ exceeds that of x^2.

7.2.7. The MPFI Library: Towards IEEE 1788-2015 Compliance

The IEEE 1788-2015 has standardized interval arithmetic. However, few libraries for interval arithmetic are compliant with this standard. In the first part of [30], the main features of the IEEE 1788-2015 standard are detailed. These features were not present in the libraries developed prior to the elaboration of the standard. MPFI is such a library: it is a C library, based on MPFR, for arbitrary precision interval arithmetic. MPFI is not (yet) compliant with the IEEE 1788-2015 standard for interval arithmetic: the planned modifications are presented.

7.3. Lattices: algorithms and cryptology

7.3.1. Approx-SVP in ideal lattices with pre-processing

In [28], we describe an algorithm to solve the approximate Shortest Vector Problem for lattices corresponding to ideals of the ring of integers of an arbitrary number field K. This algorithm has a pre-processing phase, whose run-time is exponential in $\log |\Delta|$ with Δ the discriminant of K. Importantly, this pre-processing phase depends only on K. The pre-processing phase outputs an advice, whose bit-size is no more than the run-time of the query phase. Given this advice, the query phase of the algorithm takes as input any ideal I of the ring of integers, and outputs an element of I which is at most $\exp(\widetilde{O}((\log |\Delta|)^{\alpha+1}/n))$ times longer than a shortest non-zero element of I (with respect to the Euclidean norm of its canonical embedding). This query phase runs in time and space $\exp(\widetilde{O}((\log |\Delta|)^{\max(2/3,1-2\alpha)}))$ in the classical setting, and $\exp(\widetilde{O}((\log |\Delta|)^{1-2\alpha}))$ in the quantum setting. The parameter α can be chosen arbitrarily in $[0, 1/2]$. Both correctness and cost analyses rely on heuristic assumptions, whose validity is consistent with experiments.

The algorithm builds upon the algorithms from Cramer al. [EUROCRYPT 2016] and Cramer et al. [EUROCRYPT 2017]. It relies on the framework from Buchmann [Séminaire de théorie des nombres 1990], which allows to merge them and to extend their applicability from prime-power cyclotomic fields to all number fields. The cost improvements are obtained by allowing precomputations that depend on the field only.

7.3.2. An LLL algorithm for module lattices

The LLL algorithm takes as input a basis of a Euclidean lattice, and, within a polynomial number of operations, it outputs another basis of the same lattice but consisting of rather short vectors. In [23], we provide a generalization to R-modules contained in K^n for arbitrary number fields K and dimension n, with R denoting the ring of integers of K. Concretely, we introduce an algorithm that efficiently finds short vectors in rank-n modules when given access to an oracle that finds short vectors in rank-2 modules, and an algorithm that efficiently finds short vectors in rank-2 modules given access to a Closest Vector Problem oracle for a lattice that depends only on K. The second algorithm relies on quantum computations and its analysis is heuristic.

7.3.3. The general sieve kernel and new records in lattice reduction

In [14], we propose the General Sieve Kernel (G6K), an abstract stateful machine supporting a wide variety of lattice reduction strategies based on sieving algorithms. Using the basic instruction set of this abstract stateful machine, we first give concise formulations of previous sieving strategies from the literature and then propose new ones. We then also give a light variant of BKZ exploiting the features of our abstract stateful machine. This encapsulates several recent suggestions (Ducas at Eurocrypt 2018; Laarhoven and Mariano at PQCrypto 2018) to move beyond treating sieving as a blackbox SVP oracle and to utilise strong lattice reduction as preprocessing for sieving. Furthermore, we propose new tricks to minimise the sieving computation required for a given reduction quality with mechanisms such as recycling vectors between sieves, on-the-fly lifting and flexible insertions akin to Deep LLL and recent variants of Random Sampling Reduction.

Moreover, we provide a highly optimised, multi-threaded and tweakable implementation of this machine which we make open-source. We then illustrate the performance of this implementation of our sieving strategies by applying G6K to various lattice challenges. In particular, our approach allows us to solve previously unsolved instances of the Darmstadt SVP (151, 153, 155) and LWE (e.g. (75, 0.005)) challenges. Our solution for the SVP-151 challenge was found 400 times faster than the time reported for the SVP-150 challenge, the previous record. For exact SVP, we observe a performance crossover between G6K and FPLLL's state of the art implementation of enumeration at dimension 70.

7.3.4. Statistical zeroizing attack: cryptanalysis of candidates of BP obfuscation over GGH15 multilinear map

In [19], we present a new cryptanalytic algorithm on obfuscations based on GGH15 multilinear map. Our algorithm, statistical zeroizing attack, directly distinguishes two distributions from obfuscation while it follows the zeroizing attack paradigm, that is, it uses evaluations of zeros of obfuscated programs.

Our attack breaks the recent indistinguishability obfuscation candidate suggested by Chen et al. (CRYPTO'18) for the optimal parameter settings. More precisely, we show that there are two functionally equivalent branching programs whose CVW obfuscations can be efficiently distinguished by computing the sample variance of evaluations.

This statistical attack gives a new perspective on the security of the indistinguishability obfuscations: we should consider the shape of the distributions of evaluation of obfuscation to ensure security.

In other words, while most of the previous (weak) security proofs have been studied with respect to algebraic attack model or ideal model, our attack shows that this algebraic security is not enough to achieve indistinguishability obfuscation. In particular, we show that the obfuscation scheme suggested by Bartusek et al. (TCC'18) does not achieve the desired security in a certain parameter regime, in which their algebraic security proof still holds.

The correctness of statistical zeroizing attacks holds under a mild assumption on the preimage sampling algorithm with a lattice trapdoor. We experimentally verify this assumption for implemented obfuscation by Halevi et al. (ACM CCS'17).

7.3.5. *Cryptanalysis of the CLT13 multilinear map*

The reference [6] is the journal version of the Eurocrypt'15 article with the same title and authors.

7.3.6. *Multi-Client Functional Encryption for Linear Functions in the Standard Model from LWE*

Multi-client functional encryption (MCFE) allows ℓ clients to encrypt ciphertexts $\mathbf{C}_{t,1}, \mathbf{C}_{t,2}, ..., \mathbf{C}_{t,\ell}$ under some label. Each client can encrypt his own data X_i for a label t using a private encryption key ek_i issued by a trusted authority in such a way that, as long as all $\mathbf{C}_{t,i}$ share the same label t, an evaluator endowed with a functional key dk_f can evaluate $f(X_1, X_2, ..., X_\ell)$ without learning anything else on the underlying plaintexts X_i. Functional decryption keys can be derived by the central authority using the master secret key. Under the Decision Diffie-Hellman assumption, Chotard *et al.* (Asiacrypt 2018) recently described an adaptively secure MCFE scheme for the evaluation of linear functions over the integers. They also gave a decentralized variant (DMCFE) of their scheme which does not rely on a centralized authority, but rather allows encryptors to issue functional secret keys in a distributed manner. While efficient, their constructions both rely on random oracles in their security analysis. In [27], we build a standard-model MCFE scheme for the same functionality and prove it fully secure under adaptive corruptions. Our proof relies on the Learning-With-Errors (LWE) assumption and does not require the random oracle model. We also provide a decentralized variant of our scheme, which we prove secure in the static corruption setting (but for adaptively chosen messages) under the LWE assumption.

7.3.7. *Zero-Knowledge Elementary Databases with More Expressive Queries*

Zero-knowledge elementary databases (ZK-EDBs) are cryptographic schemes that allow a prover to commit to a set D of key-value pairs so as to be able to prove statements such as “x belongs to the support of D and D(x) = y” or “x is not in the support of D”. Importantly , proofs should leak no information beyond the proven statement and even the size of D should remain private. Chase et al. (Eurocrypt'05) showed that ZK-EDBs are implied by a special flavor of non-interactive commitment, called mercurial commitment, which enables efficient instantiations based on standard number theoretic assumptions. On the other hand, the resulting ZK-EDBs are only known to support proofs for simple statements like (non-)membership and value assignments. In [25], we show that mercurial commitments actually enable significantly richer queries. We show that, modulo an additional security property met by all known efficient constructions, they actually enable range queries over keys and values-even for ranges of super-polynomial size-as well as membership/non-membership queries over the space of values. Beyond that, we exploit the range queries to realize richer queries such as k-nearest neighbors and revealing the k smallest or largest records within a given range. In addition, we provide a new realization of trapdoor mercurial commitment from standard lattice asssumptions, thus obtaining the most expressive quantum-safe ZK-EDB construction so far.

7.3.8. *Lossy Algebraic Filters With Short Tags*

Lossy algebraic filters (LAFs) are function families where each function is parametrized by a tag, which determines if the function is injective or lossy. While initially introduced by Hofheinz (Eurocrypt 2013) as a technical tool to build encryption schemes with key-dependent message chosen-ciphertext (KDM-CCA) security, they also find applications in the design of robustly reusable fuzzy extractors. So far, the only known LAF family requires tags comprised of $\Theta(n^2)$ group elements for functions with input space $\mathbb{Z}_p$, where p is the group order. In [26], we describe a new LAF family where the tag size is only linear in n and prove it secure under simple assumptions in asymmetric bilinear groups. Our construction can be used as a drop-in replacement in all applications of the initial LAF system. In particular, it can shorten the ciphertexts of Hofheinz's KDM-CCA-secure public-key encryption scheme by 19 group elements. It also allows substantial space improvements in a recent fuzzy extractor proposed by Wen and Liu (Asiacrypt 2018). As a second contribution , we show how to modify our scheme so as to prove it (almost) tightly secure, meaning that security reductions are not affected by a concrete security loss proportional to the number of adversarial queries.

7.3.9. Shorter Quadratic QA-NIZK Proofs

Despite recent advances in the area of pairing-friendly Non-Interactive Zero-Knowledge proofs, there have not been many efficiency improvements in constructing arguments of satisfiability of quadratic (and larger degree) equations since the publication of the Groth-Sahai proof system (J. of Cryptology 2012). In [20], we address the problem of aggregating such proofs using techniques derived from the interactive setting and recent constructions of SNARKs. For certain types of quadratic equations, this problem was investigated before by González et al. (Asiacrypt'15). Compared to their result, we reduce the proof size by approximately 50

7.3.10. Shorter Pairing-based Arguments under Standard Assumptions

The paper [22] constructs efficient non-interactive arguments for correct evaluation of arithmetic and Boolean circuits with proof size $O(d)$ group elements, where d is the multiplicative depth of the circuit, under falsifiable assumptions. This is achieved by combining techniques from SNARKs and QA-NIZK arguments of membership in linear spaces. The first construction is very efficient (the proof size is $\approx 4d$ group elements and the verification cost is $4d$ pairings and $O(n + n + d)$ exponentiations, where n is the size of the input and n of the output) but one type of attack can only be ruled out assuming the knowledge soundness of QA-NIZK arguments of membership in linear spaces. We give an alternative construction which replaces this assumption with a decisional assumption in bilinear groups at the cost of approximately doubling the proof size. The construction for Boolean circuits can be made zero-knowledge with Groth-Sahai proofs, resulting in a NIZK argument for circuit satisfiability based on falsifiable assumptions in bilinear groups of proof size $O(n + d)$. Our main technical tool is what we call an "argument of knowledge transfer". Given a commitment C_1 and an opening x, such an argument allows to prove that some other commitment C_2 opens to $f(x)$, for some function f, even if C_2 is not extractable. We construct very short, constant-size, pairing-based arguments of knowledge transfer with constant-time verification for any linear function and also for Hadamard products. These allow to transfer the knowledge of the input to lower levels of the circuit.

7.3.11. Shorter Ring Signatures from Standard Assumptions

Ring signatures, introduced by Rivest, Shamir and Tauman (ASIACRYPT 2001), allow to sign a message on behalf of a set of users while guaranteeing authenticity and anonymity. Groth and Kohlweiss (EUROCRYPT 2015) and Libert *et al.* (EUROCRYPT 2016) constructed schemes with signatures of size logarithmic in the number of users. An even shorter ring signature, of size independent from the number of users, was recently proposed by Malavolta and Schroeder (ASIACRYPT 2017). However, all these short signatures are obtained relying on strong and controversial assumptions. Namely, the former schemes are both proven secure in the random oracle model while the later requires non-falsifiable assumptions.

The most efficient construction under mild assumptions remains the construction of Chandran et al. (ICALP 2007) with a signature of size $\Theta(\sqrt{n})$, where n is the number of users, and security is based on the Diffie-Hellman assumption in bilinear groups (the SXDH assumption in asymmetric bilinear groups).

In [21], we construct an asymptotically shorter ring signature from the hardness of the Diffie-Hellman assumption in bilinear groups. Each signature comprises $\Theta(n^{1/3})$ group elements, signing a message requires computing $\Theta(n^{1/3})$ exponentiations, and verifying a signature requires $\Theta(n^{2/3})$ pairing operations.

7.3.12. Two-Party ECDSA from Hash Proof Systems and Efficient Instantiations

ECDSA is a widely adopted digital signature standard. Unfortunately, efficient distributed variants of this primitive are notoriously hard to achieve and known solutions often require expensive zero knowledge proofs to deal with malicious adversaries. For the two party case, Lindell (CRYPTO 2017) recently managed to get an efficient solution which, to achieve simulation-based security, relies on an interactive, non standard, assumption on Paillier's cryptosystem.

In this paper [18] we generalize Lindell's solution using hash proof systems. The main advantage of our generic method is that it results in a simulation-based security proof without resorting to non-standard interactive assumptions.

Moving to concrete constructions, we show how to instantiate our framework using class groups of imaginary quadratic fields. Our implementations show that the practical impact of dropping such interactive assumptions is minimal. Indeed, while for 128-bit security our scheme is marginally slower than Lindell's, for 256-bit security it turns out to be better both in key generation and signing time. Moreover, in terms of communication cost, our implementation significantly reduces both the number of rounds and the transmitted bits without exception.

7.3.13. Algebraic XOR-RKA-Secure Pseudorandom Functions from Post-Zeroizing Multilinear Maps

In [13], we construct the first pseudorandom functions that resist a strong class of attacks where an adversary is able to run the cryptosystem not only with the fixed secret key, but with related keys where bits of its choice of the original keys are flipped. This problem is motivated by practical attacks that have been performed against physical devices. Our construction guarantees that every output of our construction, for the original key or for tampered keys, are pseudorandom, i.e. are computationally hard to distinguish from truly random values. To achieve this, we rely on a recent tool introduced in cryptography and termed multilinear maps. While multilinear maps have been recently attacked by several techniques, we prove that our construction remains secure despite the numerous vulnerabilities of current constructions of multilinear maps.

7.3.14. Unifying Leakage Models on a Rényi Day

Most theoretical models in cryptography suppose that an attacker can only observe the input/output behavior of a cryptosystem and nothing more. Yet, in the real world, cryptosystems run on physical devices and auxiliary information leaks from these devices. This leakage can sometimes be used to attack the system, even though it is proven secure in theory. To circumvent these issues, cryptographers have introduces several new security models in an attempt to encompass the different forms of leakage. Some models are simple, such as the probing model, and simple compilers allow to transform a system into one secure in the probing model, while some more realistic problems such as the noisy-leakage model are very involved. In [29], we show that these models are actually equivalent, proving in particular that the simple compilers are sufficient to guarantee security in realistic environments.

7.4. Algebraic computing and high-performance kernels

7.4.1. Linear differential equations as a data-structure

A lot of information concerning solutions of linear differential equations can be computed directly from the equation. It is therefore natural to consider these equations as a data-structure, from which mathematical properties can be computed. A variety of algorithms has thus been designed in recent years that do not aim at "solving", but at computing with this representation. Many of these results are surveyed in [11].

7.4.2. Absolute root separation

The absolute separation of a polynomial is the minimum nonzero difference between the absolute values of its roots. In the case of polynomials with integer coefficients, it can be bounded from below in terms of the degree and the height (the maximum absolute value of the coefficients) of the polynomial. We improve the known bounds for this problem and related ones. Then we report on extensive experiments in low degrees, suggesting that the current bounds are still very pessimistic. [5]

7.4.3. Improving the complexity of block low-rank factorizations with fast matrix arithmetic

We consider in [9] the LU factorization of an $n \times n$ matrix represented as a block low-rank (BLR) matrix: most of its off-diagonal blocks are approximated by matrices of small rank r, which reduces the asymptotic complexity of computing the LU factorization down to $\mathcal{O}(n^2 r)$. Even though lower complexities can be achieved with hierarchical matrices, the BLR format allows for a very simple and efficient implementation. In this article, our aim is to further reduce the BLR complexity without losing its nonhierarchical nature by exploiting fast matrix arithmetic, that is, the ability to multiply two $n \times n$ full-rank matrices together for $\mathcal{O}(n^\omega)$ flops, where $\omega < 3$. We devise a new BLR factorization algorithm whose cost is $\mathcal{O}(n^{(\omega+1)/2} r^{(\omega-1)/2})$, which represents an asymptotic improvement compared with the standard BLR factorization as soon as $\omega < 3$. In particular, for Strassen's algorithm, $\omega \approx 2.81$ yields the cost $\mathcal{O}(n^{1.904} r^{0.904})$. Our numerical experiments are in good agreement with this analysis.

7.4.4. Fast computation of approximant bases in canonical form

In [10] we design fast algorithms for the computation of approximant bases in shifted Popov normal form. For K a commutative field, let F be a matrix in $\mathsf{K}[x]^{m \times n}$ (truncated power series) and $\vec{d}$ be a degree vector, the problem is to compute a basis $P \in \mathsf{K}[x]^{m \times m}$ of the $\mathsf{K}[x]$-module of the relations $p \in \mathsf{K}[x]^{1 \times m}$ such that $p(x) \cdot F(x) \equiv 0 \bmod x^{\vec{d}}$. We obtain improved complexity bounds for handling arbitrary (possibly highly unbalanced) vectors $\vec{d}$. We also improve upon previously known algorithms for computing P in normalized shifted form for an arbitrary shift. Our approach combines a recent divide and conquer strategy which reduces the general case to the case where information on the output degree is available, and partial linearizations of the involved matrices.

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

Bosch (Germany) ordered from us some support for implementing complex numerical algorithms (participants: Claude-Pierre Jeannerod and Jean-Michel Muller).

8.2. Bilateral Grants with Industry

- Miruna Rosca and Radu Titiu are employees of BitDefender. Their PhD's are supervised by Damien Stehlé and Benoît Libert, respectively. Miruna Rosca works on the foundations of lattice-based cryptography, and Radu Titiu works on pseudo-random functions and functional encryption.
- Adel Hamdi is doing is PhD with Orange Labs and is supervised by Fabien Laguillaumie. He is working on advanced encryption protocols for the cloud.

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR FastRelax Project

Participants: Nicolas Brisebarre, Guillaume Hanrot, Vincent Lefèvre, Jean-Michel Muller, Bruno Salvy.

FastRelax stands for "Fast and Reliable Approximation". It is a four year ANR project (started in October 2014 and extended till September 2019). The web page of the project is http://fastrelax.gforge.inria.fr/. It is headed by B. Salvy and involves AriC as well as members of the Marelle Team (Sophia), of the Mac group (LAAS, Toulouse), of the Specfun and Toccata Teams (Saclay), as well as of the Pequan group in UVSQ and a colleague in the Plume group of LIP.

The aim of this project is to develop computer-aided proofs of numerical values, with certified and reasonably tight error bounds, without sacrificing efficiency. Applications to zero-finding, numerical quadrature or global optimization can all benefit from using our results as building blocks. We expect our work to initiate a “fast and reliable” trend in the symbolic-numeric community. This will be achieved by developing interactions between our fields, designing and implementing prototype libraries and applying our results to concrete problems originating in optimal control theory.

9.1.2. ANR ALAMBIC Project

Participants: Benoît Libert, Fabien Laguillaumie, Ida Tucker.

ALAMBIC is a four-year project (started in October 2016) focused on the applications of cryptographic primitives with homomorphic or malleability properties. The web page of the project is https://crypto.di.ens.fr/projects:alambic:description. It is headed by Damien Vergnaud (ENS Paris and CASCADE team) and, besides AriC, also involves teams from the XLIM laboratory (Université de Limoges) and the CASCADE team (ENS Paris). The main goals of the project are: (i) Leveraging the applications of malleable cryptographic primitives in the design of advanced cryptographic protocols which require computations on encrypted data; (ii) Enabling the secure delegation of expensive computations to remote servers in the cloud by using malleable cryptographic primitives; (iii) Designing more powerful zero-knowledge proof systems based on malleable cryptography.

9.1.3. RISQ Project

Participants: Chitchanok Chuengsatiansup, Rikki Amit Inder Deo, Hervé Tale Kalachi, Fabien Laguillaumie, Benoît Libert, Damien Stehlé.

RISQ (Regroupement de l’Industrie française pour la Sécurité Post – Quantique) is a BPI-DGE four-year project (started in January 2017) focused on the transfer of post-quantum cryptography from academia to industrial poducts. The web page of the project is http://risq.fr. It is headed by Secure-IC and, besides AriC, also involves teams from ANSSI (Agence Nationale de la Sécurité des Systèmes d’Information), Airbus, C& S (Communication et Systèmes), CEA (CEA-List), CryptoExperts, Gemalto, Orange, Thales Communications & Security, Paris Center for Quantum Computing, the EMSEC team of IRISA, and the Cascade and Polsys Inria teams. The outcome of this project will include an exhaustive encryption and transaction signature product line, as well as an adaptation of the TLS protocol. Hardware and software cryptographic solutions meeting these constraints in terms of security and embedded integration will also be included. Furthermore, documents guiding industrials on the integration of these post-quantum technologies into complex systems (defense, cloud, identity and payment markets) will be produced, as well as reports on the activities of standardization committees.

9.2. European Initiatives

9.2.1. PROMETHEUS Project

Participants: Fabien Laguillaumie, Benoît Libert, Octavie Paris, Damien Stehlé.

PROMETHEUS (Privacy-Preserving Systems from Advanced Cryptographic Mechanisms Using Lattices) is a 4-year European H2020 project (call H2020-DS-2016-2017, Cybersecurity PPP Cryptography, DS-06-2017) that started in January 2018. It gathers 8 academic partners (ENS de Lyon and Université de Rennes 1; CWI, Pays-Bas; IDC Herzliya, Israel; Royal Holloway University of London, United Kingdom; Universitat Politècnica de Catalunya, Spain; Ruhr-Universität Bochum, Germany; Weizmann Institute, Israel), 4 industrial partners (Orange, Thales, TNO, Scytl). The goal of this project is to develop a toolbox of privacy-preserving cryptographic algorithms and protocols (like group signatures, anonymous credentials, or digital cash systems) that resist quantum adversaries. Solutions will be mainly considered in the context of Euclidean lattices and they will be analyzed from a theoretical point of view (i.e., from a provable security aspect) and a practical angle (which covers the security of cryptographic implementations and side-channel leakages). The project is hosted by ENS de Lyon and Benoît Libert is the administrative coordinator while Orange is the scientific leader.

9.3. International Initiatives

9.3.1. Participation in Other International Programs

9.3.1.1. IFCPAR grant: "Computing on Encrypted Data: New Paradigms in Functional Encryption"

Participants: Benoît Libert, Damien Stehlé.

3-year project accepted in July 2018. Expected beginning on January 1, 2019. Benoît Libert is co-PI with Shweta Agrawal (IIT Madras, India). Budget on the French side amounts to 100k€.

Functional encryption is a paradigm that enables users to perform data mining and analysis on encrypted data. Users are provided cryptographic keys corresponding to particular functionalities which enable them to learn the output of the computation without learning anything about the input. Despite recent advances, efficient realizations of functional encryption are only available for restricted function families, which are typically represented by small-depth circuits: indeed, solutions for general functionalities are either way too inefficient for pratical use or they rely on uncertain security foundations like the existence of circuit obfuscators (or both). This project will explore constructions based on well-studied hardness assumptions and which are closer to being usable in real-life applications. To this end, we will notably consider solutions supporting other models of computation than Boolean circuits – like Turing machines – which support variable-size inputs. In the context of particular functionalities, the project will aim for more efficient realizations that satisfy stronger security notions.

9.3.1.2. Inria International Chairs

- **TUCKER Warwick**
- Department of Mathematics - Uppsala University - Sweden
- Title: Attracteur de Hénon et intégrales abéliennes liées aux 16e problème de Hilbert
- 2018 – 2022

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Ron Steinfeld, Monash University (June)
- Amin Sakzad, Monash University (June)
- Shi Bai, Florida Atlantic University (June and July)
- David Wu, University of Virginia (July)
- Olivier Bernard, Université Rennes 1 and Thalès (October and November)
- Gautier Eberhart, Université Rennes 1 (October and November)
- Federico Savasta, Università degli Studi di Catania (October)

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events: Organisation

- Damien Stehlé organized a Winter School on the mathematical foundations of public-key cryptography, in Aussois (France), from March 17 to March 22.
- Bruno Salvy was a co-chair of AofA'2019 (Analysis of Algorithms), in Luminy, France.

10.1.2. Scientific Events: Selection

- Elena Kirshanova was in the program committee of Asiacrypt 2019.

- Benoît Libert was in the program committees of PKC 2019 and PKC 2020.
- Nathalie Revol is in the steering committee of the Arith conference series. She was in the program committee of Arith'26, of Correctness 2019 (workshop of SuperComputing) and of PPAM (Parallel Processing and Applied Mathematics) 2019.
- Bruno Salvy is in the steering committee of AofA. He was in the program committee for FPSAC 2019 and in the scientific committee of OPSFA 2019. He is in the program committee for AofA 2020.
- Damien Stehlé is in the steering committee of the PQCrypto conference series. He was in the program committee PQCrypto 2019 and is in the program committee of PQCrypto 2020. He was in the program committee of CRYPTO 2019.
- Gilles Villard was in the program committee of ISSAC 2019.

10.1.3. Journal

- Benoît Libert was a member of the editorial board of IET Information Security until July 31, 2019.
- Jean-Michel Muller is associate editor in chief of the IEEE Transactions on Emerging Topics in Computing.
- Nathalie Revol is a member of the editorial board of Reliable Computing.
- Bruno Salvy and Gilles Villard are members of the editorial board of Journal of Symbolic Computation.
- Bruno Salvy is a member of the editorial board of the collection *Text and Monographs in Symbolic Computation* (Springer) and of the journal *Annals of Combinatorics*.
- Damien Stehlé is a member of the editorial board of Journal of Cryptology.

10.1.4. Invited Talks

- Claude-Pierre Jeannerod gave an invited talk at the workshop *Structured Matrix Days* (Limoges, May 23–24, 2019).
- Benoît Libert gave an invited presentation during the "Workshop on Modern Trends in Cryptography" organized at Nanyang Technological University (Singapore) on June 13-14, 2019.
- Damien Stehlé gave lectures during the "Euclidean lattices: theory and applications" Summer school that was held in Kaliningrad (Russia), from July 15 to July 19.

10.1.5. Leadership within the Scientific Community

- Guillaume Hanrot was a member of selection committees for professors at Université de Lorraine (in CS) and at Université de Nouvelle-Calédonie (in Mathematics). He was also in the hiring committee of the computer science department of École polytechnique. He is a member of the working group on the revision of the CS curriculum in *Classes préparatoires aux grandes écoles*.
- Claude-Pierre Jeannerod is a member of the scientific committee of JNCF (Journées Nationales de Calcul Formel). He is also a member of the recruitment committee for postdocs and sabbaticals at Inria Grenoble–Rhône-Alpes.
- Jean-Michel Muller is co-head of the GDR Informatique Mathématique of the CNRS. He is also a member of the Scientific Council of CERFACS (Toulouse).
- Alain Passelègue is a member of the steering committee of the *Groupe de Travail Codage et Cryptographie* (GT-C2) of the GDR-IM.
- Nathalie Revol is a member of the steering committee of GDR Calcul; she was a member of the hiring committee (Comité de Sélection) for 2 positions at U. Nantes.
- Bruno Salvy is a member of the scientific councils of the CIRM, Luminy and of the GDR Informatique Mathématique of the CNRS.

10.1.6. Scientific Expertise

- Nathalie Revol has been an expert for the European H2020 program.

10.1.7. Research Administration

- Jean-Michel Muller is a member of the *Commission Administrative Paritaire* (CAP) *Directeurs de Recherches* of CNRS.
- Gilles Villard is a member of the Section 6 of the *Comité national de la recherche scientifique*.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

- Master: Guillaume Hanrot, Computer algebra, 10h, ENS de Lyon, France
- Master: Guillaume Hanrot, Cryptanalysis, 15h, ENS de Lyon, France
- Master: Claude-Pierre Jeannerod, Computer Algebra, 18h, M2Pro ISFA (Institut de Science Financière et d'Assurances), Université Claude Bernard Lyon 1, France
- Master (1&2): Fabien Laguillaumie, Cryptography, 160 h, ISFA, UCBL, France
- Master: Benoît Libert, Advanced Topics in Cryptography, 15h, ENS de Lyon, France
- Master: Nicolas Louvet, Compilers, 22h, M1, UCB Lyon 1, France
- Master: Alain Passelègue, Computer Algebra, 10h, M1, ENS de Lyon, France
- Master: Alain Passelègue, Advanced Topics in Cryptography, 30h, M2, ENS de Lyon, France
- Master: Nathalie Revol, Numerical Algorithms and Reliability, 12h, M2Pro ISFA (Institut de Science Financière et d'Assurances), Université Claude Bernard Lyon 1, France
- Master: Bruno Salvy, Computer Algebra, 6h, ENS de Lyon, France
- Master: Bruno Salvy, Logic and Complexity, 32h, École polytechnique, France
- Master: Damien Stehlé, Cryptanalysis, 15h, ENS de Lyon, France
- Master : Gilles Villard, Computer Algebra, 8h, ENS de Lyon, France
- Bachelor: Guillaume Hanrot, Calculability and complexity, 32h, ENS de Lyon, France
- Bachelor: Nicolas Louvet, Computer Architecture, 27h, L1, UCB Lyon 1, France
- Bachelor: Nicolas Louvet, Operating Systems, 50h, L2, UCB Lyon 1, France
- Bachelor: Nicolas Louvet, Data Structures and Algorithms, 24h, L2, UCB Lyon 1, France
- Bachelor: Nicolas Louvet, Data Structures and Algorithms, 40h, L3, UCB Lyon 1, France
- Bachelor: Nicolas Louvet, Formal Languages, 15h, L3, UCB Lyon 1, France
- Bachelor: Nicolas Louvet, Classical Logic, 15h, L3, UCB Lyon 1, France
- Bachelor: Bruno Salvy, Design and Analysis of Algorithms, 20h, École polytechnique, France

10.2.2. Supervision

- PhD: Florent Bréhard, Certified Numerics in Function Spaces: Polynomial Approximations Meet Computer Algebra and Formal Proof, ENS de Lyon, July 12, Nicolas Brisebarre (co-supervision with Mioara Joldes, CNRS LAAS, and Damien Pous, LIP)
- PhD: Alice Pellet-Mary, On ideal lattices and the GGH13 multilinear map, ENS de Lyon, October 16, Damien Stehlé
- PhD: Chen Qian, Lossy Trapdoor Primitives, Zero-Knowledge Proofs and Applications, IRISA Rennes, October 4, Benoît Libert (co-supervision with Pierre-Alain Fouque, IRISA)
- PhD in progress: Miruna Rosca, The middle-product learning with errors problem, January 2017, Damien Stehlé

- PhD in progress: Huyen Nguyen, Cryptographic aspects of orthogonal lattices, September 2018, Damien Stehlé
- PhD in progress: Radu Titiu, Advanced cryptographic primitives based on standard assumptions, January 2017, Benoît Libert
- PhD in progress: Adel Hamdi, Functional Encryption, December 2017, Fabien Laguillaumie (co-supervised by Sébastien Canard, Orange)
- PhD in progress: Ida Tucker, Advanced cryptographic primitives from homomorphic encryption, October 2017, Fabien Laguillaumie (co-direction with Guilhem Castagnos, Université de Bordeaux)

10.2.3. Juries

- Damien Stehlé was a jury member for the PhD defences of Ilia Iliashenko (K.U. Leuven, Belgium) and Joost Rijneveld (Radboud U., the Netherlands) and for the habilitation defence of Omar Fawzi (ENS de Lyon). He was a reviewer and jury member of the PhD of Thomas Debris-Alazard (Sorbonne U.) and for the habilitation of Guilhem Castagnos (U. Bordeaux).
- Benoît Libert was a reviewer for the PhD theses of Romain Gay (ENS Paris), Jérémy Chotard (Univ. of Limoges). He was a PhD examiner for the thesis of Andrea Cerulli (University College London, United Kingdom). He also chaired the PhD committee of Anca Nitulescu (ENS Paris).
- Fabien Laguillaumie was reviewer and jury member of the PhD of Pauline Bert (Université de Rennes) and of the HDR of Olivier Blazy (Université de Limoges)
- Jean-Michel Muller was reviewer and jury member of the PhD of Clothilde Jeangoudoux (Sorbonne University, Paris)
- Gilles Villard was reviewer for the PhD thesis of Robin Larrieu (Université Paris-Saclay); examiner for the habilitation of Pascal Giorgi (Université de Montpellier) and the PhD thesis of Matías Bender (Sorbonne Université).

10.3. Popularization

10.3.1. Internal or external Inria responsibilities

- Nathalie Revol was in the scientific committee for the Journées Scientifiques Inria (Lyon, 5-7 June 2019).
- Nathalie Revol was a member of the editorial committee of interstices; she is the scientific editor of this Web magazine since September 2019.
- Nathalie Revol belonged to the steering committee of MMI (Maison des Mathématiques et de l'Informatique) until July 2019; she is now a member of its prospective committee.
- Bruno Salvy is “référent chercheur” for the Inria Grenoble Center.

10.3.2. Articles and contents

Nathalie Revol belonged to the working group that elaborated the "7 families of computer science" playcards, launched in February 2019.

10.3.3. Education

- Nathalie Revol taught "Dissemination of Scientific Knowledge", 10h, to the 4th year students (between Master and PhD) of ENS de Lyon, France.
- Nathalie Revol works with DANE (Délégation Académique au Numérique dans l'Éducation) of Rectorat de Lyon towards educating primary school teachers, by educating educators (e-RUN); she is a member of the Conseil Scientifique du Numérique.
- Nathalie Revol presented activities for teaching computer science at every school level, and in particular activities led by Inria, for a Taiwanese delegation (Grenoble, October 2019).

10.3.4. Interventions

- Nathalie Revol spent 2 days at école Guilloux, with 50 pupils aged 10 (level: CM2), to teach computer science without any computer (so-called "unplugged computer science"): data, algorithms, networks.
- For high-school pupils ($\simeq$ 150 pupils): as an incentive, especially for girls, to choose scientific careers, Nathalie Revol gave talks at Mondial des Métiers (in February 2019), collège Jean Zay (Brignais, March 2019) and Girls Can Code (Lyon, August 2019). With Jérôme Germoni and Natacha Portier, she organized a day *Filles & Info* in November 2019, gathering about 70 high-school girls of 1e and Terminale.
- For a larger audience: she took part to Pop Science, doing magic tricks in the street at La Duchère, Lyon, May 2019; with Florent Masséglia, she introduced 5 important figures of computer science, chosen among the personalities of the "7 families of computer science" playcard, for L'Esprit Sorcier, for la Fête de la Science, Paris, October 2019, cf https://www.youtube.com/watch?v=ypnQe91Pztc
- Nathalie Revol took part to a day of teaching unplugged computer science for whoever was interested, at La Gaîté Lyrique, Paris, June 2019.

10.3.5. Creation of media or tools for science outreach

Nathalie Revol belongs to the working group "Informatique Sans Ordinateur", which creates unplugged activities to teach computer science; this group meets twice a year, usually in Lyon.

11. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] F. BRE´HARD. *Calcul numérique certifié dans les espaces fonctionnels : Un trilogue entre approximations polynomiales rigoureuses, calcul symbolique et preuve formelle*, Université de Lyon, July 2019, https://tel.archives-ouvertes.fr/tel-02337901

[2] A. PELLET-MARY. *On ideal lattices and the GGH13 multilinear map*, Université de Lyon, October 2019, https://tel.archives-ouvertes.fr/tel-02337930

[3] C. QIAN. *Lossy trapdoor primitives, zero-knowledge proofs and applications*, Université de Rennes 1, October 2019, https://hal.archives-ouvertes.fr/tel-02415243

Articles in International Peer-Reviewed Journals

[4] N. BRISEBARRE, M. JOLDES, J.-M. MULLER, A.-M. NANEŞ, J. PICOT. *Error analysis of some operations involved in the Cooley-Tukey Fast Fourier Transform*, in "ACM Transactions on Mathematical Software", 2019, pp. 1-34, forthcoming [*DOI :* 10.1145/NNNNNNN.NNNNNNN], https://hal.archives-ouvertes.fr/hal-01949458

[5] Y. BUGEAUD, A. DUJELLA, W. FANG, T. PEJKOVIĆ, B. SALVY. *Absolute root separation*, in "Experimental Mathematics", 2019, 8 p. , https://arxiv.org/abs/1907.01232 , forthcoming [*DOI :* 10.1080/10586458.2019.1699480], https://hal.archives-ouvertes.fr/hal-02185594

[6] J. H. CHEON, K. HAN, C. LEE, H. RYU, D. STEHLÉ. *Cryptanalysis of the CLT13 Multilinear Map*, in "Journal of Cryptology", April 2019, vol. 32, n^{o} 2, pp. 547-565 [*DOI :* 10.1007/S00145-018-9307-Y], https://hal.archives-ouvertes.fr/hal-02397396

[7] N. Fabiano, J.-M. Muller, J. Picot. *Algorithms for triple-word arithmetic*, in "IEEE Transactions on Computers", November 2019, vol. 68, n^{o} 11, pp. 1573-1583 [*DOI :* 10.1109/TC.2019.2918451], https://hal.archives-ouvertes.fr/hal-01869009

[8] C.-P. Jeannerod. *The relative accuracy of* $(x + y) * (x - y)$, in "Journal of Computational and Applied Mathematics", 2019, pp. 1-17, forthcoming, https://hal.inria.fr/hal-02100500

[9] C.-P. Jeannerod, T. Mary, C. Pernet, D. S. Roche. *Improving the Complexity of Block Low-Rank Factorizations with Fast Matrix Arithmetic*, in "SIAM Journal on Matrix Analysis and Applications", November 2019, vol. 40, n^{o} 4, pp. 1478-1496 [*DOI :* 10.1137/19M1255628], https://hal.inria.fr/hal-02008666

[10] C.-P. Jeannerod, V. Neiger, G. Villard. *Fast computation of approximant bases in canonical form*, in "Journal of Symbolic Computation", 2019, pp. 1-33, forthcoming [*DOI :* 10.1016/j.jsc.2019.07.011], https://hal-unilim.archives-ouvertes.fr/hal-01683632

[11] B. Salvy. *Linear Differential Equations as a Data-Structure*, in "Foundations of Computational Mathematics", October 2019, vol. 19, n^{o} 5, pp. 1071-1112, https://arxiv.org/abs/1811.08616 - Based on an invited talk at FoCM'2017 [*DOI :* 10.1007/s10208-018-09411-x], https://hal.inria.fr/hal-01940078

[12] A. Volkova, T. Hilaire, C. Lauter. *Arithmetic approaches for rigorous design of reliable Fixed-Point LTI filters*, in "IEEE Transactions on Computers", 2019, pp. 1-14, forthcoming [*DOI :* 10.1109/TC.2019.2950658], https://hal.archives-ouvertes.fr/hal-01918650

International Conferences with Proceedings

[13] M. Abdalla, F. Benhamouda, A. Passelègue. *Algebraic XOR-RKA-Secure Pseudorandom Functions from Post-Zeroizing Multilinear Maps*, in "Advances in Cryptology – ASIACRYPT 2019", Kobe, Japan, S. D. Galbraith, S. Moriai (editors), Lecture Notes in Computer Science, November 2019, vol. 11922, pp. 386-412 [*DOI :* 10.1007/978-3-030-34621-8_14], https://hal.inria.fr/hal-02375594

[14] M. Albrecht, L. Ducas, G. Herold, E. Kirshanova, E. Postlethwaite, M. Stevens. *The General Sieve Kernel and New Records in Lattice Reduction*, in "EUROCRYPT", Darmstadt, Germany, April 2019, pp. 717-746 [*DOI :* 10.1007/978-3-030-17656-3_25], https://hal.archives-ouvertes.fr/hal-02397424

[15] D. Arzelier, F. Bréhard, M. Joldes. *Exchange algorithm for evaluation and approximation error-optimized polynomials*, in "ARITH 2019 - 26th IEEE Symposium on Computer Arithmetic", Kyoto, Japan, IEEE, June 2019, pp. 1-8, https://hal.archives-ouvertes.fr/hal-02006606

[16] *Best Paper*
F. Bréhard, M. Joldes, J.-B. Lasserre. *On Moment Problems with Holonomic Functions*, in "ISSAC 2019 - 44th International Symposium on Symbolic and Algebraic Computation", Pékin, China, July 2019, pp. 66-73, https://hal.archives-ouvertes.fr/hal-02006645.

[17] F. Bréhard, A. Mahboubi, D. Pous. *A certificate-based approach to formally verified approximations*, in "ITP 2019 - Tenth International Conference on Interactive Theorem Proving", Portland, United States, 2019, pp. 1-19 [*DOI :* 10.4230/LIPIcs.ITP.2019.8], https://hal.laas.fr/hal-02088529

[18] G. Castagnos, D. Catalano, F. Laguillaumie, F. Savasta, I. Tucker. *Two-Party ECDSA from Hash Proof Systems and Efficient Instantiations*, in "CRYPTO 2019 - 39th Annual International Cryptology Conference", Santa Barbara, United States, Advances in Cryptology – CRYPTO 2019, August 2019, vol. LNCS, n^{o} 11694, pp. 191-221 [*DOI :* 10.1007/978-3-030-26954-8_7], https://hal.archives-ouvertes.fr/hal-02281931

[19] J. H. Cheon, W. Cho, M. Hhan, J. Kim, C. Lee. *Statistical Zeroizing Attack: Cryptanalysis of Candidates of BP Obfuscation over GGH15 Multilinear Map*, in "CRYPTO", Santa Barbara, United States, August 2019, pp. 253-283 [*DOI :* 10.1007/978-3-030-26954-8_9], https://hal.archives-ouvertes.fr/hal-02397408

[20] V. Daza, A. González, Z. Pindado, C. Ràfols, J. Silva. *Shorter Quadratic QA-NIZK Proofs*, in "PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography", Beijing, China, LNCS, Springer, April 2019, vol. 11442, pp. 314-343 [*DOI :* 10.1007/978-3-030-17253-4_11], https://hal.inria.fr/hal-02399179

[21] A. González. *Shorter Ring Signatures from Standard Assumptions*, in "PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography", Beijing, China, Springer, April 2019, pp. 99-126 [*DOI :* 10.1007/978-3-030-17253-4_4], https://hal.inria.fr/hal-02399172

[22] A. González, C. Ràfols. *Shorter Pairing-based Arguments under Standard Assumptions*, in "ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security", Kobe, Japan, LNCS, Springer, November 2019, vol. 11923, pp. 728-757 [*DOI :* 10.1007/978-3-030-34618-8_25], https://hal.inria.fr/hal-02401556

[23] C. Lee, A. Pellet-Mary, D. Stehlé, A. Wallet. *An LLL Algorithm for Module Lattices*, in "ASIACRYPT", Kobe, Japan, November 2019, pp. 59-90 [*DOI :* 10.1007/978-3-030-34621-8_3], https://hal.archives-ouvertes.fr/hal-02397335

[24] V. Lefèvre, J.-M. Muller. *Accurate Complex Multiplication in Floating-Point Arithmetic*, in "ARITH 2019 - 26th IEEE Symposium on Computer Arithmetic", Kyoto, Japan, ARITH 2019 - 26th IEEE Symposium on Computer Arithmetic, IEEE, June 2019, pp. 1-7, https://hal.archives-ouvertes.fr/hal-02001080

[25] B. Libert, K. Nguyen, B. H. M. Tan, H. Wang. *Zero-Knowledge Elementary Databases with More Expressive Queries*, in "PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography", Beijing, China, LNCS, Springer, April 2019, vol. 11442, pp. 255-285 [*DOI :* 10.1007/978-3-030-17253-4_9], https://hal.inria.fr/hal-02151645

[26] B. Libert, C. Qian. *Lossy Algebraic Filters With Short Tags*, in "PKC 2019 - 22nd International Conference on Practice and Theory of Public Key Cryptography", Beijing, China, LNCS, Springer, April 2019, vol. 11442, pp. 34–65 [*DOI :* 10.1007/978-3-030-17253-4_2], https://hal.inria.fr/hal-02124968

[27] B. Libert, R. Titiu. *Multi-Client Functional Encryption for Linear Functions in the Standard Model from LWE*, in "ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security", Kobe, Japan, December 2019, pp. 1-54 [*DOI :* 10.1007/978-3-030-34618-8_18], https://hal.inria.fr/hal-02352139

[28] A. Pellet-Mary, G. Hanrot, D. Stehlé. *Approx-SVP in Ideal Lattices with Pre-processing*, in "Eurocrypt 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques", Darmstadt, Germany, Advances in Cryptology – EUROCRYPT 2019. Lecture Notes in Computer

Science, vol 11477, April 2019, pp. 685-716 [*DOI :* 10.1007/978-3-030-17656-3_24], https://hal.archives-ouvertes.fr/hal-02139939

[29] T. PREST, D. GOUDARZI, A. MARTINELLI, A. PASSELÈGUE. *Unifying Leakage Models on a Rényi Day*, in "Crypto 2019 - 39th Annual International Cryptology Conference", Santa Barbara, CA, United States, August 2019, pp. 683-712 [*DOI :* 10.1007/978-3-030-26948-7_24], https://hal.inria.fr/hal-02417544

[30] N. REVOL. *The MPFI Library: Towards IEEE 1788-2015 Compliance*, in "PPAM 2019 - 13th International Conference on Parallel Processing and Applied Mathematics", Bialystok, Poland, September 2019, pp. 1-10, https://hal.inria.fr/hal-02162346

[31] A. VOLKOVA, J.-M. MULLER. *Semi-automatic implementation of the complementary error function*, in "ARITH 2019 - 26th IEEE Symposium on Computer Arithmetic", Kyoto, Japan, ARITH 2019 - 26th IEEE Symposium on Computer Arithmetic, IEEE, June 2019, pp. 1-8, https://hal.archives-ouvertes.fr/hal-02002315

[32] F. DE DINECHIN, L. FORGET, J.-M. MULLER, Y. UGUEN. *Posits: the good, the bad and the ugly*, in "CoNGA 2019 - Conference on Next-Generation Arithmetic", Singapore, Singapore, ACM Press, March 2019, pp. 1-10 [*DOI :* 10.1145/3316279.3316285], https://hal.inria.fr/hal-01959581

Software

[33] T. GIVARO GROUP. *Givaro*, June 2019, Version : 4.1.1
[SWH-ID : swh:1:dir:df65912bd1e5ea4b96b935de95f6638eb6d9472d], Software, https://hal.archives-ouvertes.fr/hal-02130729

[34] T. LINBOX GROUP. *LinBox*, June 2019, Version : 1.6.3
[SWH-ID : swh:1:dir:393b611a1424f032e83569bf6762502371cfcf65], Software, https://hal.archives-ouvertes.fr/hal-02130801

Other Publications

[35] S. BOLDO, C. Q. LAUTER, J.-M. MULLER. *Emulating round-to-nearest-ties-to-zero "augmented" floating-point operations using round-to-nearest-ties-to-even arithmetic*, October 2019, working paper or preprint, https://hal.archives-ouvertes.fr/hal-02137968

[36] A. BOSTAN, T. RIVOAL, B. SALVY. *Explicit degree bounds for right factors of linear differential operators*, July 2019, https://arxiv.org/abs/1906.05529 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-02154679

[37] F. BRÉHARD, N. BRISEBARRE, M. JOLDES, W. TUCKER. *A New Lower Bound on the Hilbert Number for Quartic Systems*, March 2019, working paper or preprint, https://hal.laas.fr/hal-02085895

[38] S. MELCZER, B. SALVY. *Effective Coefficient Asymptotics of Multivariate Rational Functions via Semi-Numerical Algorithms for Polynomial Systems*, July 2019, https://arxiv.org/abs/1905.04187 - 47 pages, https://hal.archives-ouvertes.fr/hal-02185586