
IN PARTNERSHIP WITH:
**CNRS**

**Ecole normale supérieure de Lyon**

**Université Claude Bernard (Lyon 1)**

Activity Report 2017

# 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. - Verification, reliability, certification
A4. - Security and privacy
A7. - Theory of computation
A8. - Mathematics of computing

**Other Research Topics and Application Domains:**

B9.4. - Sciences
B9.8. - Privacy

# 1. Personnel

**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]
Nathalie Revol [Inria, Researcher]
Gilles Villard [CNRS, Senior Researcher, HDR]

**Faculty Members**

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

**Post-Doctoral Fellows**

Shi Bai [École Normale Supérieure Lyon, from May 2017 until Aug 2017]
Chitchanok Chuengsatiansup [Inria, from May 2017]
Wenjie Fang [Inria, from Apr 2017 until Aug 2017]
Junqing Gong [École Normale Supérieure Lyon]
Alonso Gonzalez [École Normale Supérieure Lyon, from Jun 2017]
Gottfried Herold [École Normale Supérieure Lyon]
Elena Kirshanova [École Normale Supérieure Lyon]
Anastasiia Volkova Lozanova [Inria, from Nov 2017]
Alexandre Wallet [École Normale Supérieure Lyon]

**PhD Students**

Florent Bréhard [École Normale Supérieure Lyon]
Adel Hamdi [Université Claude Bernard Lyon 1 and Orange Labs, from Dec 2017]
Stephen Melczer [NSERC, Canada, until Aug 2017]
Fabrice Mouhartem [École Normale Supérieure Lyon]

Marie Paindavoine [France Telecom R&D, until Jan 2017]
Alice Pellet-Mary [École Normale Supérieure Lyon]
Antoine Plet [École Normale Supérieure Lyon, until Aug 2017]
Valentina Popescu [École Normale Supérieure Lyon, until Sep 2017]
Miruna Rosca [Bitdefender, Romania; École Normale Supérieure Lyon]
Radu Titiu [Bitdefender, Romania; École Normale Supérieure Lyon]
Ida Tucker [École Normale Supérieure Lyon, from Oct 2017]
Weiqiang Wen [École Normale Supérieure Lyon]

**Technical staff**

Laurent Grémy [École Normale Supérieure Lyon, from Oct 2017]
Laurent Thévenoux [Inria]
Serge Torres [École Normale Supérieure Lyon]

**Interns**

Norbert Deak [Inria, from Feb 2017 until Jun 2017]
Benjamin Graillot [École Normale Supérieure Cachan, from Jun 2017 until Jul 2017]

**Administrative Assistants**

Evelyne Blesle [Inria]
Chiraz Benamor [École Normale Supérieure Lyon]

**Visiting Scientists**

Jiangtao Li [ECNU, China, until Aug 2017]
Benjamin Hong Meng Tan [Nanyang Technological University, Singapore]
Lloyd Nicholas Trefethen [École Normale Supérieure Lyon, from Oct 2017]
Warwick Tucker [Univ. de Lyon, from Sep 2017]

# 2. Overall Objectives

## 2.1. Overview

**The overall objective of AriC (Arithmetic and Computing) is, through computer arithmetic and computational mathematics, to improve computing at large.**

A major challenge in modeling and scientific computing is the simultaneous mastery of hardware capabilities, software design, and mathematical algorithms for the efficiency of the computation. Further, performance relates as much to efficiency as to reliability, requiring progress on automatic proofs, certificates and code generation. In this context, computer arithmetic and mathematical algorithms are the keystones of AriC. Our approach conciliates fundamental studies, practical performance and qualitative aspects, with a shared strategy going from high-level problem specifications and normalization actions, to computer arithmetic and the lowest-level details of implementations.
We focus on 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 cryptology 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 arithmetics 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 cryptology. 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. These themes also correspond to complementary angles for addressing the general computing challenge stated at the beginning of this introduction:

- **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 cryptology** (§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 approximation methods

### *3.1.1. Computer algebra generation of certified approximations*

We plan to focus on the generation of certified and efficient approximations for solutions of linear differential equations. These functions cover many classical mathematical functions and many more can be built by combining them. One classical target area is the numerical evaluation of elementary or special functions. This is currently performed by code specifically handcrafted for each function. The computation of approximations and the error analysis are major steps of this process that we want to automate, in order to reduce the probability of errors, to allow one to implement "rare functions", to quickly adapt a function library to a new context: new processor, new requirements – either in terms of speed or accuracy.

In order to significantly extend the current range of functions under consideration, several methods originating from approximation theory have to be considered (divergent asymptotic expansions; Chebyshev or generalized Fourier expansions; Padé approximants; fixed point iterations for integral operators). We have done preliminary work on some of them. Our plan is to revisit them all from the points of view of effectivity, computational complexity (exploiting linear differential equations to obtain efficient algorithms), as well as in their ability to produce provable error bounds. This work is to constitute a major progress towards the automatic generation of code for moderate or arbitrary precision evaluation with good efficiency. Other useful, if not critical, applications are certified quadrature, the determination of certified trajectories of spatial objects and many more important questions in optimal control theory.

### *3.1.2. Digital Signal Processing*

As computer arithmeticians, a wide and important target for us is the design of efficient and certified linear filters in digital signal processing (DSP). Actually, following the advent of MATLAB as the major tool for filter design, the DSP experts now systematically delegate to MATLAB all the part of the design related to numerical issues. And yet, various key MATLAB routines are neither optimized, nor certified. Therefore, there is a lot of room for enhancing numerous DSP numerical implementations and there exist several promising approaches to do so.

The main challenge that we want to address over the next period is the development and the implementation of optimal methods for rounding the coefficients involved in the design of the filter. If done in a naive way, this rounding may lead to a significant loss of performance. We will study in particular FIR and IIR filters.

### *3.1.3. Table Maker's Dilemma (TMD)*

There is a clear demand for hardest-to-round cases, and several computer manufacturers recently contacted us to obtain new cases. These hardest-to-round cases are a precious help for building libraries of correctly rounded mathematical functions. The current code, based on Lefèvre's algorithm, will be rewritten and formal proofs will be done.

We plan to use uniform polynomial approximation and diophantine techniques in order to tackle the case of the IEEE quad precision, and analytic number theory techniques (exponential sums estimates) for counting the hardest-to-round cases.

## 3.2. Lattices: algorithms and cryptology

Lattice-based cryptography (LBC) is an utterly promising, attractive (and competitive) research ground in cryptography, thanks to a combination of unmatched properties:

- **Improved performance.** LBC primitives have low asymptotic costs, but remain cumbersome in practice (e.g., for parameters achieving security against computations of up to 2100 bit operations). To address this limitation, a whole branch of LBC has evolved where security relies on the restriction of lattice problems to a family of more structured lattices called *ideal lattices*. Primitives based on such lattices can have quasi-optimal costs (i.e., quasi-constant amortized complexities), outperforming all contemporary primitives. This asymptotic performance sometimes translates into practice, as exemplified by NTRUEncrypt.
- **Improved security.** First, lattice problems seem to remain hard even for quantum computers. Moreover, the security of most of LBC holds under the assumption that standard lattice problems are hard in the worst case. Oppositely, contemporary cryptography assumes that specific problems are hard with high probability, for some precise input distributions. Many of these problems were artificially introduced for serving as a security foundation of new primitives.
- **Improved flexibility.** The master primitives (encryption, signature) can all be realized based on worst-case (ideal) lattice assumptions. More evolved primitives such as ID-based encryption (where the public key of a recipient can be publicly derived from its identity) and group signatures, that were the playing-ground of pairing-based cryptography (a subfield of elliptic curve cryptography), can also be realized in the LBC framework, although less efficiently and with restricted security properties. More intriguingly, lattices have enabled long-wished-for primitives. The most notable example is homomorphic encryption, enabling computations on encrypted data. It is the appropriate tool to securely outsource computations, and will help overcome the privacy concerns that are slowing down the rise of the cloud.

We work on three directions, detailed now.

### *3.2.1. Lattice algorithms*

All known lattice reduction algorithms follow the same design principle: perform a sequence of small elementary steps transforming a current basis of the input lattice, where these steps are driven by the Gram-Schmidt orthogonalisation of the current basis.

In the short term, we will fully exploit this paradigm, and hopefully lower the cost of reduction algorithms with respect to the lattice dimension. We aim at asymptotically fast algorithms with complexity bounds closer to those of basic and normal form problems (matrix multiplication, Hermite normal form). In the same vein, we plan to investigate the parallelism potential of these algorithms.

Our long term goal is to go beyond the current design paradigm, to reach better trade-offs between run-time and shortness of the output bases. To reach this objective, we first plan to strengthen our understanding of the interplay between lattice reduction and numerical linear algebra (how far can we push the idea of working on approximations of a basis?), to assess the necessity of using the Gram-Schmidt orthogonalisation (e.g., to obtain a weakening of LLL-reduction that would work up to some stage, and save computations), and to determine whether working on generating sets can lead to more efficient algorithms than manipulating bases. We will also study algorithms for finding shortest non-zero vectors in lattices, and in particular look for quantum accelerations.

We will implement and distribute all algorithmic improvements, e.g., within the fplll library. We are interested in high performance lattice reduction computations (see application domains below), in particular in connection with/continuation of the HPAC ANR project (algebraic computing and high performance consortium).

### *3.2.2. Lattice-based cryptography*

Our long term goal is to demonstrate the superiority of lattice-based cryptography over contemporary public-key cryptographic approaches. For this, we will 1- Strengthen its security foundations, 2- Drastically improve the performance of its primitives, and 3- Show that lattices allow to devise advanced and elaborate primitives.

The practical security foundations will be strengthened by the improved understanding of the limits of lattice reduction algorithms (see above). On the theoretical side, we plan to attack two major open problems: Are ideal lattices (lattices corresponding to ideals in rings of integers of number fields) computationally as hard to handle as arbitrary lattices? What is the quantum hardness of lattice problems?

Lattice-based primitives involve two types of operations: sampling from discrete Gaussian distributions (with lattice supports), and arithmetic in polynomial rings such as $(\mathbb{Z}/q\mathbb{Z})[x]/(x^n+1)$ with $n$ a power of 2. When such polynomials are used (which is the case in all primitives that have the potential to be practical), then the underlying algorithmic problem that is assumed hard involves ideal lattices. This is why it is crucial to precisely understand the hardness of lattice problems for this family. We will work on improving both types of operations, both in software and in hardware, concentrating on values of $q$ and $n$ providing security. As these problems are very arithmetic in nature, this will naturally be a source of collaboration with the other themes of the AriC team.

Our main objective in terms of cryptographic functionality will be to determine the extent to which lattices can help securing cloud services. For example, is there a way for users to delegate computations on their outsourced dataset while minimizing what the server eventually learns about their data? Can servers compute on encrypted data in an efficiently verifiable manner? Can users retrieve their files and query remote databases anonymously provided they hold appropriate credentials? Lattice-based cryptography is the only approach so far that has allowed to make progress into those directions. We will investigate the practicality of the current constructions, the extension of their properties, and the design of more powerful primitives, such as functional encryption (allowing the recipient to learn only a function of the plaintext message). To achieve these goals, we will in particular focus on cryptographic multilinear maps.

This research axis of AriC is gaining strength thanks to the recruitment of Benoit Libert. We will be particularly interested in the practical and operational impacts, and for this reason we envision a collaboration with an industrial partner.

### *3.2.3. Application domains*

- Diophantine equations. Lattice reduction algorithms can be used to solve diophantine equations, and in particular to find simultaneous rational approximations to real numbers. We plan to investigate the interplay between this algorithmic task, the task of finding integer relations between real numbers, and lattice reduction. A related question is to devise LLL-reduction algorithms that exploit specific shapes of input bases. This will be done within the ANR DynA3S project.
- Communications. We will continue our collaboration with Cong Ling (Imperial College) on the use of lattices in communications. We plan to work on the wiretap channel over a fading channel (modeling cell phone communications in a fast moving environment). The current approaches rely

on ideal lattices, and we hope to be able to find new approaches thanks to our expertise on them due to their use in lattice-based cryptography. We will also tackle the problem of sampling vectors from Gaussian distributions with lattice support, for a very small standard deviation parameter. This would significantly improve current schemes for communication schemes based on lattices, as well as several cryptographic primitives.

- Cryptanalysis of variants of RSA. Lattices have been used extensively to break variants of the RSA encryption scheme, via Coppersmith's method to find small roots of polynomials. We plan to work with Nadia Heninger (U. of Pennsylvania) on improving these attacks, to make them more practical. This is an excellent test case for testing the practicality of LLL-type algorithm. Nadia Heninger has a strong experience in large scale cryptanalysis based on Coppersmith's method (http://smartfacts.cr.yp.to/)

## 3.3. Algebraic computing and high performance kernels

The main theme here is the study of fundamental operations ("kernels") on a hierarchy of symbolic or numeric data types spanning integers, floating-point numbers, polynomials, power series, as well as matrices of all these. Fundamental operations include basic arithmetic (e.g., how to multiply or how to invert) common to all such data, as well as more specific ones (change of representation/conversions, GCDs, determinants, etc.). For such operations, which are ubiquitous and at the very core of computing (be it numerical, symbolic, or hybrid numeric-symbolic), our goal is to ensure both high performance and reliability.

### *3.3.1. Algorithms*

On the symbolic side, we will focus on the design and complexity analysis of algorithms for matrices over various domains (fields, polynomials, integers) and possibly with specific properties (structure). So far, our algorithmic improvements for polynomial matrices and structured matrices have been obtained in a rather independent way. Both types are well known to have much in common, but this is sometimes not reflected by the complexities obtained, especially for applications in cryptology and coding theory. Our goal in this area is thus to explore these connections further, to provide a more unified treatment, and eventually bridge these complexity gaps, A first step towards this goal will be the design of enhanced algorithms for various generalizations of Hermite-Padé approximation; in the context of list decoding, this should in particular make it possible to match or even improve over the structured-matrix approach, which is so far the fastest known.

On the other hand we will focus on the design of algorithms for certified computing. We will study the use of various representations, such as mid-rad for classical interval arithmetic, or affine arithmetic. We will explore the impact of precision tuning in intermediate computations, possibly dynamically, on the accuracy of the results (e.g. for iterative refinement and Newton iterations). We will continue to revisit and improve the classical error bounds of numerical linear algebra in the light of the subtleties of IEEE floating-point arithmetic.

Our goals in linear algebra and lattice basis reduction that have been detailed above in Section 3.2 will be achieved in the light of a hybrid symbolic-numeric approach.

### *3.3.2. Computer arithmetic*

Our work on certified computing and especially on the analysis of algorithms in floating-point arithmetic leads us to manipulate floating-point data in their greatest generality, that is, as symbolic expressions in the base and the precision. Our aim here is thus to develop theorems as well as efficient data structures and algorithms for handling such quantities by computer rather than by hand as we do now. The main outcome would be a "symbolic floating-point toolbox" which provides a way to check automatically the certificates of optimality we have obtained on the error bounds of various numerical algorithms.

We will also work on the interplay between floating-point and integer arithmetics. Currently, small numerical kernels like an exponential or a $2 \times 2$ determinant are typically written using exclusively one of these two kinds of arithmetic. However, modern processors now have hardware support for both floating-point and integer arithmetics, often with vector (SIMD) extensions, and an important question is how to make the best use of all such capabilities to optimize for both accuracy and efficiency.

A third direction will be to work on algorithms for performing correctly-rounded arithmetic operations in medium precision as efficiently and reliably as possible. Indeed, many numerical problems require higher precision than the conventional floating-point (single, double) formats. One solution is to use multiple precision libraries, such as GNU MPFR, which allow the manipulation of very high precision numbers, but their generality (they are able to handle numbers with millions of digits) is a quite heavy alternative when high performance is needed. Our objective here is thus to design a multiple precision arithmetic library that would allow to tackle problems where a precision of a few hundred bits is sufficient, but which have strong performance requirements. Applications include the process of long-term iteration of chaotic dynamical systems ranging from the classical Henon map to calculations of planetary orbits. The designed algorithms will be formally proved.

Finally, our work on the IEEE 1788 standard leads naturally to the development of associated reference libraries for interval arithmetic. A first direction will be to implement IEEE 1788 interval arithmetic within MPFI, our library for interval arithmetic using the arbitrary precision floating-point arithmetic provided by MPFR: indeed, MPFI has been originally developed with definitions and handling of exceptions which are not compliant with IEEE 1788. Another one will be to provide efficient support for multiple-precision intervals, in mid-rad representation and by developing MPFR-based code-generation tools aimed at handling families of functions.

#### *3.3.3. High-performance algorithms and software*

The algorithmic developments for medium precision floating-point arithmetic discussed above will lead to high performance implementations on GPUs. As a follow-up of the HPAC project (which ended in December 2015) we shall pursue the design and implementation of high performance linear algebra primitives and 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

H2020 project Prometheus (on privacy-preserving quantum-resistant cryptographic primitives, coordinated by Benoît Libert and hosted by ENS de Lyon). 4-year project (accepted in August 2017) starting from January 2018.

Publication of the book [48] “Algorithmes Efficaces en Calcul Formel.”

J.-M. Muller was elected Fellow member of the IEEE in Jan. 2017.

# 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 multiple-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. GNU MPFR 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.

- Participants: Guillaume Hanrot, Paul Zimmermann, Philippe Théveny and Vincent Lefèvre
- Contact: Vincent Lefèvre
- URL: http://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
- 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: Computer algebra system (CAS) - Euclidean Lattices
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. Automatic generation of hardware FIR filters from a frequency domain specification*

In [53], we present an open-source tool for the automatic design of reliable finite impulse response (FIR) filters, targeting FPGAs. It shows that user intervention can be limited to a very small number of relevant input parameters: a high-level frequency-domain specification, and input/output formats. All the other design parameters are computed automatically, using novel approaches to filter coefficient quantization and direct-form architecture implementation. Our tool guarantees a priori that the resulting architecture respects the specification while attempting to minimize its cost. Our approach is evaluated on a range of examples and shown to produce designs that are very competitive with the state of the art, with very little design effort.

### 7.1.2. Exponential sums and correctly-rounded functions

The 2008 revision of the IEEE-754 standard, which governs floating-point arithmetic, recommends that a certain set of elementary functions should be correctly rounded. Successful attempts for solving the Table Maker's Dilemma in binary64 made it possible to design `CRlibm`, a library which offers correctly rounded evaluation in binary64 of some functions of the usual `libm`. It evaluates functions using a two step strategy, which relies on a folklore heuristic that is well spread in the community of mathematical functions designers. Under this heuristic, one can compute the distribution of the lengths of runs of zeros/ones after the rounding bit of the value of the function at a given floating-point number. The goal of [13] was to change, whenever possible, this heuristic into a rigorous statement. The underlying mathematical problem amounts to counting integer points in the neighborhood of a curve, which we tackle using so-called exponential sums techniques, a tool from analytic number theory.

### 7.1.3. Continued fractions in power series fields

In [5], we explicitly describe a noteworthy transcendental continued fraction in the field of power series over $\mathbb{Q}$, having irrationality measure equal to 3. This continued fraction is a generating function of a particular sequence in the set $\{1, 2\}$. The origin of this sequence, whose study was initiated in a recent paper, is to be found in another continued fraction, in the field of power series over $\mathbb{F}_3$, which satisfies a simple algebraic equation of degree 4, introduced thirty years ago by D. Robbins.

### 7.1.4. Validated and numerically efficient Chebyshev spectral methods for linear ordinary differential equations

In [51], we develop a validated numerics method for the solution of linear ordinary differential equations (LODEs). A wide range of algorithms (i.e., Runge-Kutta, collocation, spectral methods) exist for numerically computing approximations of the solutions. Most of these come with proofs of asymptotic convergence, but usually, provided error bounds are non-constructive. However, in some domains like critical systems and computer-aided mathematical proofs, one needs validated effective error bounds. We focus on both the theoretical and practical complexity analysis of a so-called *a posteriori* quasi-Newton validation method, which mainly relies on a fixed-point argument of a contracting map. Specifically, given a polynomial approximation, obtained by some numerical algorithm and expressed in Chebyshev basis, our algorithm efficiently computes an accurate and rigorous error bound. For this, we study theoretical properties like compactness, convergence, invertibility of associated linear integral operators and their truncations in a suitable coefficient space of Chebyshev series. Then, we analyze the almost-banded matrix structure of these operators, which allows for very efficient numerical algorithms for both numerical solutions of LODEs and rigorous computation of the approximation error. Finally, several representative examples show the advantages of our algorithms as well as their theoretical and practical limits.

### 7.1.5. Validated semi-analytical transition matrices for linearized relative spacecraft dynamics via Chebyshev series appproximations

In [47], we provide an efficient generic algorithm to compute validated approximations of transition matrices of linear time-variant systems using Chebyshev expansions, and apply it to two different examples of relative motion of satellites (spacecraft rendezvous with Tschauner-Hempel equations and geostationary station keeping with J2 perturbation in the linearized Orange model).

## 7.2. Lattices: algorithms and cryptology

### 7.2.1. All-But-Many Lossy Trapdoor Functions and Selective Opening Chosen-Ciphertext Security from LWE

In cryptography, selective opening (SO) security refers to adversaries that receive a number of ciphertexts and, after having corrupted a subset of the senders (thus obtaining the plaintexts and the senders' random coins), aim at breaking the security of remaining ciphertexts. So far, very few public-key encryption schemes

are known to provide simulation-based selective opening (SIM-SO-CCA2) security under chosen-ciphertext attacks and most of them encrypt messages bit-wise. The only exceptions to date rely on all-but-many lossy trapdoor functions (as introduced by Hofheinz; Eurocrypt'12) and the Composite Residuosity assumption. In a paper [43] published at Crypto 2017, the team describes the first all-but-many lossy trapdoor function with security relying on the presumed hardness of the Learning-With-Errors problem (LWE) with standard parameters. The new construction exploits homomorphic computations on lattice trapdoors for lossy LWE matrices. By carefully embedding a lattice trapdoor in lossy public keys, the paper is able to prove SIM-SO-CCA2 security under the LWE assumption. As a result of independent interest, the paper describes a variant of our scheme whose multi-challenge CCA2 security tightly relates to the hardness of LWE and the security of a pseudo-random function.

### *7.2.2. Zero-Knowledge Arguments for Lattice-Based PRFs and Applications to E-Cash*

This paper [41] deals with cryptographic pseudorandom functions from lattice assumptions and their use in e-cash systems. Beyond their security guarantees under well-studied assumptions, algebraic pseudo-random functions are motivated by their compatibility with efficient zero-knowledge proof systems, which is useful in a number of privacy applications like digital cash. The paper considers the problem of proving the correct evaluation of lattice-based PRFs based on the Learning-With-Rounding (LWR) problem introduced by Banerjee et al. (Eurocrypt'12). Namely, the paper provides zero-knowledge arguments of knowledge of triples $(y, k, x)$ such that $y = F_k(x)$ is the correct evaluation of a PRF for a secret input $x$ and a committed key $k$. While analogous statements admit efficient zero-knowledge protocols in the discrete logarithm setting, they have never been addressed in lattices so far. The paper provides such arguments for the key homomorphic PRF of Boneh et al. (Crypto'13) and the generic PRF implied by the LWR-based pseudo-random generator. As an application, the paper describes the first compact e-cash system based on lattice assumptions.

### *7.2.3. Adaptive Oblivious Transfer with Access Control from Lattice Assumptions*

Adaptive oblivious transfer (OT) is a cryptographic protocol where a sender initially commits to a database $\{M_i\}_{i=1}^N$. Then, a receiver can query the sender up to $k$ times with private indexes $\rho_1, ..., \rho_k$ so as to obtain $M_{\rho_1}, ..., M_{\rho_k}$ and nothing else. Moreover, for each $i \in [k]$, the receiver's choice $\rho_i$ may depend on previously obtained messages. Oblivious transfer with access control (OT-AC) is a flavor of adaptive OT where database records are protected by distinct access control policies that specify which credentials a receiver should obtain in order to access each $M_i$. So far, all known OT-AC protocols only support access policies made of conjunctions or rely on *ad hoc* assumptions in pairing-friendly groups (or both). The paper [40] provides an OT-AC protocol where access policies may consist of any branching program of polynomial length, which is sufficient to realize any access policy in NC1. The security of the protocol is proved under the Learning-with-Errors (LWE) and Short-Integer-Solution (SIS) assumptions. As a result of independent interest, the paper provides protocols for proving the correct evaluation of a committed branching program on a committed input.

### *7.2.4. Encoding-Free ElGamal-Type Encryption Schemes on Elliptic Curves*

At PKC 2006, Chevallier-Mames, Paillier, and Pointcheval proposed a very elegant technique over cyclic subgroups of $\mathbb{F}_p$ eliminating the need to encode the message as a group element in the ElGamal encryption scheme. Unfortunately, it is unclear how to adapt their scheme over elliptic curves. In a previous attempt, Virat suggested an adaptation of ElGamal to elliptic curves over the ring of dual numbers as a way to address the message encoding issue. Advantageously the resulting cryptosystem does not require encoding messages as points on an elliptic curve prior to their encryption. Unfortunately, it only provides one-wayness and, in particular, it is not (and was not claimed to be) semantically secure. The paper revisits Virat's cryptosystem and extends the Chevallier-Mames et al.'s technique to the elliptic curve setting. The paper [35] considers elliptic curves over the ring $\mathbb{Z}/(p^2\mathbb{Z})$ and defines the underlying class function. This yields complexity assumptions whereupon new ElGamal-type encryption schemes are built. The so-obtained schemes are proved semantically secure and make use of a very simple message encoding: messages being encrypted are viewed as elements in the range $[0, p-1]$. Further, the new schemes come equipped with a partial ring-homomorphism property: anyone can add a constant to an encrypted message –or– multiply an encrypted message by a constant. This

can prove helpful as a blinding method in a number of applications. Finally, in addition to practicability, the proposed schemes also offer better performance in terms of speed, memory, and bandwidth.

### 7.2.5. Structure-Preserving Chosen-Ciphertext Security with Shorter Verifiable Ciphertexts

Structure-preserving cryptography is a world where messages, signatures, ciphertexts and public keys are entirely made of elements of a group over which a bilinear map is efficiently computable. This property makes the primitives compatible with the Groth-Sahai non-interactive proof systems in the design of higher-level privacy-preserving protocols. While structure-preserving signatures have received much attention the last 6 years, structure-preserving encryption schemes have undergone slower development. In particular, the best known structure-preserving cryptosystems with chosen-ciphertext (IND-CCA2) security either rely on symmetric pairings or require long ciphertexts comprised of hundreds of group elements or do not provide publicly verifiable ciphertexts. The paper [42] provides a publicly verifiable construction based on the SXDH assumption in asymmetric bilinear groups $e : G_1 \times G_2 \to G_T$, which features relatively short ciphertexts. For typical parameters, the ciphertext size amounts to less than 40 elements of $G$. As a second contribution, the paper provides a structure-preserving encryption scheme with perfectly randomizable ciphertexts and replayable chosen-ciphertext security. The new RCCA-secure system significantly improves upon the best known system featuring similar properties in terms of ciphertext size.

### 7.2.6. Tightly Secure IBE under Constant-size Master Public Key

This paper is about identity-based encryption (IBE). Chen and Wee (Crypto 2013) proposed the first almost tightly and adaptively secure IBE in the standard model and left two open problems which called for a tightly secure IBE with (1) constant-size master public key and/or (2) constant security loss. This paper proposes an IBE scheme with constant-size master public key and tighter security reduction. This (partially) solves Chen and Wee's first open problem and makes progress on the second one. Technically, the new IBE scheme is built based on Wee's petit IBE scheme (TCC 2016) in composite-order bilinear groups whose order is product of four primes. The sizes of master public key, ciphertexts, and secret keys are not only constant but also nearly optimal as Wee's petit IBE. The paper [33] proves its adaptive security in the multi-instance, multi-ciphertext setting (PKC 2015) based on the decisional subgroup assumption and a subgroup variant of DBDH assumption. The security loss is $O(\log q)$ where $q$ is the upper bound of the total number of secret keys and challenge ciphertexts revealed to adversary in each single IBE instance. It is much smaller than those for all known adaptively secure IBE schemes in a concrete sense.

### 7.2.7. ABE with Tag Made Easy: Concise Framework and New Instantiations in Prime-order Groups

Among all existing identity-based encryption (IBE) schemes in bilinear groups, Wat-IBE proposed by Waters (CRYPTO 2009) and JR-IBE proposed by Jutla and Roy (Asiacrypt 2013) are quite special. A secret key and/or ciphertext in these two schemes consists of several group elements and an integer which is usually called tag. A series of prior work was devoted to extending them towards more advanced attribute-based encryption (ABE) including inner-product encryption (IPE), hierarchical IBE (HIBE). Recently, Kim et al. (SCN 2016) introduced the notion of tag-based encoding and presented a generic framework for extending Wat-IBE. We may call these ABE schemes ABE with tag or tag-based ABE. Typically, a tag-based ABE construction is more efficient than its counterpart without tag. However, the research on tag-based ABE severely lags: we do not know how to extend JR-IBE in a systematic way and there is no tag-based ABE for Boolean span program even with Kim et al.'s generic framework.

This paper [32] proposes a generic framework for tag-based ABE which is based on JR-IBE and compatible with Chen et al.'s (attribute-hiding) predicate encoding (Eurocrypt 2015). The adaptive security in the standard model relies on the $k$-linear assumption in asymmetric prime-order bilinear groups. This is the first framework showing how to extend JR-IBE systematically. In fact, the framework and its simple extension are able to cover most concrete tag-based ABE constructions in previous literature. Furthermore, since Chen et al.'s predicate encoding supports a large number of predicates including boolean span program, the paper can give the first (both key-policy and ciphertext-policy) tag-based ABE for boolean span program in the standard

model. Technically, the new framework is based on a simplified version of JR-IBE. Both the description and its proof are quite similar to the prime-order IBE derived from Chen et al.'s framework. This not only allows us to work with Chen et al.'s predicate encoding but also provides a clear explanation of the JR-IBE scheme and its proof technique.

### *7.2.8. Hardness of $k$-LWE and Applications in Traitor Tracing*

The paper introduces the $k$-LWE problem, a Learning With Errors variant of the $k$-SIS problem. The Boneh-Freeman reduction from SIS to $k$-SIS suffers from an exponential loss in $k$. The paper [24] improves and extend it to an LWE to $k$-LWE reduction with a polynomial loss in $k$, by relying on a new technique involving trapdoors for random integer kernel lattices. Based on this hardness result, the paper presents the first algebraic construction of a traitor tracing scheme whose security relies on the worstcase hardness of standard lattice problems. The proposed LWE traitor tracing is almost as efficient as the LWE encryption. Further, it achieves public traceability, i.e., allows the authority to delegate the tracing capability to trusted parties. To this aim, the paper introduces the notion of projective sampling family in which each sampling function is keyed and, with a projection of the key on a well chosen space, one can simulate the sampling function in a computationally indistinguishable way. The construction of a projective sampling family from $k$-LWE allows us to achieve public traceability, by publishing the projected keys of the users.

### *7.2.9. Middle-Product Learning With Errors*

The paper [45] introduces a new variant MPLWE of the Learning With Errors problem (LWE) making use of the Middle Product between polynomials modulo an integer $q$. It exhibits a reduction from the Polynomial-LWE problem (PLWE) parametrized by a polynomial $f$, to MPLWE which is defined independently of any such $f$. The reduction only requires $f$ to be monic with constant coefficient coprime with $q$. It incurs a noise growth proportional to the so-called expansion factor of $f$. The paper also describes a public-key encryption scheme with quasi-optimal asymptotic efficiency (the bit-sizes of the keys and the run-times of all involved algorithms are quasi-linear in the security parameter), which is secure against chosen plaintext attacks under the MPLWE hardness assumption. The scheme is hence secure under the assumption that PLWE is hard for at least one polynomial $f$ of degree $n$ among a family of $f$'s which is exponential in $n$.

### *7.2.10. Efficient Public Trace and Revoke from Standard Assumptions*

The paper [27] provides efficient constructions for trace-and-revoke systems with public traceability in the black-box confirmation model. The constructions achieve adaptive security, are based on standard assumptions and achieve significant efficiency gains compared to previous constructions. The constructions rely on a generic transformation from inner product functional encryption (IPFE) schemes to trace-and-revoke systems. The proposed transformation requires the underlying IPFE scheme to only satisfy a very weak notion of security the attacker may only request a bounded number of random keys in contrast to the standard notion of security where she may request an unbounded number of arbitrarily chosen keys. The paper exploits the much weaker security model to provide a new construction for bounded collusion and random key IPFE from the learning with errors assumption (LWE), which enjoys improved efficiency compared to the scheme of Agrawal et al. [CRYPTO'16]. Together with IPFE schemes from Agrawal et al., the paper obtains trace and revoke from LWE, Decision Diffie Hellman and Decision Quadratic Residuosity.

### *7.2.11. New Techniques for Structural Batch Verification in Bilinear Groups with Applications to Groth-Sahai Proofs*

Bilinear groups form the algebraic setting for a multitude of important cryptographic protocols including anonymous credentials, e-cash, e-voting, e-coupon, and loyalty systems. It is typical of such crypto protocols that participating parties need to repeatedly verify that certain equations over bilinear groups are satisfied, e.g., to check that computed signatures are valid, commitments can be opened, or non-interactive zero-knowledge proofs verify correctly. Depending on the form and number of equations this part can quickly become a performance bottleneck due to the costly evaluation of the bilinear map.

To ease this burden on the verifier, batch verification techniques have been proposed that allow to combine and check multiple equations probabilistically using less operations than checking each equation individually. The paper [34] revisits the batch verification problem and existing standard techniques. It introduces a new technique which, in contrast to previous work, allows to fully exploit the structure of certain systems of equations. Equations of the appropriate form naturally appear in many protocols, e.g., due to the use of Groth–Sahai proofs.

The beauty of the new technique is that the underlying idea is pretty simple: the paper observes that many systems of equations can alternatively be viewed as a single equation of products of polynomials for which probabilistic polynomial identity testing following Schwartz–Zippel can be applied. Comparisons show that the new approach can lead to significant improvements in terms of the number of pairing evaluations. Indeed, for the BeleniosRF voting system presented at CCS 2016, it is possible to reduce the number of pairings (required for ballot verification) from $4k + 140$, as originally reported by Chaidos et al., to $k + 7$. As the implementation and benchmarks demonstrate, this may reduce the verification runtime to only 5% to 13% of the original runtime.

### *7.2.12. Encryption Switching Protocols Revisited: Switching Modulo $p$*

At CRYPTO 2016, Couteau, Peters and Pointcheval introduced a new primitive called Encryption Switching Protocols (ESP), allowing to switch ciphertexts between two encryption schemes. If such an ESP is built with two schemes that are respectively additively and multiplicatively homomorphic, it naturally gives rise to a secure 2-party computation protocol. It is thus perfectly suited for evaluating functions, such as multivariate polynomials, given as arithmetic circuits. Couteau et al. built an ESP to switch between Elgamal and Paillier encryptions which do not naturally fit well together. Consequently, they had to design a clever variant of Elgamal over $\mathbf{Z}/n\mathbf{Z}$ with a costly shared decryption.

In [31], we first present a conceptually simple generic construction for encryption switching protocols. We then give an efficient instantiation of our generic approach that uses two well-suited protocols, namely a variant of Elgamal in $\mathbf{Z}/p\mathbf{Z}$ and the Castagnos-Laguillaumie encryption which is additively homomorphic over $\mathbf{Z}/p\mathbf{Z}$. Among other advantages, this allows to perform all computations modulo a prime p instead of an RSA modulus. Overall, our solution leads to significant reductions in the number of rounds as well as the number of bits exchanged by the parties during the interactive protocols. We also show how to extend its security to the malicious setting.

## 7.3. Algebraic computing and high-performance kernels

### *7.3.1. Multiple binomial sums*

Multiple binomial sums form a large class of multi-indexed sequences, closed under partial summation, which contains most of the sequences obtained by multiple summation of binomial coefficients and also all the sequences with algebraic generating function. We study the representation of the generating functions of binomial sums by integrals of rational functions. The outcome is twofold. Firstly, we show that a univariate sequence is a multiple binomial sum if and only if its generating function is the diagonal of a rational function. Secondly we propose algorithms that decide the equality of multiple binomial sums and that compute recurrence relations for them. In conjunction with geometric simplifications of the integral representations, this approach behaves well in practice. The process avoids the computation of certificates and the problem of accurate summation that afflicts discrete creative telescoping, both in theory and in practice [12].

### *7.3.2. Algebraic Diagonals and Walks: Algorithms, Bounds, Complexity*

The diagonal of a multivariate power series $F$ is the univariate power series $\mathrm{Diag}(F)$ generated by the diagonal terms of $F$. Diagonals form an important class of power series; they occur frequently in number theory, theoretical physics and enumerative combinatorics. We study algorithmic questions related to diagonals in the case where $F$ is the Taylor expansion of a bivariate rational function. It is classical that in this case $\mathrm{Diag}(F)$ is an algebraic function. We propose an algorithm that computes an annihilating polynomial for $\mathrm{Diag}(F)$. We give a precise bound on the size of this polynomial and show that generically, this polynomial is the

minimal polynomial and that its size reaches the bound. The algorithm runs in time quasi-linear in this bound, which grows exponentially with the degree of the input rational function. We then address the related problem of enumerating directed lattice walks. The insight given by our study leads to a new method for expanding the generating power series of bridges, excursions and meanders. We show that their first $N$ terms can be computed in quasi-linear complexity in $N$, without first computing a very large polynomial equation [10].

### *7.3.3. Computing minimal interpolation bases*

In [20] we consider the problem of computing univariate polynomial matrices over a field that represent minimal solution bases for a general interpolation problem, some forms of which are the vector M-Padé approximation problem in [Van Barel and Bultheel, Numerical Algorithms 3, 1992] and the rational interpolation problem in [Beckermann and Labahn, SIAM J. Matrix Anal. Appl. 22, 2000]. Particular instances of this problem include the bivariate interpolation steps of Guruswami-Sudan hard-decision and Kötter-Vardy soft-decision decodings of Reed-Solomon codes, the multivariate interpolation step of list-decoding of folded Reed-Solomon codes, and Hermite-Padé approximation. In the mentioned references, the problem is solved using iterative algorithms based on recurrence relations. Here, we discuss a fast, divide-and-conquer version of this recurrence, taking advantage of fast matrix computations over the scalars and over the polynomials. This new algorithm is deterministic, and for computing shifted minimal bases of relations between $m$ vectors of size $\sigma$ it uses $\widetilde{O}(m^{\omega-1}(\sigma+|s|))$ field operations, where $\omega$ is the exponent of matrix multiplication, $|s|$ is the sum of the entries of the input shift $s$ with $\min(s)=0$, and the soft-O notation indicates that logarithmic factors in the big-O are omitted. This complexity bound improves in particular on earlier algorithms in the case of bivariate interpolation for soft decoding, while matching fastest existing algorithms for simultaneous Hermite-Padé approximation.

### *7.3.4. Fast and deterministic computation of the Hermite normal form and determinant of a polynomial matrix*

Given a nonsingular $n \times n$ matrix of univariate polynomials over a field, we present in [22] fast and deterministic algorithms to compute its determinant and its Hermite normal form. The proposed algorithms use $\widetilde{O}(n^{\omega}\lceil s \rceil)$ field operations, where $s$ is bounded from above by both the average of the degrees of the rows and that of the columns of the matrix, and $\omega$ is the exponent of matrix multiplication. The ceiling function indicates that the cost is $\widetilde{O}(n^{\omega})$ when $s = o(1)$. Our algorithms are based on a fast and deterministic triangularization method for computing the diagonal entries of the Hermite form of a nonsingular matrix.

### *7.3.5. Computing canonical bases of modules of univariate relations*

We study in [44] the computation of canonical bases of sets of univariate relations $(p_1, ..., p_m) \in K[x]^m$ such that $p_1 f_1 + \cdots + p_m f_m = 0$; here, the input elements $f_1, ..., f_m$ are from a quotient $K[x]^n/\mathcal{M}$, where $\mathcal{M}$ is a $K[x]$-module of rank $n$ given by a basis $M \in K[x]^{n\times n}$ in Hermite form. We exploit the triangular shape of $M$ to generalize a divide-and-conquer approach which originates from fast minimal approximant basis algorithms. Besides recent techniques for this approach, we rely on high-order lifting to perform fast modular products of polynomial matrices of the form $PF \bmod M$. Our algorithm uses $\widetilde{O}(m^{\omega-1}D + n^{\omega}D/m)$ operations in $K$, where $D = \deg(\det(M))$ is the $K$-vector space dimension of $K[x]^n/\mathcal{M}$, $\widetilde{O}(\cdot)$ indicates that logarithmic factors are omitted, and $\omega$ is the exponent of matrix multiplication. This had previously only been achieved for a diagonal matrix $M$. Furthermore, our algorithm can be used to compute the shifted Popov form of a nonsingular matrix within the same cost bound, up to logarithmic factors, as the previously fastest known algorithm, which is randomized.

### *7.3.6. Matrices with displacement structure: generalized operators and faster algorithms*

For matrices with displacement structure, basic operations like multiplication, inversion, and linear system solving can be expressed in terms of the following task: evaluate the product $AB$, where $A$ is a structured $n \times n$ matrix of displacement rank $\alpha$, and $B$ is an arbitrary $n \times \alpha$ matrix. In [11], we first generalize classical displacement operators, based on block diagonal matrices with companion diagonal blocks, and then design fast algorithms to perform the task above for this extended class of structured matrices. The arithmetic cost of

these algorithms ranges from $O(\alpha^{\omega-1}M(n))$ to $O(\alpha^{\omega-1}M(n)\log(n))$, with $\omega$ such that two $n \times n$ matrices over a field can be multiplied using $O(n^\omega)$ field operations, and where $M$ is a cost function for polynomial multiplication. By combining this result with classical randomized regularization techniques, we obtain faster Las Vegas algorithms for structured inversion and linear system solving.

### 7.3.7. Absolute real root separation

While the separation (the minimal nonzero distance) between roots of a polynomial is a classical topic, its absolute counterpart (the minimal nonzero distance between their absolute values) does not seem to have been studied much. We present the general context and give tight bounds for the case of real roots [14].

### 7.3.8. Weighted Lattice Walks and Universality Classes

In this work we consider two different aspects of weighted walks in cones. To begin we examine a particular weighted model, known as the Gouyou-Beauchamps model. Using the theory of analytic combinatorics in several variables we obtain the asymptotic expansion of the total number of Gouyou-Beauchamps walks confined to the quarter plane. Our formulas are parametrized by weights and starting point, and we identify six different asymptotic regimes (called universality classes) which arise according to the values of the weights. The weights allowed in this model satisfy natural algebraic identities permitting an expression of the weighted generating function in terms of the generating function of unweighted walks on the same steps. The second part of this article explains these identities combinatorially for walks in arbitrary cones and dimensions, and provides a characterization of universality classes for general weighted walks. Furthermore, we describe an infinite set of models with non-D-finite generating function [15].

### 7.3.9. Introduction to the IEEE 1788-2015 Standard for Interval Arithmetic

Interval arithmetic is a tool of choice for numerical software verification, as every result computed using this arithmetic is self-verified: every result is an interval that is guaranteed to contain the exact numerical values, regardless of uncertainty or roundoff errors. From 2008 to 2015, interval arithmetic underwent a standardization effort, resulting in the IEEE 1788-2015 standard. The main features of this standard are developed in [26]: the structure into levels, from the mathematic model to the implementation on computers; the possibility to accomodate different mathematical models, called flavors; the decoration system that keeps track of relevant events during the course of a calculation; the exact dot product for point (as opposed to interval) vectors.

### 7.3.10. Influence of the Condition Number on Interval Computations: Some Examples

The condition number is a quantity that is well-known in "classical" numerical analysis, that is, where numerical computations are performed using floating-point numbers. This quantity appears much less frequently in interval numerical analysis, that is, where the computations are performed on intervals. In [56], two aspects are developed. On the one hand, it is stressed that the notion of condition number already appears in the literature on interval analysis, even if it does not bear that name. On the other hand, three small examples are used to illustrate experimentally the impact of the condition number on interval computations. As expected, problems with a larger condition number are more difficult to solve: this means either that the solution is not very accurate (for moderate condition numbers) or that the method fails to solve the problem, even inaccurately (for larger condition numbers). Different strategies to counteract the impact of the condition number are discussed and experimented: use of a higher precision, iterative refinement, bisection of the input.

### 7.3.11. Error bounds on complex floating-point multiplication with an FMA

The accuracy analysis of complex floating-point multiplication done by Brent, Percival, and Zimmermann is extended to the case where a fused multiply-add (FMA) operation is available. Considering floating-point arithmetic with rounding to nearest and unit roundoff $u$, we show that their bound $\sqrt{5}\,u$ on the normwise relative error $|\widehat{z}/z - 1|$ of a complex product $z$ can be decreased further to $2u$ when using the FMA in the most naive way. Furthermore, we prove that the term $2u$ is asymptotically optimal not only for this naive FMA-based algorithm, but also for two other algorithms, which use the FMA operation as an efficient way of implementing rounding error compensation. Thus, although highly accurate in the componentwise sense,

these two compensated algorithms bring no improvement to the normwise accuracy $2u$ already achieved using the FMA naively. Asymptotic optimality is established for each algorithm thanks to the explicit construction of floating-point inputs for which we prove that the normwise relative error then generated satisfies $|\widehat{z}/z - 1| \to 2u$ as $u \to 0$. All our results hold for IEEE floating-point arithmetic, with radix $\beta$, precision $p$, and rounding to nearest; it is only assumed that underflows and overflows do not occur and that $\beta^{p-1} \geq 24$ [19].

### *7.3.12. Automatic source-to-source error compensation of floating-point programs*

Numerical programs with IEEE 754 floating-point computations may suffer from inaccuracies, since finite precision arithmetic is an approximation of real arithmetic. Solutions that reduce the loss of accuracy are available, such as, compensated algorithms or double-double precision floating-point arithmetic. Our goal is to automatically improve the numerical quality of a numerical program with the smallest impact on its performance. In [25] we define and implement source code transformations in order to derive automatically compensated programs. We present several experimental results to compare the transformed programs and existing solutions. The transformed programs are as accurate and efficient as the implementations of compensated algorithms when the latter exist. Furthermore, we propose some transformation strategies allowing us to improve partially the accuracy of programs and to tune the impact on execution time. Trade-offs between accuracy and performance are assured by code synthesis. Experimental results show that, with the help of the tools presented here, user-defined trade-offs are achievable in a reasonable amount of time.

### *7.3.13. Formal correctness of comparison algorithms between binary64 and decimal64 floating-point numbers*

We present a full Coq formalisation of the correctness of some comparison algorithms between binary64 and decimal64 floating-point numbers [28].

### *7.3.14. Implementation and performance evaluation of an extended precision floating-point arithmetic library for high-accuracy semidefinite programming*

Semidefinite programming (SDP) is widely used in optimization problems with many applications, however, certain SDP instances are ill-posed and need more precision than the standard double-precision available. Moreover, these problems are large-scale and could benefit from parallelization on specialized architectures such as GPUs. In this article, we implement and evaluate the performance of a floating-point expansion-based arithmetic library (newFPLib) in the context of such numerically highly accurate SDP solvers. We plugged-in the newFPLib with the state-of-the-art SDPA solver for both CPU and GPU-tuned implementations. We compare and contrast both the numerical accuracy and performance of SDPA-GMP,-QD and-DD, which employ other multiple-precision arithmetic libraries against SDPA-newFPLib. We show that our newFPLib is a very good trade-off for accuracy and speed when solving ill-conditioned SDP problems [38].

### *7.3.15. The classical relative error bounds for computing $\sqrt{a^2+b^2}$ and $c/\sqrt{a^2+b^2}$ in binary floating-point arithmetic are asymptotically optimal*

We study the accuracy of classical algorithms for evaluating expressions of the form $\sqrt{a^2+b^2}$ and $c/\sqrt{a^2+b^2}$ in radix-2, precision-$p$ floating-point arithmetic, assuming that the elementary arithmetic operations $\pm, \times, /, \sqrt{}$ are rounded to nearest, and assuming an unbounded exponent range. Classical analyses show that the relative error is bounded by $2u + \mathcal{O}(u^2)$ for $\sqrt{a^2+b^2}$, and by $3u + \mathcal{O}(u^2)$ for $c/\sqrt{a^2+b^2}$, where $u = 2^{-p}$ is the unit roundoff. Recently, it was observed that for $\sqrt{a^2+b^2}$ the $\mathcal{O}(u^2)$ term is in fact not needed. We show here that it is not needed either for $c/\sqrt{a^2+b^2}$. Furthermore, we show that these error bounds are asymptotically optimal. Finally, we show that the possible availability of an FMA instruction does not change the bounds, nor their asymptotic optimality [37].

### *7.3.16. On the relative error of computing complex square roots in floating-point arithmetic*

We study the accuracy of a classical approach to computing complex square-roots in floating-point arithmetic. Our analyses are done in binary floating-point arithmetic in precision $p$, and we assume that the (real)

arithmetic operations $+$, $-$, $\times$, $\div$, $\sqrt{}$ are rounded to nearest, so the unit roundoff is $u = 2^{-p}$. We show that in the absence of underflow and overflow, the componentwise and normwise relative errors of this approach are at most $\frac{7}{2}u$ and $\frac{\sqrt{37}}{2}u$, respectively, and this without having to neglect terms of higher order in $u$. We then provide some input examples showing that these bounds are reasonably sharp for the three basic binary interchange formats (binary32, binary64, and binary128) of the IEEE 754 standard for floating-point arithmetic.

### 7.3.17. More accurate complex multiplication for embedded processors

In [36] we present some work in progress on the development of fast and accurate support for complex floating-point arithmetic on embedded processors. Focusing on the case of multiplication, we describe algorithms and implementations for computing both the real and imaginary parts with high relative accuracy. We show that, in practice, such accuracy guarantees can be achieved with reasonable overhead compared with conventional algorithms (which are those offered by current implementations and for which the real or imaginary part of a product can have no correct digit at all). For example, the average execution-time overheads when computing an FFT on the ARM Cortex-A53 and -A57 processors range from 1.04x to 1.17x only, while arithmetic costs suggest overheads from 1.5x to 1.8x.

### 7.3.18. Tight and rigorous error bounds for basic building blocks of double-word arithmetic

We analyze several classical basic building blocks of double-word arithmetic (frequently called "double-double arithmetic" in the literature): the addition of a double-word number and a floating-point number, the addition of two double-word numbers, the multiplication of a double-word number by a floating-point number, the multiplication of two double-word numbers, the division of a double-word number by a floating-point number, and the division of two double-word numbers. For multiplication and division we get better relative error bounds than the ones previously published. For addition of two double-word numbers, we show that the previously published bound was incorrect, and we provide a new relative error bound. We introduce new algorithms for division. We also give examples that illustrate the tightness of our bounds [21].

### 7.3.19. On the robustness of the 2Sum and Fast2Sum algorithms

The 2Sum and Fast2Sum algorithms are important building blocks in numerical computing. They are used (implicitely or explicitely) in many compensated algorithms (such as compensated summation or compensated polynomial evaluation). They are also used for manipulating floating-point expansions. We show that these algorithms are much more robust than it is usually believed: The returned result makes sense even when the rounding function is not round-to-nearest, and they are almost immune to overflow [9].

### 7.3.20. Formal verification of a floating-point expansion renormalization algorithm

Many numerical problems require a higher computing precision than the one offered by standard floating-point formats. A common way of extending the precision is to use floating-point expansions. As the problems may be critical and as the algorithms used have very complex proofs (many sub-cases), a formal guarantee of correctness is a wish that can now be fulfilled, using interactive theorem proving. In this article we give a formal proof in Coq for one of the algorithms used as a basic brick when computing with floating-point expansions, the renormalization, which is usually applied after each operation. It is a critical step needed to ensure that the resulted expansion has the same property as the input one, and is more "compressed". The formal proof uncovered several gaps in the pen-and-paper proof and gives the algorithm a very high level of guarantee [30].

### 7.3.21. Interactive proof protocols

We present in [46] an interactive probabilistic proof protocol that certifies in $(\log N)^{O(1)}$ arithmetic and Boolean operations for the verifier for example the determinant of an $N \times N$ matrix over a field whose entries are given by a single $(\log N)^{O(1)}$-depth arithmetic circuit, which contains $(\log N)^{O(1)}$ field constants and which is polynomial time uniform. The prover can produce the interactive certificate within a $(\log N)^{O(1)}$ factor of the cost of computing the determinant. Our protocol is a version of the proofs for muggles protocol by Goldwasser, Kalai and Rothblum [STOC 2008, J. ACM 2015]. More generally, our verifier checks a

computation on a family of circuits of size $N^{O(1)}$, or even $2^{(\log N)^{O(1)}}$, for $g_N(f_N(0), ..., f_N(N-1))$ in $(\log N)^{O(1)}$ bit communication and bit-operation complexity. Here $g_N$ is a family of $(\log N)^{O(1)}$-depth circuits, and $f_N$ is a family of $(\log N)^{O(1)}$-depth circuits for the scalars (such as hypergeometric terms); $f_N$ can contain $(\log N)^{O(1)}$ input field constants. If the circuits $f_N$ for the scalars are of size $(\log N)^{O(1)}$, they are input for the verifier. The circuit $g_N$ and in the general case $f_N$ are $N^{O(1)}$-sized and cannot be built by the verifier with poly-log complexity. The verifier rather accesses the circuits via algorithms that probe the circuit structures, which are called uniformity properties.

#### *7.3.22. New development on GNU MPFR*

Work on the new fast, low-level algorithm to compute the correctly rounded summation of several floating-point numbers in arbitrary precision in radix 2 (each number having its own precision), and its implementation in GNU MPFR (new `mpfr_sum` function), has been completed [23].

The basic operations of GNU MPFR have also been optimized in small precision, and faithful rounding (mainly for internal use) is now partly supported [39].

These improvements, among many other ones, will be available in GNU MPFR 4.0.0; a release candidate is distributed in December 2017.

# 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.

## 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.
- Within the program Nano 2017, we collaborate with the Compilation Expertise Center of STMicroelectronics on the theme of floating-point arithmetic for embedded processors.

# 9. Partnerships and Cooperations

## 9.1. Regional Initiatives

The PhD grant of Valentina Popescu has been funded since September 2014 by Région Rhône-Alpes through the "ARC6" programme.

## 9.2. National Initiatives

#### *9.2.1. ANR DYNA3S Project*

**Participants:** Guillaume Hanrot, Gilles Villard.

Dyna3s is a four year ANR project that started in October 2013. The Web page of the project is https://www.irif.fr/~dyna3s. It is headed by Valérie Berthé (U. Paris 7) and involves also the University of Caen.

The aim is to study algorithms that compute the greatest common divisor (gcd) from the point of view of dynamical systems. A gcd algorithm is considered as a discrete dynamical system by focusing on integer input. We are mainly interested in the computation of the gcd of several integers. Another motivation comes from discrete geometry, a framework where the understanding of basic primitives, discrete lines and planes, relies on algorithm of the Euclidean type.

### *9.2.2. ANR FastRelax Project*

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

FastRelax stands for "Fast and Reliable Approximation". It is a four year ANR project started in October 2014. 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.

### *9.2.3. ANR MetaLibm Project*

**Participants:** Claude-Pierre Jeannerod, Jean-Michel Muller.

MetaLibm is a four-year project (started in October 2013 and recently extended till March 2018) focused on the design and implementation of code generators for mathematical functions and filters. The web page of the project is http://www.metalibm.org/ANRMetaLibm/. It is headed by Florent de Dinechin (INSA Lyon and Socrate team) and, besides Socrate and AriC, also involves teams from LIRMM (Perpignan), LIP6 (Paris), CERN (Geneva), and Kalray (Grenoble). The main goals of the project are to automate the development of mathematical libraries (libm), to extend it beyond standard functions, and to make it unified with similar approaches developed in or useful for signal processing (filter design). Within AriC, we are especially interested in studying the properties of fixed-point arithmetic and floating-point arithmetic that can help develop such a framework.

### *9.2.4. 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.

### *9.2.5. RISQ Project*

**Participants:** Benoît Libert, Fabien Laguillaumie, Damien Stehlé, Chitchanok Chuengsatiansup.

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.

## 9.3. European Initiatives

### *9.3.1. FP7 & H2020 Projects*

#### *9.3.1.1. LattAC ERC grant*

Damien Stehlé was awarded an ERC Starting Grant for his project *Euclidean lattices: algorithms and cryptography* (LattAC) in 2013 (1.4Meur for 5 years from January 2014). The LattAC project aims at studying all computational aspects of lattices, from algorithms for manipulating them to applications. The main objective is to enable the rise of lattice-based cryptography.

#### *9.3.1.2. PROMETHEUS Project*

**Participants:** Benoît Libert, Fabien Laguillaumie, 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 will start in January 2018. It gathers 7 academic partners (ENS de Lyon and Université de Rennes 1; CWI, Pays-Bas; Royal Holloway University of London, United Kingdom; Universitat Politècnica de Catalunya, Spain; Ruhr-Universität Bochum, Germany; Weizmann Institute, Israel), 5 industrial partners (Orange, IBM, 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.

## 9.4. International Initiatives

### *9.4.1. Participation in International Programs*

Vincent Lefèvre participated in the standardization of interval arithmetic (simplified version of the standard, IEEE 1788.1). He actively participates in the revision of the IEEE 754 standard for 2018.

## 9.5. International Research Visitors

### *9.5.1. Visits of International Scientists*

- Lloyd Nicholas Trefethen, from Oxford University (UK), is an expert in numerical analysis and notably the systematic use of Chebyshev approximation. He is spending the academic year 2017-2018 with AriC.
- Warwick Tucker, from Uppsala University (Sweden), is an expert of certified computation for dynamical systems. He is spending the academic year 2017-2018 with AriC.

- Huaxiong Wang, from Nanyang Technological University (Singapore), is an expert in cryptographic protocols and multi-party computation. He visited us in March and April 2017.
- Jung Hee Cheon, from Seoul National University (South Korea), is an expert in algorithmic number theory and the mathematical foundations of cryptography. He is visiting us since October 2017, until January 2018.

### *9.5.2. Internships*

Benjamin Graillot

Date: May 2017–July 2017

Institution: ENS de Cachan

Supervisor: Bruno Salvy

### *9.5.3. Visits to International Teams*

*9.5.3.1. Research Stays Abroad*

Benoît Libert spent one month in the cryptography team of Nanyang Technological University (Singapore), to collaborate with Khoa Nguyen and Huaxiong Wang.

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### *10.1.1. Scientific Events Organisation*

*10.1.1.1. Member of Organizing Committees*

Nicolas Brisebarre was a member of the organization committee of JNCF 2017 (Journées Nationales de Calcul Formel) that took place at CIRM, in Luminy in January 2017. There were more than 70 participants.

Claude-Pierre Jeannerod and Nicolas Louvet organized RAIM 2017 (Rencontres "Arithmétiques de l'Informatique Mathématique") at ENS Lyon in October 2017.

### *10.1.2. Scientific Events Selection*

*10.1.2.1. Member of the Conference Program Committees*

Bruno Salvy is a member of the program Committee of AofA2018 (Analysis of Algorithms) and of FPSAC'2019 (Formal Power Series and Algebraic Combinatorics).

Benoît Libert was a program committee member for Eurocrypt 2017 and TCC (Theory of Cryptography Conference) 2017. He is in the program committees of SCN 2018 (Security and Cryptography for Networks) and ACNS 2018 (Applied Cryptography and Network Security).

Nathalie Revol was a member of the program committee for Arith 24, Correctness 2017, CRE 2017 (Computational Reproducibility at Exascale, Workshop of Supercomputing 2017).

Damien Stehlé is in the program committees of PQCrypto 2017 and 2018, Eurocrypt 2017 and 2018, Asiacrypt 2017 and SCN 2018.

Chitchanok Chuengsatiansup is in the program committee of CRYPTO 2018.

Jean-Michel Muller is a member of the board of the Steering Committee of the ARITH (IEEE Symposium on Computer Arithmetic) series of conferences.

Fabien Laguillaumie is a program committee member for Africacrypt 2017, ACISP 2018 and C2SI-SEA 2018.

### *10.1.3. Journal*

*10.1.3.1. Member of Editorial Boards*

Bruno Salvy is a member of the editorial boards of the *Journal of Symbolic Computation*, of the *Journal of Algebra* (section Computational Algebra) and of the collection *Texts and Monographs in Symbolic Computation* (Springer).

Jean-Michel Muller is a member of the Editorial board of IEEE Transactions on Computers.

Nathalie Revol was guest editor and Jean-Michel Muller was supervising associate editor of a special issue on Computer Arithmetic of IEEE Transactions on Computers [18].

Nathalie Revol is a member of the editorial board of the journal *Reliable Computing*.

Gilles Villard is a member of the editorial board of the *Journal of Symbolic Computation*.

### *10.1.4. Invited Talks*

Bruno Salvy was an invited speaker at AofA'2017 (Princeton), where he gave a talk on effective methods in the asymptotic analysis of sequences. He also gave an invited plenary talk at FoCM'2017 (Barcelona), on the use of linear differential equations as a data structure. He will be giving a tutorial at STACS'2018 on random generation of combinatorial structures.

Damien Stehlé gave an invited tutorial talk at the ISSAC 2017 conference (Kaiserslautern, Germany), on lattice reduction algorithms. He was an invited speaker at the Africacrypt 2017 conference (Dakar, Senegal), on the Learning With Errors problem and its applications in cryptography.

Jean-Michel Muller gave an invited talk at the 2017 Asilomar Conference on Signals, Systems, and Computers (Pacific Grove, CA, USA), on the analysis and design of algorithms for complex arithmetic.

### *10.1.5. Leadership within the Scientific Community*

Paola Boito and Claude-Pierre Jeannerod were members of the scientific committee of JNCF (Journées Nationales de Calcul Formel).

Nathalie Revol is the chair of the IEEE 1788 group for the standardization of interval arithmetic: a simplified version of the standard, based only on the binary64 format of IEEE-754, has been approved in December 2017 and will be published as IEEE 1788.1.

### *10.1.6. Scientific Expertise*

Paola Boito was a member of the recruitment committees for two associate professor positions in Limoges (mathematics and computer science).

Jean-Michel Muller was a member of the recruitment committee for an associate professor position in Université Grenoble Alpes (computer science).

Jean-Michel Muller is a member of the Scientific committee of CERFACS, Toulouse. Until October 2017 he was a member of the Steering Committee of "Défi 7" (*information and communication society*) of the french Agence Nationale de la Recherche. He is a member of the Scientific Council of CERFACS, Toulouse. In January 2017, he chaired the Evaluation Committee of LIF Laboratory, Marseille.

Nathalie Revol was a member of the visiting committee for the Computer Science Department and the Mathematics Department of Uppsala University, Sweden.

Fabien Laguillaumie was a member of the recruitement committee for an associate professor position in the Université Claude Bernard Lyon 1.

Claude-Pierre Jeannerod was a member of the recruitment committee for postdocs and sabbaticals at Inria Grenoble Rhône-Alpes.

### 10.1.7. Research Administration

Jean-Michel Muller is co-head of the GDR (Groupement de Recherches) IM of CNRS (around 1400 permanent members, www.gdr-im.fr).

## 10.2. Teaching - Supervision - Juries

### 10.2.1. Teaching

Master: Claude-Pierre Jeannerod, Nathalie Revol, *Algorithmique numérique et fiabilité des calculs en arithmétique flottante* (24h), M2 ISFA (Institut de Science Financière et d'Assurances), Université Claude Bernard Lyon 1.

Master: Vincent Lefèvre, *Arithmétique des ordinateurs* (12h), M2 ISFA (Institut de Science Financière et d'Assurances), Université Claude Bernard Lyon 1.

Master: Fabien Laguillaumie, Cryptography, Error Correcting Codes, 150h, Université Claude Bernard Lyon 1 (on CNRS secondment in 2016-2017).

Master: Damien Stehlé, Cryptography, 12h, ENS de Lyon.

Master: Benoît Libert, Cryptography, 12h, ENS de Lyon.

Master: Damien Stehlé, Hard lattice problems, 24h, ENS de Lyon.

Post-graduate: Claude-Pierre Jeannerod and Nathalie Revol, *Arithmétique flottante et erreurs d'arrondi* (3h), École Jeunes Chercheurs et Jeunes Chercheuses en Informatique Mathématique.

Post-graduate: Damien Stehlé, Foundations of lattice-based cryptography, 10h, NTT (Japan).

Post-graduate: Damien Stehlé, Foundations of lattice-based cryptography, 3h, Seoul National University (South Korea).

Professional teaching: Nathalie Revol, *Introduction à l'arithmétique par intervalles* (3h00), École Précis (Précision, Reproductibilité en Calcul et Informatique Scientifique).

Professional teaching: Nathalie Revol, *Contrôler et améliorer la qualité numérique d'un code de calcul industriel* (2h30), Collège de Polytechnique.

Master: Bruno Salvy, Calcul Formel (9h), MPRI.

Master: Bruno Salvy, Mathématiques expérimentales (44h), École polytechnique.

Master: Bruno Salvy, Logique et complexité (32h), École polytechnique.

### 10.2.2. Supervision

- PhD: Stephen Melczer, *Effective analytic combinatorics in one and several variables*, defended on June 13, 2017, co-supervised by George Labahn (U. Waterloo, Canada) and Bruno Salvy.
- PhD: Marie Paindavoine, *Méthodes de calculs sur des données chiffrées*, defended on January 27, 2017, co-supervised by Fabien Laguillaumie and Sébastien Canard (Orange).
- PhD: Antoine Plet, *Contribution à l'analyse d'algorithmes en arithmétique virgule flottante* [3], defended on July 7, 2017, co-supervised by Nicolas Louvet and Jean-Michel Muller.
- PhD: Valentina Popescu, *Vers des bibliothèques multi-précision certifiées et performantes* [4], defended on july 6, 2017, co-supervised by Mioara Joldes (LAAS) and Jean-Michel Muller
- PhD in progress: Fabrice Mouhartem, *Privacy-preserving protocols from lattices and bilinear maps*, since September 2015, supervised by Benoît Libert.
- PhD in progress: Chen Qiang, *Applications of Malleability in Cryptography*, since September 2016, co-supervised by Benoît Libert, Adeline Langlois (IRISA) and Pierre-Alain Fouque (IRISA).
- PhD in progress: Radu Titiu, *Pseudorandom functions and functional encryption from lattices and bilinear maps*, since January 2017, supervised by Benoît Libert.

- PhD in progress: Weiqiang Wen, *Hard problems on lattices*, since September 2015, supervised by Damien Stehlé.
- PhD in progress: Alice Pellet–Mary, *Cryptographic obfuscation*, since September 2016, supervised by Damien Stehlé.
- PhD in progress: Miruna Rosca, *Hardness of lattice problems over rings*, since January 2017, supervised by Damien Stehlé.
- PhD in progress: Florent Bréhard, *Outils pour un calcul certifié. Applications aux systèmes dynamiques et à la théorie du contrôle*, since September 2016, co-supervised by Nicolas Brisebarre, Mioara Joldeş (LAAS, Toulouse) and Damien Pous (LIP).
- PhD in progress: Ida Tucker, *Conception de systèmes cryptographiques avancés reposant sur des briques homomorphes*, since Octobre 2017, co-supervised by Guilhem Castagnos (IMB, Bordeaux) and Fabien Laguillaumie.
- PhD in progress: Adel Hamdi, *Chiffrement fonctionnel pour le traitement de données externes en aveugle*, since December 2017, co-supervised by Sébastien Canard (Orange Labs, Caen) and Fabien Laguillaumie.

### *10.2.3. Juries*

Bruno Salvy was a reviewer for the HdR of Thomas Cluzeau (Limoges) and for the PhD thesis of Thomas Sibut-Pinote (École polytechnique). He was also a member of the Habilitation committee of Michael Rao (ENS Lyon). He was a member of the recruitment committee for junior researchers at Inria Grenoble.

Benoît Libert was a reviewer for the PhD theses of Florian Bourse (ENS Paris) and Alonso Gonzalez (University of Chile, Santiago). He was the president of the PhD committee of Geoffroy Couteau (ENS Paris), and a member of the PhD committees of Florian Bourse (ENS Paris) and Alonso Gonzalez (University of Chile, Santiago).

Damien Stehlé was a reviewer for the PhD theses of Pierrick Méaux (ENS Paris) and Philippe Moustrou (University of Bordeaux). He was the president of the PhD committee of Thomas Camus (University of Grenoble).

Jean-Michel Muller was the president of the PhD committee of Anastasia Volkova (Pierre et Marie Curie University, Paris), and a member of the Habilitation committee of Nicolas Brisebarre (ENS Lyon).

Fabien Laguillaumie was a reviewer for the PhD thesis of Francisco Vial-Prado (Université Versailles St-Quentin-en-Yvelines) and Laurent Grémy (Université de Lorraine). He was the president of the PhD committee of Thierry Menfenza (ENS Paris and Université de Yaoundé). He was was also a member of the HDR committee of Céline Chevalier (ENS Paris).

## 10.3. Popularization

Nathalie Revol is a member of the steering committee of the MMI: Maison des Mathématiques et de l'Informatique, and in particular she was involved in the creation of the *Magimatique 2* exhibition. She presented some magic tricks at Bibliothèque Municipale de la Part-Dieu and at MMI for 3 classes during the Science Fair. She gave talks for a large audience during "Forum Maths Vivantes" and for "La tournée de Pi" (mathematical musical, around 600 attendees) (March 2017). As an incentive for high-school pupils, and especially girls, to choose scientific careers, she gave talks at Lycée Ella Fitzgerald (Saint-Romain-en-Gal) and Mondial des Métiers (in February 2017) and during "Journée Filles et Sciences" in Musée des Confluences and "Journée Filles" by INSA Lyon (above 550 attendees in total, March 2017). She co-organized for two "Coding gouters" organized by MixTeen. She co-organized two days on "Info Sans Ordinateur" gathering researchers interested in unplugged activities. She is a member of the editorial committee of Interstices: https://interstices.info. She taught how to disseminate (computer) science for PhD students in a 20h module of *Insertion Professionnelle*.

Bruno Salvy will give a talk at the Collège de France in December 2017 on methods of analytic combinatorics in random generation.

Damien Stehlé hosted a visit at ENS de Lyon by the regional winners of the Alkindi competition (midde highschool and highschool).

# 11. Bibliography

## Publications of the year

### Doctoral Dissertations and Habilitation Theses

[1] N. BRISEBARRE. *Un peu de théorie des nombres et de calcul formel au service de l'arithmétique des ordinateurs*, École Normale Supérieure de Lyon, September 2017, Habilitation à diriger des recherches, https://hal.archives-ouvertes.fr/tel-01658342

[2] S. MELCZER. *Analytic Combinatorics in Several Variables : Effective Asymptotics and Lattice Path Enumeration*, Université de Lyon, June 2017, https://tel.archives-ouvertes.fr/tel-01587716

[3] A. PLET. *Contribution to error analysis of algorithms in floating-point arithmetic*, Université de Lyon, July 2017, https://tel.archives-ouvertes.fr/tel-01582218

[4] V. POPESCU. *Towards fast and certified multiple-precision librairies*, Université de Lyon, July 2017, https://hal.archives-ouvertes.fr/tel-01534090

### Articles in International Peer-Reviewed Journals

[5] B. ALLOMBERT, N. BRISEBARRE, A. LASJAUNIAS. *On a two-valued sequence and related continued fractions in power series fields*, in "The Ramanujan Journal", 2017, https://arxiv.org/abs/1607.07235 , forthcoming [*DOI :* 10.1007/s11139-017-9892-7], https://hal.archives-ouvertes.fr/hal-01348576

[6] P. BOITO, Y. EIDELMAN, L. GEMIGNANI. *A Real QZ Algorithm for Structured Companion Pencils*, in "Calcolo", July 2017, https://arxiv.org/abs/1608.05395 [*DOI :* 10.1007/s10092-017-0231-6], https://hal.inria.fr/hal-01407864

[7] P. BOITO, Y. EIDELMAN, L. GEMIGNANI. *Efficient Solution of Parameter Dependent Quasiseparable Systems and Computation of Meromorphic Matrix Functions*, in "Numerical Linear Algebra with Applications", 2017, forthcoming, https://hal.inria.fr/hal-01407857

[8] P. BOITO, R. GRENA. *Optimal focal length of primary mirrors in Fresnel linear collectors*, in "Solar Energy", October 2017, vol. 155, pp. 1313 - 1318 [*DOI :* 10.1016/J.SOLENER.2017.07.079], https://hal.inria.fr/hal-01647602

[9] S. BOLDO, S. GRAILLAT, J.-M. MULLER. *On the robustness of the 2Sum and Fast2Sum algorithms*, in "ACM Transactions on Mathematical Software", July 2017, vol. 44, n° 1, https://hal-ens-lyon.archives-ouvertes.fr/ensl-01310023

[10] A. BOSTAN, L. DUMONT, B. SALVY. *Algebraic Diagonals and Walks: Algorithms, Bounds, Complexity*, in "Journal of Symbolic Computation", 2017, vol. 83, pp. 68–92, https://arxiv.org/abs/1510.04526 [*DOI :* 10.1016/J.JSC.2016.11.006], https://hal.archives-ouvertes.fr/hal-01244914

[11] A. BOSTAN, C.-P. JEANNEROD, C. MOUILLERON, E. SCHOST. *On Matrices With Displacement Structure: Generalized Operators and Faster Algorithms*, in "SIAM Journal on Matrix Analysis and Applications", 2017, vol. 38, n° 3, pp. 733-775, https://arxiv.org/abs/1703.03734 [*DOI :* 10.1137/16M1062855], https://hal.archives-ouvertes.fr/hal-01588552

[12] A. BOSTAN, P. LAIREZ, B. SALVY. *Multiple binomial sums*, in "Journal of Symbolic Computation", 2017, vol. 80, n° 2, pp. 351–386 [*DOI :* 10.1016/J.JSC.2016.04.002], https://hal.archives-ouvertes.fr/hal-01220573

[13] N. BRISEBARRE, G. HANROT, O. ROBERT. *Exponential sums and correctly-rounded functions*, in "IEEE Transactions on Computers", April 2017 [*DOI :* 10.1109/TC.2017.2690850], https://hal.archives-ouvertes.fr/hal-01396027

[14] Y. BUGEAUD, A. DUJELLA, T. PEJKOVIĆ, B. SALVY. *Absolute Real Root Separation*, in "The American Mathematical Monthly", 2017, vol. 124, n° 10, pp. 930-936 [*DOI :* 10.4169/AMER.MATH.MONTHLY.124.10.930], https://hal.archives-ouvertes.fr/hal-01655531

[15] J. COURTIEL, S. MELCZER, M. MISHNA, K. RASCHEL. *Weighted Lattice Walks and Universality Classes*, in "Journal of Combinatorial Theory, Series A", 2017, https://arxiv.org/abs/1609.05839 [*DOI :* 10.1016/J.JCTA.2017.06.008], https://hal.archives-ouvertes.fr/hal-01368786

[16] J.-G. DUMAS, C. PERNET, Z. SULTAN. *Fast Computation of the Rank Profile Matrix and the Generalized Bruhat Decomposition*, in "Journal of Symbolic Computation", November 2017, vol. 83, pp. 187–210, https://arxiv.org/abs/1601.01798 [*DOI :* 10.1016/J.JSC.2016.11.011], https://hal.archives-ouvertes.fr/hal-01251223

[17] J.-C. FAUGÈRE, A. WALLET. *The Point Decomposition Problem over Hyperelliptic Curves: toward efficient computations of Discrete Logarithms in even characteristic*, in "Designs, Codes and Cryptography", 2017, forthcoming [*DOI :* 10.1007/S10623-017-0449-Y], https://hal.inria.fr/hal-01658573

[18] J. HORMIGO, J.-M. MULLER, S. OBERMANN, N. REVOL, A. TISSERAND, J. VILLALBA-MORENO. *Introduction to the Special Section on Computer Arithmetic*, in "IEEE Transactions on Computers", December 2017, vol. 66, n° 12, pp. 1991-1993 [*DOI :* 10.1109/TC.2017.2761278], https://hal.archives-ouvertes.fr/hal-01648100

[19] C.-P. JEANNEROD, P. KORNERUP, N. LOUVET, J.-M. MULLER. *Error bounds on complex floating-point multiplication with an FMA*, in "Mathematics of Computation", 2017, vol. 86, n° 304, pp. 881-898 [*DOI :* 10.1090/MCOM/3123], https://hal.inria.fr/hal-00867040

[20] C.-P. JEANNEROD, V. NEIGER, E. SCHOST, G. VILLARD. *Computing minimal interpolation bases*, in "Journal of Symbolic Computation", November 2017, vol. 83, pp. 272–314 [*DOI :* 10.1016/J.JSC.2016.11.015], https://hal.inria.fr/hal-01241781

[21] M. M. JOLDES, J.-M. MULLER, V. POPESCU. *Tight and rigourous error bounds for basic building blocks of double-word arithmetic*, in "ACM Transactions on Mathematical Software", 2017, vol. 44, n° 2, pp. 1 - 27 [*DOI :* 10.1145/3121432], https://hal.archives-ouvertes.fr/hal-01351529

[22] G. LABAHN, V. NEIGER, W. ZHOU. *Fast, deterministic computation of the Hermite normal form and determinant of a polynomial matrix*, in "Journal of Complexity", October 2017 [*DOI :* 10.1016/J.JCO.2017.03.003], https://hal.inria.fr/hal-01345627

[23] V. LEFÈVRE. *Correctly Rounded Arbitrary-Precision Floating-Point Summation*, in "IEEE Transactions on Computers", 2017 [*DOI :* 10.1109/TC.2017.2690632], https://hal.inria.fr/hal-01394289

[24] S. LING, D. H. PHAN, D. STEHLÉ, R. STEINFELD. *Hardness of k-LWE and Applications in Traitor Tracing*, in "Algorithmica", December 2017, vol. 79, n° 4, pp. 1318 - 1352 [*DOI :* 10.1007/S00453-016-0251-7], https://hal.archives-ouvertes.fr/hal-01643505

[25] L. THÉVENOUX, P. LANGLOIS, M. MARTEL. *Automatic source-to-source error compensation of floating-point programs: code synthesis to optimize accuracy and time*, in "Concurrency and Computation: Practice and Experience", 2017, vol. 29, n° 7, e3953 p. [*DOI :* 10.1002/CPE.3953], https://hal.archives-ouvertes.fr/hal-01236919

### Invited Conferences

[26] N. REVOL. *Introduction to the IEEE 1788-2015 Standard for Interval Arithmetic*, in "10th International Workshop on Numerical Software Verification - NSV 2017, workshop of CAV 2017", Heidelberg, Germany, A. ABATE, S. BOLDO (editors), LNCS, Springer, July 2017, n° 10381, pp. 14-21 [*DOI :* 10.1007/978-3-319-63501-9], https://hal.inria.fr/hal-01559955

### International Conferences with Proceedings

[27] S. AGRAWAL, S. BHATTACHERJEE, D. H. PHAN, D. STEHLÉ, S. YAMADA. *Efficient Public Trace and Revoke from Standard Assumptions*, in "Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS'2017", Dallas, United States, October 2017, https://hal.archives-ouvertes.fr/hal-01643498

[28] A. BLOT, J.-M. MULLER, L. THÉRY. *Formal correctness of comparison algorithms between binary64 and decimal64 floating-point numbers*, in "Numerical Software Verification", Heidelberg, Germany, Lecture Notes in Computer Science (LNCS), Springer, July 2017, n° 10381, https://hal.archives-ouvertes.fr/hal-01512294

[29] P. BOITO, Y. EIDELMAN, L. GEMIGNANI. *Efficient Solution of Shifted Quasiseparable Systems and Applications*, in "CMMSE 2017 - 17th International Conference on Computational and Mathematical Methods in Science and Engineering", Cadiz, Spain, July 2017, pp. 1-4, https://hal.inria.fr/hal-01644741

[30] S. BOLDO, M. JOLDES, J.-M. MULLER, V. POPESCU. *Formal Verification of a Floating-Point Expansion Renormalization Algorithm*, in "8th International Conference on Interactive Theorem Proving (ITP'2017)", Brasilia, Brazil, Lecture Notes in Computer Science, September 2017, vol. 10499, https://hal.archives-ouvertes.fr/hal-01512417

[31] G. CASTAGNOS, L. IMBERT, F. LAGUILLAUMIE. *Encryption Switching Protocols Revisited: Switching Modulo p*, in "CRYPTO 2017 - 37th International Cryptology Conference", Santa Barbara, United States, Advances in Cryptology – CRYPTO 2017, August 2017, vol. 10401, pp. 255-287 [*DOI :* 10.1007/978-3-319-63688-7_9], https://hal-lirmm.ccsd.cnrs.fr/lirmm-01587451

[32] J. CHEN, J. GONG. *ABE with Tag Made Easy: Concise Framework and New Instantiations in Prime-order Groups*, in "Asiacrypt 2017", Hong Kong, China, December 2017, https://hal.inria.fr/hal-01643435

[33] J. CHEN, J. GONG, J. WENG. *Tightly Secure IBE under Constant-size Master Public Key*, in "PKC 2017 - Public Key Cryptography", Amsterdam, Netherlands, March 2017, https://hal.inria.fr/hal-01643457

[34] G. HEROLD, M. HOFFMANN, M. KLOOSS, C. RÀFOLS, A. RUPP. *New Techniques for Structural Batch Verification in Bilinear Groups with Applications to Groth-Sahai Proofs*, in "Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security", Dallas, United States, 2017, https://hal.archives-ouvertes.fr/hal-01643558

[35] M. JOYE, B. LIBERT. *Encoding-Free ElGamal-Type Encryption Schemes on Elliptic Curves*, in "CT-RSA 2017 - RSA Conference 2017 – Cryptographers' Track", San Francisco, United States, LNCS, Springer, February 2017, vol. 10159, pp. 19 - 35 [*DOI :* 10.1007/978-3-540-72738-5_21], https://hal.inria.fr/hal-01621014

[36] C.-P. JEANNEROD, C. MONAT, L. THÉVENOUX. *More accurate complex multiplication for embedded processors*, in "12th IEEE International Symposium on Industrial Embedded Systems (SIES 2017)", Toulouse, France, June 2017, https://hal.archives-ouvertes.fr/hal-01512760

[37] C.-P. JEANNEROD, J.-M. MULLER, A. PLET. *The Classical Relative Error Bounds for Computing $\sqrt{a2}$ + b2 and c/ $\sqrt{a2}$ + b2 in Binary Floating-Point Arithmetic are Asymptotically Optimal*, in "ARITH-24 2017 - 24th IEEE Symposium on Computer Arithmetic", London, United Kingdom, Proceedings of the 24th IEEE Symposium on Computer Arithmetic, July 2017, 8 p. , https://hal-ens-lyon.archives-ouvertes.fr/ensl-01527202

[38] M. JOLDES, J.-M. MULLER, V. POPESCU. *Implementation and performance evaluation of an extended precision floating-point arithmetic library for high-accuracy semidefinite programming*, in "IEEE Symposium on Computer Arithmetic (Arith24)", London, United Kingdom, July 2017, https://hal.archives-ouvertes.fr/hal-01491255

[39] V. LEFÈVRE, P. ZIMMERMANN. *Optimized Binary64 and Binary128 Arithmetic with GNU MPFR*, in "24th IEEE Symposium on Computer Arithmetic (ARITH 24)", London, United Kingdom, July 2017, https://hal.inria.fr/hal-01502326

[40] B. LIBERT, S. LING, F. MOUHARTEM, K. NGUYEN, H. WANG. *Adaptive Oblivious Transfer with Access Control from Lattice Assumptions*, in "ASIACRYPT 2017 - Advances in Cryptology", Hong Kong, China, T. TAKAGI, T. PEYRIN (editors), International Conference on the Theory and Application of Cryptology and Information Security : Advances in Cryptology – ASIACRYPT 2017, Springer, December 2017, vol. 10624, pp. 533-563 [*DOI :* 10.1007/978-3-319-70694-8_19], https://hal.inria.fr/hal-01622197

[41] B. LIBERT, S. LING, K. NGUYEN, H. WANG. *Zero-Knowledge Arguments for Lattice-Based PRFs and Applications to E-Cash*, in "Asiacrypt 2017", Hong Kong, China, LNCS, Springer, December 2017, https://hal.inria.fr/hal-01621027

[42] B. LIBERT, T. PETERS, C. QIAN. *Structure-Preserving Chosen-Ciphertext Security with Shorter Verifiable Ciphertexts*, in "PKC 2017 - Public Key Cryptography", Amsterdam, Netherlands, LNCS, Springer, March 2017, vol. 10174, pp. 247 - 276 [*DOI :* 10.1007/BFB0054113], https://hal.inria.fr/hal-01621022

[43] B. LIBERT, A. SAKZAD, D. STEHLÉ, R. STEINFELD. *All-But-Many Lossy Trapdoor Functions and Selective Opening Chosen-Ciphertext Security from LWE*, in "Crypto 2017 - 37th International Cryptology Conference", Santa Barbara, United States, LNCS, Springer, August 2017, vol. 10403, pp. 332 - 364 [*DOI :* 10.1007/978-3-662-53018-4_18], https://hal.inria.fr/hal-01621025

[44] V. NEIGER, T. X. VU. *Computing Canonical Bases of Modules of Univariate Relations*, in "ISSAC '17 - 42nd International Symposium on Symbolic and Algebraic Computation", Kaiserslautern, Germany, July 2017, 8 p. , https://arxiv.org/abs/1705.10649 , https://hal.inria.fr/hal-01457979

[45] R. STEINFELD, A. SAKZAD, M. ROCA, D. STEHLÉ. *Middle-Product Learning with Errors*, in "Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference", Santa Barbara, United States, 2017, https://hal.archives-ouvertes.fr/hal-01643517

[46] G. VILLARD, E. KALTOFEN, L. ZHI, J.-G. DUMAS. *Polynomial Time Interactive Proofs for Linear Algebra with Exponential Matrix Dimensions and Scalars Given by Polynomial Time Circuits*, in "ISSAC 2017 - 42nd International Symposium on Symbolic and Algebraic Computation", Kaiserslautern, Germany, Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, ACM, July 2017, pp. 125-132 [*DOI :* 10.1145/3087604.3087640], https://hal.archives-ouvertes.fr/hal-01657873

### Conferences without Proceedings

[47] P. R. ARANTES GILZ, F. BRÉHARD, C. GAZZINO. *Validated Semi-Analytical Transition Matrices for Linearized Relative Spacecraft Dynamics via Chebyshev Series Approximations*, in "2018 Space Flight Mechanics Meeting, AIAA Science and Technology Forum and Exposition 2018", Kissimmee, United States, January 2018, pp. 1-23, https://hal.archives-ouvertes.fr/hal-01540170

### Scientific Books (or Scientific Book chapters)

[48] A. BOSTAN, F. CHYZAK, M. GIUSTI, R. LEBRETON, G. LECERF, B. SALVY, E. SCHOST. *Algorithmes Efficaces en Calcul Formel*, published by the Authors, 2017, Voir la page du livre à l'adresse https://hal.archives-ouvertes.fr/AECF/, https://hal.inria.fr/hal-01431717

[49] C.-P. JEANNEROD, N. REVOL. *Analyser et encadrer les erreurs dues à l'arithmétique flottante*, in "Informatique mathématique : une photographie en 2017", CNRS Editions, January 2017, pp. 115-144, https://hal.inria.fr/hal-01658296

### Books or Proceedings Editing

[50] B. SALVY (editor). *Informatique Mathématique. Une photographie en 2017*, CNRS éditions, January 2017, pp. 1-258, https://hal.inria.fr/hal-01658949

### Other Publications

[51] F. BRÉHARD, N. BRISEBARRE, M. JOLDES. *Validated and numerically efficient Chebyshev spectral methods for linear ordinary differential equations*, July 2017, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01526272

[52] F. BRÉHARD. *Fixed-Point Validation with Componentwise Error Enclosures and Application to Coupled Systems of Linear Ordinary Differential Equations* , December 2017, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01654396

[53] S.-I. FILIP, M. ISTOAN, F. DE DINECHIN, N. BRISEBARRE. *Automatic generation of hardware FIR filters from a frequency domain specification*, May 2017, working paper or preprint, https://hal.inria.fr/hal-01308377

[54] J. GONG, B. LIBERT, S. C. RAMANNA. *Compact IBBE and Fuzzy IBE from Simple Assumptions*, January 2018, working paper or preprint, https://hal.inria.fr/hal-01686690

[55] C.-P. JEANNEROD, V. NEIGER, G. VILLARD. *Fast computation of approximant bases in canonical form*, January 2018, working paper or preprint, https://hal-unilim.archives-ouvertes.fr/hal-01683632

[56] N. REVOL. *Influence of the Condition Number on Interval Computations: Illustration on Some Examples*, in honour of Vladik Kreinovich' 65th birthday, 2017, in honour of Vladik Kreinovich' 65th birthday, https://hal.inria.fr/hal-01588713

[57] D. STEHLÉ. *Lattice Reduction Algorithms*, 2017, Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2017, https://hal.archives-ouvertes.fr/hal-01643523