IN PARTNERSHIP WITH:
CNRS

Ecole normale supérieure de Lyon

Université Claude Bernard (Lyon 1)

Activity Report 2016

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:

1.1. - Architectures
2.4. - Verification, reliability, certification
4. - Security and privacy
7. - Fundamental Algorithmics

Other Research Topics and Application Domains:

9.4. - Sciences
9.8. - Privacy

1. Members

Research Scientists

Bruno Salvy [Team leader, Inria, Senior Researcher]
Nicolas Brisebarre [CNRS, Researcher]
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. Limoges, Associate Professor, from Sep 2016]
Guillaume Hanrot [ENS de Lyon, Professor, HDR]
Fabien Laguillaumie [Univ. Lyon I, Professor, HDR]
Nicolas Louvet [Univ. Lyon I, Associate Professor]
Clément Pernet [Univ. Grenoble I, Associate Professor, until Aug 2016, HDR]
Damien Stehlé [ENS de Lyon, Professor, HDR]

Engineers

Serge Torres [ENS de Lyon, Faculty Member]
Abderahman Cheniour [CNRS, until Jul 2016]
Laurent Thévenoux [Inria]

PhD Students

Florent Bréhard [ENS de Lyon]
Silviu Filip [ENS de Lyon, until Sep 2016]
Stephen Melczer [NSERC, cosupervision with Waterloo, Ontario, Canada]
Fabrice Mouhartem [ENS de Lyon]
Vincent Neiger [Inria, until Nov 2016]
Marie Paindavoine [ENS de Lyon and Orange Labs, CIFRE]
Alice Pellet-Mary [ENS de Lyon, since Sep 2016]
Antoine Plet [ENS de Lyon]
Valentina Popescu [ENS de Lyon]

Chen Qiang [Univ. de Rennes 1, from Mar to Aug 2016 as an intern from ENS Rennes, since Sep 2016 as a PhD student]
Weiqiang Wen [ENS de Lyon]

Post-Doctoral Fellows

Shi Bai [ENS de Lyon, until Nov 2016]
Sanjay Bhattacherjee [ENS de Lyon, until Nov 2016]
Jie Chen [ENS de Lyon, until Aug 2016]
Olga Kupriianova [ENS de Lyon, until Aug 2016]
Somindu Ramanna [ENS de Lyon, until Nov 2016]
Jinming Wen [ENS de Lyon, until Aug 2016]

Visiting Scientists

Elena Kirshanova [Ruhr-Univ. Bochum, Visiting PhD student, Feb and March 2016]
George Labahn [ENS de Lyon, Visiting Scientist, Apr 2016]
Jiangtao Li [East China Normal Univ., Visiting PhD student, from Sep 2016]
Miruna Rosca [BitDefender, Visiting Scientist, from Oct 2016]
Radu Titiu [BitDefender, Visiting Scientist, from Oct 2016]

Administrative Assistants

Evelyne Blesle [Inria]
Chiraz Benamor [ENS de Lyon]

Others

Balthazar Bauer [ENS de Lyon, Intern, from Mar to Aug 2016]
Qian Chen [ENS de Rennes, Intern, from Mar to Aug 2016]
Willy Quach [ENS de Lyon, Intern, from Feb to Jun 2016]
Vu Thi Xuan [ENS de Lyon, Intern, from May to Jul 2016]

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 2×2 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. New Software and Platforms

5.1. FPLLL

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 the LLL algorithm is central to the code, hence the name. It includes implementations of floating-point LLL reduction algorithms, offering different speed/guarantees ratios. It further includes an implementation of the BKZ reduction algorithm and variants thereof. It includes an 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. 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.

- Participants: Martin Albrecht, Shi Bai, Guillaume Bonnoron, Léo Ducas, Damien Stehlé and Marc Stevens
- Contact: Damien Stehlé
- URL: https://github.com/fplll/fplll

5.2. HPLLL

hplll is an experimental C++ library companion to fplll.

FUNCTIONAL DESCRIPTION

hplll provides a specific LLL reduction algorithm using Householder orthogonalization, and HPC preliminary solutions especially for integer relation finding.

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

5.3. 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.

There have been two new releases in 2016: 3.1.4 and 3.1.5. An MPFR-MPC developers meeting took place on 23 and 24 May 2016.

- Participants: Vincent Lefèvre and Paul Zimmermann
- Contact: Vincent Lefèvre
- URL: http://www.mpfr.org/

5.4. Gfun

A Maple package for solutions of linear differential or recurrence equations

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/

5.5. 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/

5.6. LinBox: a C++ library for exact, high-performance linear algebra computation

LinBox is a C++ template library for exact, high-performance linear algebra computation with dense, sparse, and structured matrices over the integers and over finite fields. LinBox is distributed under the LGPL license. The library is developed by a consortium of researchers in Canada, USA, and France. Clément Pernet is a main contributor, especially with a focus on parallel aspects during the period covered by this report.

- Participants: Clément Pernet, Gilles Villard
- Contact: Clément Pernet
- URL: http://www.linalg.org

6. New Results

6.1. Floating-point arithmetic

6.1.1. Parallel floating-point expansions for extended-precision GPU computations

GPUs are an important hardware development platform for problems where massive parallel computations are needed. Many of these problems require a higher precision than the standard double floating-point (FP) available. One common way of extending the precision is the multiple-component approach, in which real numbers are represented as the unevaluated sum of several standard machine precision FP numbers. This representation is called an FP expansion and it offers the simplicity of using directly available and highly optimized FP operations. In [30] we present new data-parallel algorithms for adding and multiplying FP expansions specially designed for extended precision computations on GPUs. These are generalized algorithms that can manipulate FP expansions of different sizes (from double-double up to a few tens of doubles) and ensure a certain worst case error bound on the results.

6.1.2. Error analysis of the Cornea-Harrison-Tang method

Assuming floating-point arithmetic with a fused multiply-add operation and rounding to nearest, the Cornea-Harrison-Tang method aims to evaluate expressions of the form $ab + cd$ with high relative accuracy. In [12] we provide a rounding error analysis of this method, which unlike previous studies is not restricted to binary floating-point arithmetic but holds for any radix β. We show first that an asymptotically optimal bound on the relative error of this method is $\frac{2\beta u+2u^2}{\beta-2u^2} = 2u + \frac{2}{\beta}u^2 + O(u^3)$, where $u = \frac{1}{2}\beta^{1-p}$ is the unit roundoff in radix β and precision p. Then we show that the possibility of removing the $O(u^2)$ term from this bound is governed by the radix parity and the tie-breaking strategy used for rounding: if β is odd or rounding is *to nearest even*, then the simpler bound $2u$ is obtained, while if β is even and rounding is *to nearest away*, then there exist floating-point inputs a, b, c, d that lead to a relative error larger than $2u + \frac{2}{\beta}u^2 - 4u^3$. All these results hold provided underflows and overflows do not occur and under some mild assumptions on β and p satisfied by IEEE 754-2008 formats.

6.1.3. Sharp error bounds for complex floating-point inversion

In [14] we study the accuracy of the classic algorithm for inverting a complex number given by its real and imaginary parts as floating-point numbers. Our analyses are done in binary floating-point arithmetic, with an unbounded exponent range and in precision p; we also assume that the basic arithmetic operations ($+$, $-$, $\times$, $/$) are rounded to nearest, so that the unit roundoff is $u = 2^{-p}$. We bound the largest relative error in the computed inverse either in the componentwise or in the normwise sense. We prove the componentwise relative error bound $3u$ for the complex inversion algorithm (assuming $p \geq 4$), and we show that this bound is asymptotically optimal (as $p \to \infty$) when p is even, and sharp when using one of the basic IEEE 754 binary formats with an odd precision ($p = 53, 113$). This componentwise bound obviously leads to the same bound $3u$ for the normwise relative error. However, we prove that the smaller bound $2.707131u$ holds (assuming $p \geq 24$) for the normwise relative error, and we illustrate the sharpness of this bound for the basic IEEE 754 binary formats ($p = 24, 53, 113$) using numerical examples.

6.1.4. On relative errors of floating-point operations: optimal bounds and applications

Rounding error analyses of numerical algorithms are most often carried out via repeated applications of the so-called standard models of floating-point arithmetic. Given a round-to-nearest function fl and barring underflow and overflow, such models bound the relative errors $E_1(t) = |t-\mathrm{fl}(t)|/|t|$ and $E_(t) = |t-\mathrm{fl}(t)|/|\mathrm{fl}(t)|$ by the unit roundoff u. With S. M. Rump (Hamburg University of Technology), we investigate in [15] the possibility and the usefulness of refining these bounds, both in the case of an arbitrary real t and in the case where t is the exact result of an arithmetic operation on some floating-point numbers. We show that $E_1(t)$ and $E_2(t)$ are optimally bounded by $u/(1 + u)$ and u, respectively, when t is real or, under mild assumptions on the base and the precision, when $t = x \pm y$ or $t = xy$ with x, y two floating-point numbers. We prove that while this remains true for division in base $\beta > 2$, smaller, attainable bounds can be derived for both division in base $\beta = 2$ and square root. This set of optimal bounds is then applied to the rounding error analysis of various numerical algorithms: in all cases, we obtain significantly shorter proofs of the best-known error bounds for such algorithms, and/or improvements on these bounds themselves.

6.1.5. Computing floating-point logarithms with fixed-point operations

Elementary functions from the mathematical library input and output floating-point numbers. However, it is possible to implement them purely using integer/fixed-point arithmetic. This option was not attractive between 1985 and 2005, because mainstream processor hardware supported 64-bit floating-point, but only 32-bit integers. Besides, conversions between floating-point and integer were costly. This has changed in recent years, in particular with the generalization of native 64-bit integer support. The purpose of this article is therefore to reevaluate the relevance of computing floating-point functions in fixed-point. For this, several variants of the double-precision logarithm function are implemented and evaluated. Formulating the problem as a fixed-point one is easy after the range has been (classically) reduced. Then, 64-bit integers provide slightly more accuracy than 53-bit mantissa, which helps speed up the evaluation. Finally, multi-word arithmetic, critical for accurate implementations, is much faster in fixed-point, and natively supported by recent compilers. Novel

techniques of argument reduction and rounding test are introduced in this context. Thanks to all this, a purely integer implementation of the correctly rounded double-precision logarithm outperforms the previous state of the art, with the worst-case execution time reduced by a factor 5. This work also introduces variants of the logarithm that input a floating-point number and output the result in fixed-point. These are shown to be both more accurate and more efficient than the traditional floating-point functions for some applications [35].

6.1.6. A library for symbolic floating-point arithmetic

To analyze a priori the accuracy of an algorithm in floating-point arithmetic, one usually derives a uniform error bound on the output, valid for most inputs and parametrized by the precision p. To show further that this bound is sharp, a common way is to build an input example for which the error committed by the algorithm comes close to that bound, or even attains it. Such inputs may be given as floating-point numbers in one of the IEEE standard formats (say, for $p = 53$) or, more generally, as expressions parametrized by p, that can be viewed as symbolic floating-point numbers. With such inputs, a sharpness result can thus be established for virtually all reasonable formats instead of just one of them. This, however, requires the ability to run the algorithm on those inputs and, in particular, to compute the correctly-rounded sum, product, or ratio of two symbolic floating-point numbers. We show in [61] how these basic arithmetic operations can be performed automatically. We introduce a way to model symbolic floating-point data, and present algorithms for round-to-nearest addition, multiplication, fused multiply-add, and division. An implementation as a Maple library is also described, and experiments using examples from the literature are provided to illustrate its interest in practice.

6.1.7. On the robustness of the 2Sum and Fast2Sum algorithms

The 2Sum and Fast2Sum algorithms are important building blocks in numerical computing. They are used (implicitly or explicitly) in many *compensated* algorithms (such as compensated summation or compensated polynomial evaluation). They are also used for manipulating floating-point *expansions*. We show in [56] 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.

6.1.8. Tight and rigourous error bounds for basic building blocks of double-word arithmetic

In [63] 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 wrong, and we provide a relative error bound. We introduce new algorithms for division. We also give examples that illustrate the tightness of our bounds.

6.1.9. A new multiplication algorithm for extended precision using floating-point expansions

Some important computational problems must use a floating-point (FP) precision several times higher than the hardware-implemented available one. These computations critically rely on software libraries for high-precision FP arithmetic. The representation of a high-precision data type crucially influences the corresponding arithmetic algorithms. Recent work showed that algorithms for FP expansions, that is, a representation based on unevaluated sum of standard FP types, benefit from various high-performance support for native FP, such as low latency, high throughput, vectorization, threading, etc. Bailey's QD library and its corresponding Graphics Processing Unit (GPU) version, GQD, are such examples. Despite using native FP arithmetic as the key operations, QD and GQD algorithms are focused on double-double or quad-double representations and do not generalize efficiently or naturally to a flexible number of components in the FP expansion. In [45] we introduce a new multiplication algorithm for FP expansion with flexible precision, up to the order of tens of FP elements in mind. The main feature consists in the partial products being accumulated in a special designed data structure that has the regularity of a fixed-point representation while allowing the computation to be naturally carried out using native FP types. This allows us to easily avoid unnecessary computation and

to present rigorous accuracy analysis transparently. The algorithm, its correctness and accuracy proofs and some performance comparisons with existing libraries are all contributions of this paper.

6.1.10. CAMPARY: Cuda Multiple Precision Arithmetic Library and Applications

Many scientific computing applications demand massive numerical computations on parallel architectures such as Graphics Processing Units (GPUs). Usually, either floating-point single or double precision arithmetic is used. Higher precision is generally not available in hardware, and software extended precision libraries are much slower and rarely supported on GPUs. We develop CAMPARY: a multiple-precision arithmetic library, using the CUDA programming language for the NVidia GPU platform. In our approach, the precision is extended by representing real numbers as the unevaluated sum of several standard machine precision floating-point numbers. We make use of error-free transforms algorithms, which are based only on native precision operations, but keep track of all rounding errors that occur when performing a sequence of additions and multiplications. This offers the simplicity of using hardware highly optimized floating-point operations, while also allowing for rigorously proven rounding error bounds. This also allows for easy implementation of an interval arithmetic. Currently, all basic multiple-precision arithmetic operations are supported. Our target applications are in chaotic dynamical systems or automatic control [34].

6.1.11. Arithmetic algorithms for extended precision using floating-point expansions

Many numerical problems require a higher computing precision than the one offered by standard floating-point (FP) formats. One common way of extending the precision is to represent numbers in a *multiple component* format. By using the so-called *floating-point expansions*, real numbers are represented as the unevaluated sum of standard machine precision FP numbers. This representation offers the simplicity of using directly available, hardware implemented and highly optimized, FP operations. It is used by multiple-precision libraries such as Bailey's QD or the analogue Graphics Processing Units (GPU) tuned version, GQD. In this article we briefly revisit algorithms for adding and multiplying FP expansions, then we introduce and prove new algorithms for normalizing, dividing and square rooting of FP expansions. The new method used for computing the reciprocal a^{-1} and the square root $\sqrt{a}$ of an FP expansion a is based on an adapted Newton-Raphson iteration where the intermediate calculations are done using "truncated" operations (additions, multiplications) involving FP expansions. We give here a thorough error analysis showing that it allows very accurate computations. More precisely, after q iterations, the computed FP expansion $x = x_0 + \cdots + x_{2^q-1}$ satisfies, for the reciprocal algorithm, the relative error bound: $|(x - a^{-1})/a^{-1}| \leq 2^{-2^q(p-3)-1}$ and, respectively, for the square root one: $|x - 1/\sqrt{a}| \leq 2^{-2^q(p-3)-1}/\sqrt{a}$, where $p > 2$ is the precision of the FP representation used ($p = 24$ for single precision and $p = 53$ for double precision) [16].

6.1.12. Comparison between binary and decimal floating-point numbers

We introduce an algorithm to compare a binary floating-point (FP) number and a decimal FP number, assuming the "binary encoding" of the decimal formats is used, and with a special emphasis on the basic interchange formats specified by the IEEE 754-2008 standard for FP arithmetic. It is a two-step algorithm: a first pass, based on the exponents only, quickly eliminates most cases, then, when the first pass does not suffice, a more accurate second pass is performed. We provide an implementation of several variants of our algorithm, and compare them [8].

6.1.13. Automatic source-to-source error compensation of floating-point programs: code synthesis to optimize accuracy and time

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. With Ph. Langlois and M. Martel (LIRMM and Université de Perpignan), we show in [21] how to automatically improve the numerical quality of a numerical program with the smallest impact on its performance. 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 user-defined trade-offs are achievable in a reasonable amount of time, with the help of the tools we present here.

6.1.14. Correctly rounded arbitrary-precision floating-point summation

We have designed a fast, low-level algorithm to compute the correctly rounded summation of several floating-point numbers in arbitrary precision in radix 2, each number (each input and the output) having its own precision. We have implemented it in GNU MPFR; it will be part of the next MPFR major release (GNU MPFR 4.0). In addition to a pen-and-paper proof, various kinds of tests are provided. Timings show that this new algorithm/implementation is globally much faster and takes less memory than the previous one (from MPFR 3.1.5): the worst-case time and memory complexity was exponential and it is now polynomial. Timings on pseudo-random inputs with various sets of parameters also show that this new implementation is even much faster than the (inaccurate) basic sum implementation in some cases. [36], [65]

6.2. Lattices: algorithms and cryptology

6.2.1. Zero-Knowledge Arguments for Lattice-Based Accumulators: Logarithmic-Size Ring Signatures and Group Signatures Without Trapdoors

An accumulator is a function that hashes a set of inputs into a short, constant-size string while preserving the ability to efficiently prove the inclusion of a specific input element in the hashed set. It has proved useful in the design of numerous privacy-enhancing protocols, in order to handle revocation or simply prove set membership. In the lattice setting, currently known instantiations of the primitive are based on Merkle trees, which do not interact well with zero-knowledge proofs. In order to efficiently prove the membership of some element in a zero-knowledge manner, the prover has to demonstrate knowledge of a hash chain without revealing it, which is not known to be efficiently possible under well-studied hardness assumptions. In [39], we provide an efficient method of proving such statements using involved extensions of Stern's protocol. Under the Small Integer Solution assumption, we provide zero-knowledge arguments showing possession of a hash chain. As an application, [39] describes new lattice-based group and ring signatures in the random oracle model. In particular, the paper obtains: (i) The first lattice-based ring signatures with logarithmic size in the cardinality of the ring; (ii) The first lattice-based group signature that does not require any GPV trapdoor and thus allows for a much more efficient choice of parameters.

6.2.2. A Lattice-Based Group Signature Scheme with Message-Dependent Opening

Group signatures are an important anonymity primitive allowing users to sign messages while hiding in a crowd. At the same time, signers remain accountable since an authority is capable of de-anonymizing signatures via a process called opening. In many situations, this authority is granted too much power as it can identify the author of any signature. Sakai et al. proposed a flavor of the primitive, called Group Signature with Message-Dependent Opening (GS-MDO), where opening operations are only possible when a separate authority (called "admitter") has revealed a trapdoor for the corresponding message. So far, all existing GS-MDO constructions rely on bilinear maps, partially because the message-dependent opening functionality inherently implies identity-based encryption. In [40], the team proposes the first GS-MDO candidate based on lattice assumptions. The construction combines the group signature of Ling, Nguyen and Wang (PKC'15) with two layers of identity-based encryption. These components are tied together using suitable zero-knowledge argument systems.

6.2.3. Practical "Signatures with Efficient Protocols" from Simple Assumptions

Digital signatures are perhaps the most important base for authentication and trust relationships in large scale systems. More specifically, various applications of signatures provide privacy and anonymity preserving mechanisms and protocols, and these, in turn, are becoming critical (due to the recently recognized need to protect individuals according to national rules and regulations). A specific type of signatures called "signatures

with efficient protocols", as introduced by Camenisch and Lysyanskaya (CL), efficiently accommodates various basic protocols and extensions like zero-knowledge proofs, signing committed messages, or re-randomizability. These are, in fact, typical operations associated with signatures used in typical anonymity and privacy-preserving scenarios. To date there are no "signatures with efficient protocols" which are based on simple assumptions and truly practical. These two properties assure us a robust primitive: First, simple assumptions are needed for ensuring that this basic primitive is mathematically robust and does not require special ad hoc assumptions that are more risky, imply less efficiency, are more tuned to the protocol itself, and are perhaps less trusted. In the other dimension, efficiency is a must given the anonymity applications of the protocol, since without proper level of efficiency the future adoption of the primitives is always questionable (in spite of their need). In [41], the team presents a new CL-type signature scheme that is re-randomizable under a simple, well-studied, and by now standard, assumption (SXDH). The signature is efficient (built on the recent QA-NIZK constructions), and is, by design, suitable to work in extended contexts that typify privacy settings (like anonymous credentials, group signature, and offline e-cash). The paper demonstrates its power by presenting practical protocols based on it.

6.2.4. *Functional Commitment Schemes: From Polynomial Commitments to Pairing-Based Accumulators from Simple Assumptions*

In [42], the team formalizes a cryptographic primitive called functional commitment (FC) which can be viewed as a generalization of vector commitments (VCs), polynomial commitments and many other special kinds of commitment schemes. A non-interactive functional commitment allows committing to a message in such a way that the committer has the flexibility of only revealing a function $F(M)$ of the committed message during the opening phase. We provide constructions for the functionality of linear functions, where messages consist of a vectors of n elements over some domain D (e.g., $m = (m_1, ..., m_n) \in D_n$) and commitments can later be opened to a specific linear function of the vector coordinates. An opening for a function $F : D_n \rightarrow R$ thus generates a witness for the fact that $F(m)$ indeed evaluates to $y \in R$. One security requirement is called function binding and requires that no adversary be able to open a commitment to two different evaluations y, y' for the same function F. The paper [42] proposes a construction of functional commitment for linear functions based on constant-size assumptions in composite order groups endowed with a bilinear map. The construction has commitments and openings of constant size (i.e., independent of n or function description) and is perfectly hiding – the underlying message is information theoretically hidden. Our security proofs builds on the Déjà Q framework of Chase and Meiklejohn (Eurocrypt 2014) and its extension by Wee (TCC 2016) to encryption primitives, thus relying on constant-size subgroup decisional assumptions. The paper shows that the FC for linear functions are sufficiently powerful to solve four open problems. They, first, imply polynomial commitments, and, then, give cryptographic accumulators (i.e., an algebraic hash function which makes it possible to efficiently prove that some input belongs to a hashed set). In particular, specializing the new FC construction leads to the first pairing-based polynomial commitments and accumulators for large universes known to achieve security under simple assumptions. We also substantially extend our pairing-based accumulator to handle subset queries which requires a non-trivial extension of the Déjà Q framework.

6.2.5. *Fully Secure Functional Encryption for Inner Products, from Standard Assumptions*

Functional encryption is a modern public-key paradigm where a master secret key can be used to derive sub-keys SKF associated with certain functions F in such a way that the decryption operation reveals $F(M)$, if M is the encrypted message, and nothing else. Recently, Abdalla *et al.* gave simple and efficient realizations of the primitive for the computation of linear functions on encrypted data: given an encryption of a vector y over some specified base ring, a secret key SK_x for the vector x allows computing $\langle x, y \rangle$. Their technique surprisingly allows for instantiations under standard assumptions, like the hardness of the Decision Diffie-Hellman (DDH) and Learning-with-Errors (LWE) problems. Their constructions, however, are only proved secure against selective adversaries, which have to declare the challenge messages M_0 and M_1 at the outset of the game. In [22], we provide constructions that provably achieve security against more realistic adaptive attacks (where the messages M_0 and M_1 may be chosen in the challenge phase, based on the previously collected information) for the same inner product functionality. The constructions of [22] are obtained from hash proof systems endowed with homomorphic properties over the key space. They are (almost) as efficient as

those of Abdalla *et al.* and rely on the same hardness assumptions. In addition, the paper [22] obtains a solution based on Paillier's composite residuosity assumption, which was an open problem even in the case of selective adversaries. We also propose LWE-based schemes that allow evaluation of inner products modulo a prime p, as opposed to the schemes of Abdalla et al. that are restricted to evaluations of integer inner products of short integer vectors. The paper [22] finally proposes a solution based on Paillier's composite residuosity assumption that enables evaluation of inner products modulo an RSA integer $N = pq$. The paper [22] demonstrates that the functionality of inner products over a prime field is powerful and can be used to construct bounded collusion FE for all circuits.

6.2.6. *Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions*

A recent line of works – initiated by Gordon, Katz and Vaikuntanathan (Asiacrypt 2010) – gave lattice-based realizations of privacy-preserving protocols allowing users to authenticate while remaining hidden in a crowd. Despite five years of efforts, known constructions remain limited to static populations of users, which cannot be dynamically updated. For example, none of the existing lattice-based group signatures seems easily extendable to the more realistic setting of dynamic groups. In [37], the team provides new tools enabling the design of anonymous authen-tication systems whereby new users can register and obtain credentials at any time. The first contribution of [37] is a signature scheme with efficient protocols, which allows users to obtain a signature on a committed value and subsequently prove knowledge of a signature on a committed message. This construction, which builds on the lattice-based signature of Böhl *et al.* (Eurocrypt'13), is well-suited to the design of anonymous credentials and dynamic group signatures. As a second technical contribution, [37] provides a simple, round-optimal joining mechanism for introducing new members in a group. This mechanism consists of zero-knowledge arguments allowing registered group members to prove knowledge of a secret short vector of which the corresponding public syndrome was certified by the group manager. This method provides similar advantages to those of structure-preserving signatures in the realm of bilinear groups. Namely, it allows group members to generate their public key on their own without having to prove knowledge of the underlying secret key. This results in a two-round join protocol supporting concurrent enrollments, which can be used in other settings such as group encryption.

6.2.7. *Zero-Knowledge Arguments for Matrix-Vector Relations and Lattice-Based Group Encryption*

Group encryption (GE) is the natural encryption analogue of group signatures in that it allows verifiably encrypting messages for some anonymous member of a group while providing evidence that the receiver is a properly certified group member. Should the need arise, an opening authority is capable of identifying the receiver of any ciphertext. As introduced by Kiayias, Tsiounis and Yung (Asiacrypt'07), GE is motivated by applications in the context of oblivious retriever storage systems, anonymous third parties and hierarchical group signatures. In [38], we provide the first realization of group encryption under lattice assumptions. The construction of [38] is proved secure in the standard model (assuming interaction in the proving phase) under the Learning-With-Errors (LWE) and Short-Integer-Solution (SIS) assumptions. As a crucial component of our system, [38] describes a new zero-knowledge argument system allowing to demonstrate that a given ciphertext is a valid encryption under some hidden but certified public key, which incurs to prove quadratic statements about LWE relations. Specifically, the protocol of [38] allows arguing knowledge of witnesses consisting of $X \in \mathbb{Z}_q^{m\times}$, $s \in \mathbb{Z}_q^n$ and a small-norm $e \in \mathbb{Z}^m$ which underlie a public vector $b = X \cdot s + e \in \mathbb{Z}_q^m$ while simultaneously proving that the matrix $X \in \mathbb{Z}_q^{m\times n}$ has been correctly certified.

6.2.8. *Efficient Cryptosystems From 2^k-th Power Residue Symbols*

Goldwasser and Micali (1984) highlighted the importance of randomizing the plaintext for public-key encryption and introduced the notion of semantic security. They also realized a cryptosystem meeting this security notion under the standard complexity assumption of deciding quadratic residuosity modulo a composite number. The Goldwasser-Micali cryptosystem is simple and elegant but is quite wasteful in bandwidth when encrypting large messages. A number of works followed to address this issue and proposed

various modifications. In [4], we revisit the original Goldwasser-Micali cryptosystem using 2^k-th power residue symbols. The so-obtained cryptosystems appear as a very natural generalization for $k \geq 2$ (the case $k = 1$ corresponds exactly to the Goldwasser-Micali cryptosystem). Advantageously, they are efficient in both bandwidth and speed; in particular, they allow for fast decryption. Further, the cryptosystems described in this paper inherit the useful features of the original cryptosystem (like its homomorphic property) and are shown to be secure under a similar complexity assumption. As a prominent application, the paper [4] describes an efficient lossy trapdoor function based thereon.

6.2.9. Born and raised distributively: Fully distributed non-interactive adaptively-secure threshold signatures with short shares

Threshold cryptography is a fundamental distributed computational paradigm for enhancing the availability and the security of cryptographic public-key schemes. It does it by dividing private keys into n shares handed out to distinct servers. In threshold signature schemes, a set of at least $t + 1 \leq n$ servers is needed to produce a valid digital signature. Availability is assured by the fact that any subset of $t + 1$ servers can produce a signature when authorized. At the same time, the scheme should remain robust (in the fault tolerance sense) and unforgeable (cryptographically) against up to t corrupted servers; i.e., it adds quorum control to traditional cryptographic services and introduces redundancy. Originally, most practical threshold signatures have a number of demerits: They have been analyzed in a static corruption model (where the set of corrupted servers is fixed at the very beginning of the attack); they require interaction; they assume a trusted dealer in the key generation phase (so that the system is not fully distributed); or they suffer from certain overheads in terms of storage (large share sizes). In [17], we construct practical fully distributed (the private key is born distributed), non-interactive schemes – where the servers can compute their partial signatures without communication with other servers – with adaptive security (i.e., the adversary corrupts servers dynamically based on its full view of the history of the system). The schemes of [17] are very efficient in terms of computation, communication, and scalable storage (with private key shares of size $O(1)$, where certain solutions incur $O(n)$ storage costs at each server). Unlike other adaptively secure schemes, the new schemes [17] are erasure-free (reliable erasure is hard to assure and hard to administer properly in actual systems). To the best of our knowledge, such a fully distributed highly constrained scheme has been an open problem in the area. In particular, and of special interest, is the fact that Pedersen's traditional distributed key generation (DKG) protocol can be safely employed in the initial key generation phase when the system is born although it is well-known not to ensure uniformly distributed public keys. An advantage of this is that this protocol only takes one round optimistically (in the absence of faulty player).

6.2.10. Non-Zero Inner Product Encryption with Short Ciphertexts and Private Keys

In [28], the team describes two constructions of non-zero inner product encryption (NIPE) systems in the public index setting, both having ciphertexts and secret keys of constant size. Both schemes are obtained by tweaking the Boneh-Gentry-Waters broadcast encryption system (Crypto 2005) and are proved selectively secure without random oracles under previously considered assumptions in groups with a bilinear map. Our first realization builds on prime-order bilinear groups and is proved secure under the Decisional Bilinear Diffie-Hellman Exponent assumption, which is parameterized by the length n of vectors over which the inner product is defined. By moving to composite order bilinear groups, the paper [28] obtains security under static subgroup decision assumptions following the Déjà Q framework of Chase and Meiklejohn (Eurocrypt 2014) and its extension by Wee (TCC 2016). The schemes of [28] are the first NIPE systems to achieve such parameters, even in the selective security setting. Moreover, they are the first proposals to feature optimally short private keys, which only consist of one group element. The prime-order-group realization of [28] is also the first one with a deterministic key generation mechanism.

6.2.11. More Efficient Constructions for Inner-Product Encryptions

In [48], the team describes new constructions for inner product encryption (called IPE1 and IPE2), which are both secure under the eXternal Diffie-Hellman assumption (SXDH) in asymmetric pairing groups. The IPE1 scheme of [48] has constant-size ciphertexts whereas the second one is weakly attribute hiding. The second scheme is derived from the identity-based encryption scheme of Jutla and Roy (Asiacrypt 2013), that

was extended from tag-based quasi-adaptive non-interactive zero-knowledge (QA-NIZK) proofs for linear subspaces of vector spaces over bilinear groups. The verifier common reference string (CRS) in these tag-based systems are split into two parts, that are combined during verification. The paper [48] considers an alternate form of the tag-based QA-NIZK proof with a single verifier CRS that already includes a tag, different from the one defining the language. The verification succeeds as long as the two tags are unequal. Essentially, we embed a two-equation revocation mechanism in the verification. The new QA-NIZK proof system leads to IPE1, a constant-sized ciphertext IPE scheme with very short ciphertexts. Both the IPE schemes are obtained by applying the n-equation revocation technique of Attrapadung and Libert (PKC 2010) to the corresponding identity based encryption schemes and proved secure under SXDH assumption. As an application, the paper [48] shows how the new schemes can be specialized to obtain the first fully secure identity-based broadcast encryption based on SXDH with a trade-off among the public parameters, ciphertext and key sizes, all of them being sub-linear in the maximum number of recipients of a broadcast.

6.2.12. Verifiable Message-Locked Encryption

One of today's main challenge related to cloud storage is to maintain the functionalities and the efficiency of customers' and service providers' usual environments, while protecting the confidentiality of sensitive data. Deduplication is one of those functionalities: it enables cloud storage providers to save a lot of memory by storing only once a file uploaded several times. But classical encryption blocks deduplication. One needs to use a "message-locked encryption" (MLE), which allows the detection of duplicates and the storage of only one encrypted file on the server, which can be decrypted by any owner of the file. However, in most existing scheme, a user can bypass this deduplication protocol. In [27], we provide servers verifiability for MLE schemes: the servers can verify that the ciphertexts are well-formed. This property that we formally define forces a customer to prove that she complied to the deduplication protocol, thus preventing her to deviate from *the prescribed functionality* of MLE. We call it *deduplication consistency*. To achieve this deduplication consistency, we provide (i) a generic transformation that applies to any MLE scheme and (ii) an ElGamal-based deduplication-consistent MLE, which is secure in the random oracle model.

6.2.13. Privately Outsourcing Exponentiation to a Single Server: Cryptanalysis and Optimal Constructions

In [29], we address the problem of speeding up group computations in cryptography using a single untrusted computational resource. We analyze the security of an efficient protocol for securely outsourcing multi-exponentiations proposed at ESORICS 2014. We show that this scheme does not achieve the claimed security guarantees and we present several practical polynomial-time attacks on the delegation protocol which allows the untrusted helper to recover part (or the whole) of the device secret inputs. We then provide simple constructions for outsourcing group exponentiations in different settings (e.g. public/secret, fixed/variable bases and public/secret exponents). Finally, we prove that our attacks on the ESORICS 2014 protocol are unavoidable if one wants to use a single untrusted computational resource and to limit the computational cost of the limited device to a constant number of (generic) group operations. In particular, we show that our constructions are actually optimal.

6.3. Algebraic computing and high-performance kernels

6.3.1. 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 [6].

6.3.2. 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 products 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 the appearance of spurious singularities that afflicts discrete creative telescoping, both in theory and in practice [7].

6.3.3. Fast and Accurate Computation of Orbital Collision Probability for Short-Term Encounters

We provide a new method for computing the probability of collision between two spherical space objects involved in a short-term encounter under Gaussian-distributed uncertainty. In this model of conjunction, classical assumptions reduce the probability of collision to the integral of a two-dimensional Gaussian probability density function over a disk. The computational method is based on an analytic expression for the integral, derived by use of Laplace transform and D-finite functions properties. The formula has the form of a product between an exponential term and a convergent power series with positive coefficients. Analytic bounds on the truncation error are also derived and are used to obtain a very accurate algorithm. Another contribution is the derivation of analytic bounds on the probability of collision itself, allowing for a very fast and — in most cases — very precise evaluation of the risk. The only other analytical method of the literature — based on an approximation — is shown to be a special case of the new formula. A numerical study illustrates the efficiency of the proposed algorithms on a broad variety of examples and favorably compares the approach to the other methods of the literature [20].

6.3.4. Efficient Algorihtms for Mixed Creative Telescoping

Creative telescoping is a powerful computer algebra paradigm — initiated by Doron Zeilberger in the 90's — for dealing with definite integrals and sums with parameters. We address the mixed continuous-discrete case, and focus on the integration of bivariate hypergeometric-hyperexponential terms. We design a new creative telescoping algorithm operating on this class of inputs, based on a Hermite-like reduction procedure. The new algorithm has two nice features: it is efficient and it delivers, for a suitable representation of the input, a minimal-order telescoper. Its analysis reveals tight bounds on the sizes of the telescoper it produces [26].

6.3.5. Symbolic-Numeric Tools for Analytic Combinatorics in Several Variables

Analytic combinatorics studies the asymptotic behaviour of sequences through the analytic properties of their generating functions. This article provides effective algorithms required for the study of analytic combinatorics in several variables, together with their complexity analyses. Given a multivariate rational function we show how to compute its smooth isolated critical points, with respect to a polynomial map encoding asymptotic behaviour, in complexity singly exponential in the degree of its denominator. We introduce a numerical Kronecker representation for solutions of polynomial systems with rational coefficients and show that it can be used to decide several properties (0 coordinate, equal coordinates, sign conditions for real solutions, and vanishing of a polynomial) in good bit complexity. Among the critical points, those that are minimal—a property governed by inequalities on the moduli of the coordinates—typically determine the dominant asymptotics of the diagonal coefficient sequence. When the Taylor expansion at the origin has all non-negative coefficients (known as the 'combinatorial case') and under regularity conditions, we utilize this Kronecker

representation to determine probabilistically the minimal critical points in complexity singly exponential in the degree of the denominator, with good control over the exponent in the bit complexity estimate. Generically in the combinatorial case, this allows one to automatically and rigorously determine asymptotics for the diagonal coefficient sequence. Examples obtained with a preliminary implementation show the wide applicability of this approach [43].

6.3.6. Tableau sequences, open diagrams, and Baxter families

Walks on Young's lattice of integer partitions encode many objects of algebraic and combinatorial interest. Chen *et al.* established connections between such walks and arc diagrams. We show that walks that start at $\varnothing$, end at a row shape, and only visit partitions of bounded height are in bijection with a new type of arc diagram — open diagrams. Remarkably, two subclasses of open diagrams are equinumerous with well known objects: standard Young tableaux of bounded height, and Baxter permutations. We give an explicit combinatorial bijection in the former case, and a generating function proof and new conjecture in the second case [9].

6.3.7. On 3-dimensional lattice walks confined to the positive octant

Many recent papers deal with the enumeration of 2-dimensional walks with prescribed steps confined to the positive quadrant. The classification is now complete for walks with steps in $\{0,\pm 1\}^2$: the generating function is differentially finite if and only if a certain group associated with the step set is finite. We explore in this paper the analogous problem for 3-dimensional walks confined to the positive octant. The first difficulty is their number: we have to examine no less than 11074225 step sets in $\{0,\pm 1\}^3$ (instead of 79 in the quadrant case). We focus on the 35548 that have at most six steps. We apply to them a combined approach, first experimental and then rigorous. On the experimental side, we try to guess differential equations. We also try to determine if the associated group is finite. The largest finite groups that we find have order 48 — the larger ones have order at least 200 and we believe them to be infinite. No differential equation has been detected in those cases. On the rigorous side, we apply three main techniques to prove D-finiteness. The algebraic kernel method, applied earlier to quadrant walks, works in many cases. Certain, more challenging, cases turn out to have a special Hadamard structure, which allows us to solve them via a reduction to problems of smaller dimension. Finally, for two special cases, we had to resort to computer algebra proofs. We prove with these techniques all the guessed differential equations. This leaves us with exactly 19 very intriguing step sets for which the group is finite, but the nature of the generating function still unclear [5].

6.3.8. Asymptotic Lattice Path Enumeration Using Diagonals

We consider d-dimensional lattice path models restricted to the first orthant whose defining step sets exhibit reflective symmetry across every axis. Given such a model, we provide explicit asymptotic enumerative formulas for the number of walks of a fixed length: the exponential growth is given by the number of distinct steps a model can take, while the sub-exponential growth depends only on the dimension of the underlying lattice and the number of steps moving forward in each coordinate. The generating function of each model is first expressed as the diagonal of a multivariate rational function, then asymptotic expressions are derived by analyzing the singular variety of this rational function. Additionally, we show how to compute subdominant growth, reflect on the difference between rational diagonals and differential equations as data structures for D-finite functions, and show how to determine first order asymptotics for the subset of walks that start and end at the origin [18].

6.3.9. Asymptotics of lattice walks via analytic combinatorics in several variables

We consider the enumeration of walks on the two-dimensional non-negative integer lattice with steps defined by a finite set $S \subset \{0,\pm 1\}^2$. Up to isomorphism there are 79 unique two-dimensional models to consider, and previous work in this area has used the kernel method, along with a rigorous computer algebra approach, to show that 23 of the 79 models admit D-finite generating functions. In 2009, Bostan and Kauers used Padé-Hermite approximants to guess differential equations which these 23 generating functions satisfy, in the process guessing asymptotics of their coefficient sequences. In this article we provide, for the first time, a complete rigorous verification of these guesses. Our technique is to use the kernel method to express 19 of

the 23 generating functions as diagonals of tri-variate rational functions and apply the methods of analytic combinatorics in several variables (the remaining 4 models have algebraic generating functions and can thus be handled by univariate techniques). This approach also shows the link between combinatorial properties of the models and features of its asymptotics such as asymptotic and polynomial growth factors. In addition, we give expressions for the number of walks returning to the x-axis, the y-axis, and the origin, proving recently conjectured asymptotics of Bostan, Chyzak, van Hoeij, Kauers, and Pech [44].

6.3.10. Linear Time Interactive Certificates

With J.G. Dumas (LJK, Grenoble), E. Kaltofen (NCSU, USA), and E. Thomé (Inria Nancy) we work on interactive certificates. Computational problem certificates are additional data structures for each output, which can be used by a (possibly randomized) verification algorithm that proves the correctness of each output. In [32] we give a new certificate for the minimal polynomial of sparse or structured matrices whose Monte Carlo verification complexity requires a single matrix-vector multiplication and a linear number of extra field operations (sufficiently large cardinality field). We also propose a novel preconditioner that ensures irreducibility of the characteristic polynomial of the generically preconditioned matrix. This preconditioner takes linear time to be applied and uses only two random entries. We combine these two techniques to give algorithms that compute certificates for the determinant, and thus for the characteristic polynomial, whose Monte Carlo verification complexity is therefore also linear.

6.3.11. Computing minimal interpolation bases

With É. Schost (U. Waterloo, Canada), we consider the problem of computing minimal bases of solutions for a general interpolation problem, which encompasses Hermite-Padé approximation and constrained multivariate interpolation, and has applications in coding theory and security. The problem is classically solved using iterative algorithms based on recurrence relations. First, we discuss in [62] 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 σ it uses $\widetilde{O}(m^{\omega-1}(\sigma+|s|))$ field operations, where the notation $\widetilde{O}(\cdot)$ indicates that logarithmic terms are omitted, $\omega \in [2, 2.38]$ is the exponent of matrix multiplication, and $|s|$ is the sum of the entries of the input shift s, with $\min(s) = 0$. 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. Then we propose in [33] an algorithm for the computation of an interpolation basis in shifted-Popov normal form with a cost of $\widetilde{O}(m^{\omega-1}\sigma)$ field operations. Previous works, in the case of Hermite-Padé approximation and in the general interpolation case, compute non-normalized bases. Since for arbitrary shifts such bases may have size $\Theta(m^2\sigma)$, the cost bound $\widetilde{O}(m^{\omega-1}\sigma)$ was feasible only with restrictive assumptions on the shift that ensure small output sizes. The question of handling arbitrary shifts with the same complexity bound was left open. To obtain the target cost for any shift, we strengthen the properties of the output bases, and of those obtained during the course of the algorithm: all the bases are computed in shifted Popov form, whose size is always $O(m\sigma)$. Then, we design a divide-and-conquer scheme. We recursively reduce the initial interpolation problem to sub-problems with more convenient shifts by first computing information on the degrees of the intermediate bases.

6.3.12. Fast computation of shifted Popov forms of polynomial matrices via systems of modular polynomial equations

In [46] we give a Las Vegas algorithm which computes the shifted Popov form of an $m \times m$ nonsingular polynomial matrix of degree d in expected $\widetilde{O}(m^\omega d)$ field operations, where ω is the exponent of matrix multiplication and $\widetilde{O}(\cdot)$ indicates that logarithmic factors are omitted. This is the first algorithm in $\widetilde{O}(m^\omega d)$ for shifted row reduction with arbitrary shifts. Using partial linearization, we reduce the problem to the case $d \leq \lceil \sigma/m \rceil$ where σ is the generic determinant bound, with σ/m bounded from above by both the average row degree and the average column degree of the matrix. The cost above becomes $\widetilde{O}(m^\omega \lceil \sigma/m \rceil)$, improving upon the cost of the fastest previously known algorithm for row reduction, which is deterministic. Our algorithm first builds a system of modular equations whose solution set is the row space of the input matrix, and then finds

the basis in shifted Popov form of this set. We give a deterministic algorithm for this second step supporting arbitrary moduli in $\widetilde{O}(m^{\omega-1}\sigma)$ field operations, where m is the number of unknowns and σ is the sum of the degrees of the moduli. This extends previous results with the same cost bound in the specific cases of order basis computation and M-Padé approximation, in which the moduli are products of known linear factors.

6.3.13. Fast, deterministic computation of the Hermite normal form and determinant of a polynomial matrix

With G. Labahn and W. Zhou (U. Waterloo, Canada) we give in [64] fast and deterministic algorithms to compute the determinant and Hermite normal form of a nonsingular $n \times n$ matrix of univariate polynomials over a field $\mathbb{K}$. Our algorithms use $\widetilde{O}(n^{\omega}\lceil s \rceil)$ operations in $\mathbb{K}$, 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 ω is the exponent of matrix multiplication. The soft-O notation indicates that logarithmic factors in the big-O are omitted while 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.

6.3.14. Fast Computation of the Rank Profile Matrix and the Generalized Bruhat Decomposition

The row (resp. column) rank profile of a matrix describes the stair-case shape of its row (resp. column) echelon form. With J. G. Dumas and Z. Sultan (LJK, Grenoble), we propose in [11] a new matrix invariant, the rank profile matrix, summarizing all information on the row and column rank profiles of all the leading sub-matrices. We show that this normal form exists and is unique over any ring, provided that the notion of McCoy's rank is used, in the presence of zero divisors. We then explore the conditions for a Gaussian elimination algorithm to compute all or part of this invariant, through the corresponding PLUQ decomposition. This enlarges the set of known Elimination variants that compute row or column rank profiles. As a consequence a new Crout base case variant significantly improves the practical efficiency of previously known implementations over a finite field. With matrices of very small rank, we also generalize the techniques of Storjohann and Yang to the computation of the rank profile matrix, achieving an $(r^{\omega} + mn)^{1+o(1)}$ time complexity for an $m \times n$ matrix of rank r, where ω is the exponent of matrix multiplication. Finally, by give connections to the Bruhat decomposition, and several of its variants and generalizations. Thus, our algorithmic improvements for the PLUQ factorization, and their implementations, directly apply to these decompositions. In particular, we show how a PLUQ decomposition revealing the rank profile matrix also reveals both a row and a column echelon form of the input matrix or of any of its leading sub-matrices, by a simple post-processing made of row and column permutations.

6.3.15. Computing with quasiseparable matrices

The class of quasiseparable matrices is defined by a pair of bounds, called the quasiseparable orders, on the ranks of the sub-matrices entirely located in their strictly lower and upper triangular parts. These arise naturally in applications, as e.g. the inverse of band matrices, and are widely used for they admit structured representations allowing to compute with them in time linear in the dimension. In [47] we show the connection between the notion of quasiseparability and the rank profile matrix invariant of Dumas et al. This allows us to propose an algorithm computing the quasiseparable orders (r_L, r_U) in time $O(n^2 s^{\omega-2})$, where $s = \max(r_L, r_U)$ and ω is the exponent of matrix multiplication. We then present two new structured representations, a binary tree of PLUQ decompositions, and the Bruhat generator, using respectively $O(ns\log(n/s))$ and $O(ns)$ field elements instead of $O(ns^2)$ for the classical generator and $O(nslogn)$ for the hierarchically semiseparable representations. We present algorithms computing these representations in time $O(n^2 s^{\omega-2})$. These representations allow a matrix-vector product in time linear in the size of their representation. Lastly we show how to multiply two such structured matrices in time $O(n^2 s^{\omega-2})$.

6.3.16. A Real QZ Algorithm for Structured Companion Pencils

With Y. Eidelman (U. Tel Aviv) and L. Gemignani (U. Pisa), we design in [54] a fast implicit real QZ algorithm for eigenvalue computation of structured companion pencils arising from linearizations of polynomial

rootfind-ing problems. The modified QZ algorithm computes the generalized eigenvalues of an $N \times N$ structured matrix pencil using $O(N^2)$ flops and $O(N)$ memory storage. Numerical experiments and comparisons confirm the effectiveness and the stability of the proposed method.

6.3.17. Efficient Solution of Parameter Dependent Quasiseparable Systems and Computation of Meromorphic Matrix Functions

In [55], with Y. Eidelman (U. Tel Aviv) and L. Gemignani (U. Pisa), we focus on the solution of shifted quasiseparable systems and of more general parameter dependent matrix equations with quasiseparable representations. We propose an efficient algorithm exploiting the invariance of the quasiseparable structure under diagonal shifting and inversion. This algorithm is applied to compute various functions of matrices. Numerical experiments show the effectiveness of the approach.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

Bosch (Germany) ordered us some support for implementing complex numerical algorithms.

7.2. Bilateral Grants with Industry

- Marie Paindavoine is supported by an Orange Labs PhD Grant (from October 2013 to November 2016). She works on privacy-preserving encryption mechanisms.
- Miruna Rosca and Radu Titiu are employees of BitDefender. Their research internships (from October to December 2016) are supervised by Damien Stehlé and Benoît Libert, respectively. Miruna Rosca works on the foundations of lattice-based cryptography, and Radu Titiu works on functional encryption.
- Within the program Nano 2017, we collaborate with the Compilation Expertise Center of STMicroelectronics on the theme of floating-point arithmetic for embedded processors.

8. Partnerships and Cooperations

8.1. Regional Initiatives

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

PALSE PROJECT. Benoît Libert was awarded a 500keur grant (from July 2014 to November 2016) for his PALSE (Programme d'Avenir Lyon Saint-Etienne) project *Towards practical enhanced asymmetric encryption schemes*.

8.2. National Initiatives

8.2.1. ANR HPAC Project

Participants: Claude-Pierre Jeannerod, Nicolas Louvet, Clément Pernet, Nathalie Revol, Gilles Villard.

"High-performance Algebraic Computing" (HPAC) was a four year ANR project that started in January 2012 and was extended till mid-2016. The final report has been sent in July 2016. The Web page of the project is http://hpac.gforge.inria.fr/. HPAC has been headed by Jean-Guillaume Dumas (CASYS team, LJK laboratory, Grenoble); it was involving AriC as well as the Inria project-team MOAIS (LIG, Grenoble), the Inria project-team PolSys (LIP6 lab., Paris), the ARITH group (LIRMM laboratory, Montpellier), and the HPC Project company.

The overall ambition of HPAC was to provide international reference high-performance libraries for exact linear algebra and algebraic systems on multi-processor architecture and to influence parallel programming approaches for algebraic computing. The central goal has been to extend the efficiency of the LinBox and FGb libraries to new trend parallel architectures such as clusters of multi-processor systems and graphics processing units in order to tackle a broader class of problems in lattice-based cryptography and algebraic cryptanalysis. HPAC has conducted researches along three axes:

- A domain specific parallel language (DSL) adapted to high-performance algebraic computations;
- Parallel linear algebra kernels and higher-level mathematical algorithms and library modules;
- Library composition, their integration into state-of-the-art software, and innovative high-performance solutions for cryptology challenges.

8.2.2. 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.

8.2.3. ANR FastRelax Project

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

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.

8.2.4. ANR MetaLibm Project

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

MetaLibm is a four-year project (started in October 2013) 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.

8.2.5. ANR ALAMBIC Project

Participants: Benoît Libert, Fabien Laguillaumie.

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.

8.3. European Initiatives

8.3.1. FP7 & H2020 Projects

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.

OPENDREAMKIT is a H2020 Infrastructure project providing substantial funding to the open source computational mathematics ecosystem. It will run for four years, starting from September 2015. Clément Pernet is a participant.

8.4. International Research Visitors

8.4.1. Visiting Scientists

- George Labahn, Professor at U. Waterloo, Ontario, Canada spent the month of April with our team.
- Elena Kirshanova, PhD student at Ruhr-U. Bochum, Germany spent one month with our team, from mid-February to mid-March.
- Jiantao Li, PhD student at East China Normal U., China spends a year with our team. He arrived in September.

8.4.2. Internships

Willy Quach

Date: February 2016–June 2016

Institution: ENS de Lyon

Supervisor: Damien Stehlé

Balthazar Bauer

Date: March 2016–August 2016

Institution: Paris 7

Supervisor: Benoît Libert

Qian Chen

Date: March 2016–August 2016

Institution: ENS Rennes

Supervisors: Fabien Laguillaumie and Benoît Libert

Thi Xuan Vu

Date: May 2016–July 2016

Institution: ENS de Lyon

Supervisors: Claude-Pierre Jeannerod and Vincent Neiger

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

Nathalie Revol, with Javier Hormigo and Stuart Oberman, were general chairs of the Arith 23 conference, Santa Clara, California, USA.

9.1.1.2. Member of the Organizing Committees

Nathalie Revol was the organizer of the SWIM 2016: Summer Workshop on Interval Methods, gathering above 35 participants in Lyon, June 2016.

Bruno Salvy was a co-organizer of the meeting Alea'16 gathering about 80 participants in Luminy, March 2016.

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

Jean-Michel Muller belongs to the 3-member board of the steering committee of the Arith series of conferences.

9.1.2.2. Member of the Conference Program Committees

Nathalie Revol was a member of the program committees of REC'16 and SCAN 2016.

Bruno Salvy was a member of the program committee of AofA'16, Krakow, Poland.

Damien Stehlé was member of the program committees of Asiacrypt'16, Eurocrypt'17, SCN'16, ANTS'16, PKC'16 and PQCrypto'16.

Benoît Libert was member of the program committees of PKC'16, Africacrypt'16, ACM-CCS 2016, Eurocrypt'17.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

Jean-Michel Muller is a member of the editorial board of the *IEEE Transactions on Computers.* He is a member of the board of foundation editors of the *Journal for Universal Computer Science*.

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

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).

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

9.1.4. Invited Talks

Damien Stehlé gave an invited talk at the YACC conference (Porquerolles, June), on the Learning With Errors Problem. He gave an invited talk at the HEAT workshop (Paris, July) on lattice reduction.

Jean-Michel Muller gave an invited talk at a minisymposium on reproducible research at the CANUM conference (Obernai, May).

Claude-Pierre Jeannerod and Clément Pernet gave invited talks at RAIM (Rencontres Arithmétique de l'Informatique Mathématique; Banyuls-sur-mer, June).

Nathalie Revol gave an invited talk at a minisymposium on numerical reproducibility for high-performance computing at SIAM Parallel Processing (Paris, April).

9.1.5. Leadership within the Scientific Community

Damien Stehlé is a member of the steering committee of the PQCrypto conference series. He is also a member of the steering committee of the Cryptography and Coding French research grouping (C2).

Paola Boito and Claude-Pierre Jeannerod are 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: the work now addresses the set-based model and its implementation using simple IEEE-754 formats (IEEE P1788.1).

9.1.6. Scientific Expertise

Jean-Michel Muller is a member of the Scientific Council of CERFACS (Toulouse). He was a member of the Scientific Council of the "La Recherche" prize for 2015.

Jean-Michel Muller is a member of the steering committee of the "Defi 7" (information sciences) of the French Agence Nationale de la Recherche (ANR).

Bruno Salvy was a member of the recruitment committees for University Professors in Bordeaux (computer science) and in Toulouse (Mathematics).

Damien Stehlé is a member of the 2016 Gilles Kahn PhD award committees for 2016.

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

9.1.7. Research Administration

Guillaume Hanrot is director of the LIP laboratory (Laboratoire de l'Informatique du Parallélisme).

Jean-Michel Muller is co-director of the Groupement de Recherche (GDR) *Informatique Mathématique* of CNRS.

9.2. Teaching - Supervision - Juries

9.2.1. 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.

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

Master: Benoît Libert, Computer science and privacy, 12h, ENS de Lyon; Cryptography, 12h, ENS de Lyon.

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.

9.2.2. Supervision

- PhD: Serge Torres, *Tools for the design of reliable and efficient function evaluation libraries*, École normale supérieure de Lyon; defended on September 22, 2016; co-supervised by Nicolas Brisebarre and Jean-Michel Muller.

- PhD: Vincent Neiger, *Bases of relations in one or several variables: fast algorithms and applications*, École normale supérieure de Lyon; defended on November 30, 2016; co-supervised by Claude-Pierre Jeannerod and Gilles Villard (together with Éric Schost (U. Waterloo, Canada)).
- PhD: Silviu-Ioan Filip, *Robust tools for weighted Chebyshev approximation and applications to digital filter design*, École normale supérieure de Lyon; defended on December 7, 2016; co-supervised by Nicolas Brisebarre and Guillaume Hanrot.
- PhD in progress: Marie Paindavoine, *Méthodes de calculs sur des données chiffrées*, since October 2013 (Orange Labs - UCBL), co-supervised by Fabien Laguillaumie (together with Sébastien Canard).
- PhD in progress : Antoine Plet, *Contribution à l'analyse d'algorithmes en arithmétique virgule flottante*, since September 2014, co-supervised by Nicolas Louvet and Jean-Michel Muller.
- PhD in progress : Valentina Popescu, *Vers des bibliothèques multi-précision certifiées et performantes*, since September 2014, co-supervised by Mioara Joldes (LAAS) and Jean-Michel Muller
- PhD in progress: Louis Dumont, *Algorithmique efficace pour les diagonales, applications en combinatoire, physique et théorie des nombres*, since September 2013, co-supervised by Alin Bostan (SpecFun team) and Bruno Salvy.
- PhD in progress: Stephen Melczer, *Effective analytic combinatorics in one and several variables*, since September 2014, co-supervised by George Labahn (U. Waterloo, Canada) and Bruno Salvy.
- 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: 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: 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).

9.2.3. Juries

Paola Boito was an external reviewer for the PhD thesis of Bahar Arslan (University of Manchester, UK). She was also in the PhD committee of Louis Dumont (LIX, École polytechnique).

Claude-Pierre Jeannerod was in the PhD committee of Alexandre Temperville (CRIStAL, U. Lille 1).

Fabien Laguillaumie was a reviewer for the Habilitation thesis of Abderrahmane Nitaj (LMNO, U. Caen) and for the PhD thesis of Mario Cornejo-Ramirez (LIENS, UPSL).

Jean-Michel Muller was a reviewer for the PhD thesis of Arjun Suresh (U. Rennes). He was in the Habilitation committee of Claude Michel (U. Nice Sophia Antipolis).

Nathalie Revol was in the PhD committee of Rafife Nheili (U. Perpignan Via Domitia).

Bruno Salvy was a reviewer for the PhD thesis of Thibaut Verron (LIP6, UPMC) and for the HdR of Loïck Lhôte (Greyc, U. Caen). He was also in the PhD committees of Wenjie Fang (LIAFA, U. Paris-Diderot) and Louis Dumont (LIX, École polytechnique).

Damien Stehlé was a reviewer for the PhD thesis of Hansol Ryu (SNU, South Korea). He was in the PhD committee of Thijs Laarhoven (TU Eindhoven, The Netherlands) and in the Habilitation committee of Hoeteck Wee (DI, CNRS).

9.3. Popularization

Claude-Pierre Jeannerod gave an invited talk at *Journés Nationales de l'APMEP* (Lyon, October 2016), on the theme of algorithms for computer arithmetic.

Paolo Montuschi (Politecnico di Torino) and Jean-Michel Muller wrote a short paper on Computer Arithmetic for Computer Magazine [51].

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* exhibition. She presented some magic tricks during *Forum des Associations de Lyon 7e* and during the Science Fair, and she helped a class of high-school pupils (2nd) of Lycée Juliette Récamier (Lyon) to prepare a show for other pupils. She belonged to the selection committee for the MathInfoLy summer school for high-school pupils (around 90 french-speaking pupils). As an incentive for high-school pupils, and especially girls, to choose scientific careers, she gave talks at Lycée Lucie Aubrac (Ceyzériat), Lycée Xavier Bichat (Nantua) and Mondial des Métiers (in January and February 2016). She presented computer science for primary school pupils (CM2, École Guilloux, St-Genis-Laval: 12 lectures and hands-on of 1h30 in 2015-2016, for each of the 2 classes). She presented this work during the *Journées Passeurs de Science Informatique* of SIF in June 2016 and during the workshop *Robots pour l'éducation*. She also presented this work at a TEDxINSA talk and for IESF (Ingénieurs et Scientifiques de France). She took part in a training session for teachers, sponsored by Google, in September 2016. She co-organized two days on "Info Sans Ordinateur" gathering researchers interested in unplugged activities. With Jérôme Germoni and Natacha Portier, she co-organized a day *Filles & Maths* in May 2016 and a day *Filles & Info* in November 2016, each gathering about 100 high-school girls of 1e S. She is one of the editors of Interstices: https://interstices.info. She taught how to disseminate (computer) science for PhD students in a 20h module of *Insertion Professionnelle*.

Damien Stehlé will give a talk at the CNRS 'Colloque Sociétal Sécurité Informatique' (December 2016), on Fully Homomorphic Encryption.

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] S. TORRES. *Tools for the Design of Reliable and Efficient Functions Evaluation Libraries*, Université de Lyon, September 2016, https://tel.archives-ouvertes.fr/tel-01396907

Articles in International Peer-Reviewed Journals

[2] S. BAI, C. BOUVIER, A. KRUPPA, P. ZIMMERMANN. *Better polynomials for GNFS*, in "Mathematics of Computation / Mathematics of Computation", 2016, vol. 85, 12 p. [*DOI :* 10.1090/MCOM3048], https://hal.inria.fr/hal-01089507

[3] S. BAI, C. TONG, J. WEN. *Effects of Some Lattice Reductions on the Success Probability of the Zero-Forcing Decoder*, in "IEEE Communications Letters", 2016 [*DOI :* 10.1109/LCOMM.2016.2594196], https://hal.inria.fr/hal-01394219

[4] F. BENHAMOUDA, J. HERRANZ, M. JOYE, B. LIBERT. *Efficient Cryptosystems From 2^k -th Power Residue Symbols*, in "Journal of Cryptology", April 2016 [*DOI :* 10.1007/S00145-016-9229-5], https://hal.inria.fr/hal-01394400

[5] A. BOSTAN, M. BOUSQUET-MÉLOU, M. KAUERS, S. MELCZER. *On 3-dimensional lattice walks confined to the positive octant*, in "Annals of Combinatorics", October 2016, 36 p. , First Online: 14 October 2016 [*DOI :* 10.1007/s00026-016-0328-7], https://hal.archives-ouvertes.fr/hal-01063886

[6] A. BOSTAN, L. DUMONT, B. SALVY. *Algebraic Diagonals and Walks: Algorithms, Bounds, Complexity*, in "Journal of Symbolic Computation", 2016 [*DOI :* 10.1016/J.JSC.2016.11.006], https://hal.archives-ouvertes.fr/hal-01244914

[7] A. BOSTAN, P. LAIREZ, B. SALVY. *Multiple binomial sums*, in "Journal of Symbolic Computation", 2016 [*DOI :* 10.1016/J.JSC.2016.04.002], https://hal.archives-ouvertes.fr/hal-01220573

[8] N. BRISEBARRE, C. LAUTER, M. MEZZAROBBA, J.-M. MULLER. *Comparison between binary and decimal floating-point numbers*, in "IEEE Transactions on Computers", 2016, vol. 65, n° 7, pp. 2032–2044 [*DOI :* 10.1109/TC.2015.2479602], https://hal.archives-ouvertes.fr/hal-01021928

[9] S. BURRILL, J. COURTIEL, E. FUSY, S. MELCZER, M. MISHNA. *Tableau sequences, open diagrams, and Baxter families*, in "European Journal of Combinatorics", November 2016, vol. 58, pp. 144 - 165 [*DOI :* 10.1016/J.EJC.2016.05.011], https://hal.inria.fr/hal-01394155

[10] J.-G. DUMAS, T. GAUTIER, C. PERNET, J.-L. ROCH, Z. SULTAN. *Recursion based parallelization of exact dense linear algebra routines for Gaussian elimination*, in "Parallel Computing", September 2016, vol. 57, pp. 235–249 [*DOI :* 10.1016/J.PARCO.2015.10.003], https://hal.archives-ouvertes.fr/hal-01084238

[11] 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 2016, to appear [*DOI :* 10.1016/J.JSC.2016.11.011], https://hal.archives-ouvertes.fr/hal-01251223

[12] C.-P. JEANNEROD. *A radix-independent error analysis of the Cornea-Harrison-Tang method*, in "ACM Transactions on Mathematical Software", 2016 [*DOI :* 10.1145/2824252], https://hal.inria.fr/hal-01050021

[13] 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

[14] C.-P. JEANNEROD, N. LOUVET, J.-M. MULLER, A. PLET. *Sharp error bounds for complex floating-point inversion*, in "Numerical Algorithms", November 2016, vol. 73, n° 3, pp. 735-760 [*DOI :* 10.1007/S11075-016-0115-X], https://hal-ens-lyon.archives-ouvertes.fr/ensl-01195625

[15] C.-P. JEANNEROD, S. M. RUMP. *On relative errors of floating-point operations: optimal bounds and applications*, in "Mathematics of Computation", 2016 [*DOI :* 10.1090/MCOM/3234], https://hal.inria.fr/hal-00934443

[16] M. JOLDES, O. MARTY, J.-M. MULLER, V. POPESCU. *Arithmetic algorithms for extended precision using floating-point expansions*, in "IEEE Transactions on Computers", April 2016, vol. 65, n° 4, pp. 1197 - 1210, Rapport LAAS n° 15016 [*DOI :* 10.1109/TC.2015.2441714], https://hal.archives-ouvertes.fr/hal-01111551

[17] B. LIBERT, M. JOYE, M. YUNG. *Born and raised distributively: Fully distributed non-interactive adaptively-secure threshold signatures with short shares*, in "Theoretical Computer Science", September 2016, vol. 645, pp. 1-24 [*DOI :* 10.1016/J.TCS.2016.02.031], https://hal.inria.fr/hal-01394405

[18] S. MELCZER, M. MISHNA. *Asymptotic Lattice Path Enumeration Using Diagonals*, in "Algorithmica", August 2016, vol. 75, n° 4, pp. 782 - 811 [*DOI :* 10.1007/s00453-015-0063-1], https://hal.inria.fr/hal-01394157

[19] S. M. RUMP, F. BÜNGER, C.-P. JEANNEROD. *Improved error bounds for floating-point products and Horner's scheme*, in "BIT Numerical Mathematics", March 2016, vol. 56, n° 1, pp. 293 - 307 [*DOI :* 10.1007/s10543-015-0555-z], https://hal.inria.fr/hal-01137652

[20] R. SERRA, D. ARZELIER, M. JOLDES, J.-B. LASSERRE, A. RONDEPIERRE, B. SALVY. *Fast and Accurate Computation of Orbital Collision Probability for Short-Term Encounters*, in "Journal of Guidance, Control, and Dynamics", May 2016, vol. 39, n° 5, pp. 1009-1021 [*DOI :* 10.2514/1.G001353], https://hal.archives-ouvertes.fr/hal-01132149

[21] 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", August 2016 [*DOI :* 10.1002/CPE.3953], https://hal.archives-ouvertes.fr/hal-01236919

International Conferences with Proceedings

[22] S. AGRAWAL, B. LIBERT, D. STEHLÉ. *Fully Secure Functional Encryption for Inner Products, from Standard Assumptions*, in "Crypto 2016", Santa Barbara, United States, Crypto 2016, Springer, August 2016, vol. 9816, pp. 333 - 362 [*DOI :* 10.1007/978-3-662-53015-3_12], https://hal.inria.fr/hal-01228559

[23] M. ALBRECHT, S. BAI, L. DUCAS. *A subfield lattice attack on overstretched NTRU assumptions: Cryptanalysis of some FHE and Graded Encoding Schemes*, in "CRYPTO 2016", Santa Barbara, United States, 2016 [*DOI :* 10.1007/978-3-662-53018-4_6], https://hal.inria.fr/hal-01394211

[24] S. BAI, T. LAARHOVEN, D. STEHLÉ. *Tuple lattice sieving,*, in "ANTS 2016", Kaiserslautern, Germany, 2016, https://hal.inria.fr/hal-01394212

[25] S. BAI, D. STEHLÉ, W. WEIQIANG. *Improved Reduction from the Bounded Distance Decoding Problem to the Unique Shortest Vector Problem in Lattices*, in "ICALP 2016", Roma, Italy, 2016 [*DOI :* 10.4230/LIPICS.ICALP.2016.76], https://hal.inria.fr/hal-01394213

[26] A. BOSTAN, L. DUMONT, B. SALVY. *Efficient Algorithms for Mixed Creative Telescoping*, in "ISSAC 2016", Waterloo, Canada, Proceedings ISSAC'16, pp. 127–134, ACM Press, 2016, July 2016, 8 p. [*DOI :* 10.1145/2930889.2930907], https://hal.inria.fr/hal-01317940

[27] S. CANARD, F. LAGUILLAUMIE, M. PAINDAVOINE. *Verifiable Message-Locked Encryption*, in "CANS 2016 - 15th International Conference Cryptology and Network Security", Milano, Italy, S. FORESTI, G. PERSIANO (editors), Proc. of CANS 2016, Springer, November 2016, vol. 10052, pp. 299 - 315 [*DOI :* 10.1007/978-3-319-48965-0_18], https://hal.inria.fr/hal-01404486

[28] J. CHEN, B. LIBERT, S. C. RAMANNA. *Non-Zero Inner Product Encryption with Short Ciphertexts and Private Keys*, in "10th Conference on Security and Cryptography for Networks (SCN 2016)", Amalfi, Italy, 10th Conference on Security and Cryptography for Networks (SCN 2016), August 2016, https://hal.inria.fr/hal-01309562

[29] C. CHEVALIER, F. LAGUILLAUMIE, D. VERGNAUD. *Privately Outsourcing Exponentiation to a Single Server: Cryptanalysis and Optimal Constructions*, in "Computer Security - ESORICS 2016", Heraklion, Greece, I. G. ASKOXYLAKIS, S. IOANNIDIS, S. K. KATSIKAS, C. A. MEADOWS (editors), Computer Security – ESORICS 2016, Springer, September 2016, vol. 9878, pp. 261-278 [*DOI :* 10.1007/978-3-319-45744-4_13], https://hal.inria.fr/hal-01375817

[30] S. COLLANGE, M. JOLDES, J.-M. MULLER, V. POPESCU. *Parallel floating-point expansions for extended-precision GPU computations*, in "The 27th Annual IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP)", London, United Kingdom, July 2016, https://hal.archives-ouvertes.fr/hal-01298206

[31] L. DUCAS, D. STEHLÉ. *Sanitization of FHE Ciphertexts*, in "EUROCRYPT", Wien, Austria, 2016, https://hal.inria.fr/hal-01394216

[32] J.-G. DUMAS, E. KALTOFEN, E. THOMÉ, G. VILLARD. *Linear Time Interactive Certificates for the Minimal Polynomial and the Determinant of a Sparse Matrix*, in "International Symposium on Symbolic and Algebraic Computation", Waterloo, Canada, X.-S. GAO (editor), ISSAC'2016, Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation, ACM, July 2016, https://hal.archives-ouvertes.fr/hal-01266041

[33] C.-P. JEANNEROD, V. NEIGER, E. SCHOST, G. VILLARD. *Fast computation of minimal interpolation bases in Popov form for arbitrary shifts*, in "41st International Symposium on Symbolic and Algebraic Computation", Waterloo, ON, Canada, Proceedings of the 41st International Symposium on Symbolic and Algebraic Computation, July 2016 [*DOI :* 10.1145/2930889.2930928], https://hal.inria.fr/hal-01265983

[34] M. JOLDES, J.-M. MULLER, V. POPESCU, W. TUCKER. *CAMPARY: Cuda Multiple Precision Arithmetic Library and Applications*, in "5th International Congress on Mathematical Software (ICMS)", Berlin, Germany, July 2016, https://hal.archives-ouvertes.fr/hal-01312858

[35] J. LE MAIRE, N. BRUNIE, F. DE DINECHIN, J.-M. MULLER. *Computing floating-point logarithms with fixed-point operations*, in "23rd IEEE Symposium on Computer Arithmetic", Santa Clara, United States, IEEE, July 2016, https://hal.archives-ouvertes.fr/hal-01227877

[36] V. LEFÈVRE. *Correctly Rounded Arbitrary-Precision Floating-Point Summation*, in "23rd IEEE Symposium on Computer Arithmetic (ARITH)", Santa Clara, CA, United States, IEEE, July 2016 [*DOI :* 10.1109/ARITH.2016.9], https://hal.inria.fr/hal-01242127

[37] B. LIBERT, S. LING, F. MOUHARTEM, K. NGUYEN, H. WANG. *Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions*, in "Asiacrypt 2016", Hanoi, Vietnam, Advances in Cryptology - Asiacrypt 2016, Springer, December 2016, vol. 10032, https://hal.inria.fr/hal-01267123

[38] B. LIBERT, S. LING, F. MOUHARTEM, K. NGUYEN, H. WANG. *Zero-Knowledge Arguments for Matrix-Vector Relations and Lattice-Based Group Encryption*, in "Asiacrypt 2016", Hanoi, Vietnam, Advances in Cryptology - Asiacrypt 2016, Springer, December 2016, vol. 10032, pp. 101 - 131 [*DOI :* 10.1007/978-3-662-53890-6_4], https://hal.inria.fr/hal-01394087

[39] B. LIBERT, S. LING, K. NGUYEN, H. WANG. *Zero-Knowledge Arguments for Lattice-Based Accumulators: Logarithmic-Size Ring Signatures and Group Signatures Without Trapdoors*, in "Eurocrypt 2016", Vienne,

Austria, Eurocrypt 2016, Springer, May 2016, vol. 9666 [*DOI :* 10.1007/978-3-662-49896-5_1], https://hal.inria.fr/hal-01314642

[40] B. LIBERT, F. MOUHARTEM, K. NGUYEN. *A Lattice-Based Group Signature Scheme with Message-Dependent Opening*, in "14th International Conference on Applied Cryptography and Network Security (ACNS 2016)", Guildford, United Kingdom, Applied Cryptography and Network Security (ACNS 2016), Springer, June 2016, https://hal.inria.fr/hal-01302790

[41] B. LIBERT, F. MOUHARTEM, T. PETERS, T. PETERS, M. YUNG. *Practical "Signatures with Efficient Protocols" from Simple Assumptions*, in "AsiaCCS 2016", Xi'an, China, ACM, ACM, May 2016 [*DOI :* 10.1145/2897845.2897898], https://hal.inria.fr/hal-01303696

[42] B. LIBERT, S. C. RAMANNA, M. YUNG. *Functional Commitment Schemes: From Polynomial Commitments to Pairing-Based Accumulators from Simple Assumptions*, in "43rd International Colloquium on Automata, Languages and Programming (ICALP 2016)", Rome, Italy, 43rd International Colloquium on Automata, Languages and Programming (ICALP 2016) – Track A (Algorithms, Complexity and Games), July 2016, https://hal.inria.fr/hal-01306152

[43] S. MELCZER, B. SALVY. *Symbolic-Numeric Tools for Analytic Combinatorics in Several Variables*, in "ISSAC 2016", Waterloo, Canada, ACM, 2016, 8 p. [*DOI :* 10.1145/2930889.2930913], https://hal.inria.fr/hal-01310691

[44] S. MELCZER, M. C. WILSON. *Asymptotics of lattice walks via analytic combinatorics in several variables*, in "Formal Power Series and Algebraic Combinatorics (FPSAC)", Vancouver, Canada, DMTCS Proceedings of FPSAC 2016, July 2016, pp. 863-874, https://hal.inria.fr/hal-01394166

[45] J.-M. MULLER, V. POPESCU, P. T. PETER TANG. *A new multiplication algorithm for extended precision using floating-point expansions*, in "ARITH23", Santa Clara, United States, July 2016, https://hal.archives-ouvertes.fr/hal-01298195

[46] V. NEIGER. *Fast computation of shifted Popov forms of polynomial matrices via systems of modular polynomial equations*, in "41st International Symposium on Symbolic and Algebraic Computation", Waterloo, ON, Canada, Proceedings of the 41st International Symposium on Symbolic and Algebraic Computation, July 2016 [*DOI :* 10.1145/2930889.2930936], https://hal.inria.fr/hal-01266014

[47] C. PERNET. *Computing with quasiseparable matrices*, in "International Symposium on Symbolic and Algebraic Computation (ISSAC'16)", Waterloo, Canada, July 2016, pp. 389-396 [*DOI :* 10.1145/2930889.2930915], https://hal.archives-ouvertes.fr/hal-01264131

[48] S. C. RAMANNA. *More Efficient Constructions for Inner-Product Encryption*, in "Applied Cryptography and Network Security (ACNS 2016)", Guildford, United Kingdom, Applied Cryptography and Network Security (ACNS 2016), Springer, June 2016, vol. 9696, pp. 231 - 248 [*DOI :* 10.1007/978-3-319-39555-5_13], https://hal.inria.fr/hal-01394288

[49] D. STEHLÉ, A. NEUMAIER. *Faster LLL-type reduction of lattice bases*, in "ISSAC", Waterloo, Canada, 2016, https://hal.inria.fr/hal-01394214

Scientific Books (or Scientific Book chapters)

[50] J.-M. MULLER. *Elementary functions, algorithms and implementation, 3rd Edition*, Birkhaüser Boston, 2016 [*DOI :* 10.1007/978-1-4899-7983-4], https://hal-ens-lyon.archives-ouvertes.fr/ensl-01398294

Scientific Popularization

[51] P. MONTUSCHI, J.-M. MULLER. *Modern Computer Arithmetic*, in "Computer", September 2016, vol. 49, n^{o} 9, 12 p. , https://hal.archives-ouvertes.fr/hal-01394408

Other Publications

[52] B. ALLOMBERT, N. BRISEBARRE, A. LASJAUNIAS. *From a quartic continued fraction in $\mathbb{F}_3((T^{-1}))$ to a transcendental continued fraction in $Q((T^{-1}))$ through an infinite word over 1,2*, July 2016, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01348576

[53] S. BAI, P. GAUDRY, A. KRUPPA, E. THOMÉ, P. ZIMMERMANN. *Factorisation of RSA-220 with CADO-NFS*, May 2016, working paper or preprint, https://hal.inria.fr/hal-01315738

[54] P. BOITO, Y. EIDELMAN, L. GEMIGNANI. *A Real QZ Algorithm for Structured Companion Pencils*, 2016, working paper or preprint, https://hal.inria.fr/hal-01407864

[55] P. BOITO, Y. EIDELMAN, L. GEMIGNANI. *Efficient Solution of Parameter Dependent Quasiseparable Systems and Computation of Meromorphic Matrix Functions*, 2016, working paper or preprint, https://hal.inria.fr/hal-01407857

[56] S. BOLDO, S. GRAILLAT, J.-M. MULLER. *On the robustness of the 2Sum and Fast2Sum algorithms*, May 2016, working paper or preprint, https://hal-ens-lyon.archives-ouvertes.fr/ensl-01310023

[57] N. BRISEBARRE, F. DE DINECHIN, S.-I. FILIP, M. ISTOAN. *Automatic generation of hardware FIR filters from a frequency domain specification*, April 2016, working paper or preprint, https://hal.inria.fr/hal-01308377

[58] N. BRISEBARRE, S.-I. FILIP, G. HANROT. *A Lattice Basis Reduction Approach for the Design of Quantized FIR Filters*, April 2016, submitted for publication, https://hal.inria.fr/hal-01308801

[59] N. BRISEBARRE, G. HANROT, O. ROBERT. *Exponential sums and correctly-rounded functions*, November 2016, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01396027

[60] J. COURTIEL, S. MELCZER, M. MISHNA, K. RASCHEL. *Weighted Lattice Walks and Universality Classes*, September 2016, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01368786

[61] C.-P. JEANNEROD, N. LOUVET, J.-M. MULLER, A. PLET. *A Library for Symbolic Floating-Point Arithmetic*, August 2016, working paper or preprint, https://hal.inria.fr/hal-01232159

[62] C.-P. JEANNEROD, V. NEIGER, E. SCHOST, G. VILLARD. *Computing minimal interpolation bases*, June 2016, working paper or preprint, https://hal.inria.fr/hal-01241781

[63] M. JOLDES, V. POPESCU, J.-M. MULLER. *Tight and rigourous error bounds for basic building blocks of double-word arithmetic*, July 2016, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01351529

[64] G. LABAHN, V. NEIGER, W. ZHOU. *Fast, deterministic computation of the Hermite normal form and determinant of a polynomial matrix*, July 2016, working paper or preprint, https://hal.inria.fr/hal-01345627

[65] V. LEFÈVRE. *Correctly Rounded Arbitrary-Precision Floating-Point Summation*, November 2016, working paper or preprint, https://hal.inria.fr/hal-01394289

[66] J. WEN, X.-W. CHANG. *A Linearithmic Time Algorithm for a Shortest Vector Problem in Compute-and-Forward Design*, January 2016, working paper or preprint, https://hal.inria.fr/hal-01403929

[67] J. WEN, X.-W. CHANG. *GfcLLL: A Greedy Selection Based Approach for Fixed-Complexity LLL Reduction*, July 2016, working paper or preprint, https://hal.inria.fr/hal-01403926