IN PARTNERSHIP WITH:
CNRS

Ecole normale supérieure de Lyon

Université Claude Bernard (Lyon 1)

Activity Report 2015

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. - 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

Jean-Michel Muller [Team leader, CNRS, Senior Researcher, HdR]
Nicolas Brisebarre [CNRS, Researcher]
Claude-Pierre Jeannerod [Inria, Researcher]
Vincent Lefèvre [Inria, Researcher]
Nathalie Revol [Inria, Researcher]
Bruno Salvy [Inria, Senior Researcher]
Gilles Villard [CNRS, Senior Researcher, HdR]

Faculty Members

Guillaume Hanrot [ENS Lyon, Professor, HdR]
Fabien Laguillaumie [Univ. Lyon I, Professor, HdR]
Nicolas Louvet [Univ. Lyon I, Associate Professor]
Clément Pernet [Univ. Grenoble I, Associate Professor, HdR]
Damien Stehlé [ENS Lyon, Professor, HdR]
Serge Torres [ENS Lyon]

Engineer

Laurent Thevenoux [Inria]

PhD Students

Silviu Filip [ENS Lyon]
Sébastien Maulat [ENS Lyon, until Aug 2015]
Stephen Melczer [NSERC, codirection with Waterloo, Ontario, Canada]
Vincent Neiger [ENS Lyon, codirection with Waterloo, Ontario, Canada]
Marie Paindavoine [ENS Lyon and Orange Labs, CIFRE]
Antoine Plet [ENS Lyon]
Valentina Popescu [ENS Lyon]
Weiqiang Wen [ENS Lyon, from Feb 2015]
Fabrice Mouhartem [ENS Lyon, from Feb 2015]

Post-Doctoral Fellows

Shi Bai [ENS Lyon]
Sanjay Bhattacherjee [ENS Lyon, from Feb 2015]
Benoît Libert [ENS Lyon, HdR]

Somindu Ramanna [ENS Lyon, from Feb 2015]
Jinming Wen [CNRS, from Mar 2015]

Visiting Scientists

Jung Hee Cheon [SNU Korea, from Jul 2015 until Aug 2015]
Arnold Neumaier [U. of Vienna, from Sep 2015 to Dec 2015]
Khoa Ta Toan Nguyen [NTU Singapore, Oct 2015]
Yongseo Song [SNU Korea, from Jul 2015 until Aug 2015]
Thomas Prest [ENS Paris, from Jun 2015 until Aug 2015]

Administrative Assistant

Chiraz Benamor [ENS Lyon]

Others

Andrada Popa [Inria, Intern, from Jul 2015 until Sep 2015]
Alice Pellet-Mary [ENS Lyon, Intern, from Jul 2015 until Sep 2015]
Pablo Rotondo Suarez [Inria, Intern, from Mar 2015 until Jun 2015]

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/continuation with 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 will end in December 2015) we will pursue the design and implementation of high performance linear algebra primitives and algorithms.

4. Application Domains

4.1. Floating-point and Validated Numerics

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

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

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

- reproducibility of floating-point computations.

4.2. Cryptography, Cryptology, Communication Theory

Lattice reduction algorithms have direct applications in

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

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. ARITH conference in Lyon

Since 1969, ARITH is the primary and reference international conference for presenting scientific work on the latest research in computer arithmetic. In June 2015, we organized it in Lyon.

5.1.2. Best student paper

At ISSAC'2015 [20].

5.1.3. Best papers

Best papers at Eurocrypt'2015 , Asiacrypt'2015 and ISSAC'2015 .

BEST PAPERS AWARDS:

[14]
J. H. Cheon, K. Han, C. Lee, H. Ryu, D. Stehlé. *Cryptanalysis of the Multilinear Map over the Integers*, in "EUROCRYPT", Sofia, Bulgaria, 2015, https://hal.archives-ouvertes.fr/hal-01240445

[11]
S. Bai, A. Langlois, T. Lepoint, D. Stehlé, R. Steinfeld. *Improved security proofs in lattice-based cryptography: using the Rényi divergence rather than the statistical distance*, in "ASIACRYPT", Auckland, New Zealand, 2015, https://hal.archives-ouvertes.fr/hal-01240434

[16]
J.-G. Dumas, C. Pernet, Z. Sultan. *Computing the Rank Profile Matrix*, in "ISSAC", Bath, United Kingdom, K. Yokoyama (editor), ISSAC 2015, ACM, July 2015, pp. 146–153 [*DOI :* 10.1145/2755996.2756682], https://hal.archives-ouvertes.fr/hal-01107722

6. New Software and Platforms

6.1. FPLLL: a lattice reduction library

fplll contains several algorithms on lattices that rely on floating-point computations. This includes implementations of the floating-point LLL reduction algorithm, offering different speed/guarantees ratios. It contains a “wrapper” choosing the estimated best sequence of variants in order to provide a guaranteed output as fast as possible. In the case of the wrapper, the succession of variants is oblivious to the user. It also includes a rigorous floating-point implementation of the Kannan-Fincke-Pohst algorithm that finds a shortest non-zero lattice vector, and the BKZ reduction algorithm.

The fplll library is distributed under the LGPL license. It has been used in or ported to several mathematical computation systems such as Magma, Sage, and PariGP. It is also used for cryptanalytic purposes, to test the resistance of cryptographic primitives.

- Participants: Shi Bai, Damien Stehlé
- Contact: Damien Stehlé
- URL: https://github.com/dstehle/fplll

6.2. GNU MPFR: a library for arbitrary precision floating-point arithmetic

Keywords: Multiple-Precision - Floating-point - Correct Rounding
GNU MPFR is an efficient multiple-precision floating-point library written in C 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. It is distributed under the LGPL license.

The development of MPFR started in Loria (Nancy). When Vincent Lefèvre moved from Nancy to Lyon, it became a joint project between the project-team Caramel (Nancy) and AriC. Many systems use MPFR, several of them being listed on its web page. MPFR 3.1.3 was released on 19 June 2015.

New developments in the trunk: Full rewrite of `mpfr_sum` completed, with new tests [38]. Generic tests improved. Bug fixes and various improvements, in particular concerning the flags.

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

6.3. Gfun: a Maple package for solutions of linear differential or recurrence equations

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

Its development moved to AriC with Bruno Salvy in 2012, while a submodule NumGfun dedicated to symbolic-numeric computations with linear ODEs has been developed by Marc Mezzarobba during his post-doc at AriC. An old version of gfun is distributed with the Maple library. Newer versions are available on the web page of gfun, which also lists a number of articles by scientists who cited it.

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

6.4. Sipe: a library for very low precision computations with correct rounding

KEYWORDS: Floating-point - Correct Rounding

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. It is distributed under the LGPL license and mostly used internally.

- Participant: Vincent Lefèvre
- Contact: Vincent Lefèvre
- URL: https://www.vinc17.net/research/sipe/

6.5. 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.

- Participant:
- Contact: Clément Pernet
- URL: http://www.linalg.org

6.6. Exhaustive Tests for the Correct Rounding of Mathematical Functions

Participant: Vincent Lefèvre.

The search for the worst cases for the correct rounding (hardest-to-round cases) of mathematical functions ($\exp$, $\log$, $\sin$, $\cos$, etc.) in a fixed precision (mainly double precision) using Lefèvre's algorithm is implemented by a set of utilities written in Perl, with calls to Maple/intpakX for computations on intervals and with C code generation for fast computations. It also includes a client-server system for the distribution of intervals to be tested and for tracking the status of intervals (fully tested, being tested, aborted).

The support for the $\tanh$ function has been added, and this function has been tested on the full domain (together with its inverse function). Results are available from: https://www.vinc17.net/research/testlibm/

- Participant: Vincent Lefèvre
- Contact: Vincent Lefèvre

6.7. Multiplication by Integer Constants

Participant: Vincent Lefèvre.

A Perl implementation of algorithms for the multiplication by integer constants has been updated to get more results based on exhaustive tests: threading has been implemented in this part of the script.

- Participant: Vincent Lefèvre
- Contact: Vincent Lefèvre
- URL: https://www.vinc17.net/research/mulbyconst/#patterns

7. New Results

7.1. Floating-point Arithmetic

7.1.1. On the maximum relative error when computing integer powers by iterated multiplications in floating-point arithmetic

We improve the usual relative error bound for the computation of x^n through iterated multiplications by x in binary floating-point arithmetic. The obtained error bound is only slightly better than the usual one, but it is simpler. We also discuss the more general problem of computing the product of n terms. [5]

7.1.2. Formally verified certificate checkers for hardest-to-round computation

In order to derive efficient and robust floating-point implementations of a given function f, it is crucial to compute its hardest-to-round points, i.e. the floating-point numbers x such that $f(x)$ is closest to the midpoint of two consecutive floating-point numbers. Depending on the floating-point format one is aiming at, this can be highly computationally intensive. In this paper, we show how certificates based on Hensel's lemma can be added to an algorithm using lattice basis reduction so that the result of a computation can be formally checked in the Coq proof assistant. [7]

7.1.3. On the error of Computing $ab + cd$ using Cornea, Harrison and Tang's method

In their book, Scientific Computing on the Itanium, Cornea et al. (2002) introduce an accurate algorithm for evaluating expressions of the form $ab + cd$ in binary floating-point arithmetic, assuming an FMA instruction is available. They show that if p is the precision of the floating-point format and if $u = 2^{-p}$, the relative error of the result is of order u. We improve their proof to show that the relative error is bounded by $2u + 7u^2 + 6u^3$. Furthermore, by building an example for which the relative error is asymptotically (as $p \to \infty$ or, equivalently, as $u \to 0$) equivalent to $2u$, we show that our error bound is asymptotically optimal. [8]

7.1.4. Improved error bounds for floating-point products and Horner's scheme

Let u denote the relative rounding error of some floating-point format. Recently it has been shown that for a number of standard Wilkinson-type bounds the typical factors $\gamma_k := ku/(1-ku)$ can be improved into ku, and that the bounds are valid without restriction on k. Problems include summation, dot products and thus matrix multiplication, residual bounds for LU- and Cholesky-decomposition, and triangular system solving by substitution. In this note we show a similar result for the product $\prod_{i=0}^{k} x_i$ of real and/or floating-point numbers x_i, for computation in any order, and for any base $\beta \geq 2$. The derived error bounds are valid under a mandatory restriction of k. Moreover, we prove a similar bound for Horner's polynomial evaluation scheme. [9]

7.1.5. Comparison between binary and decimal floating-point numbers

In collaboration with Christoph Lauter and Marc Mezzarobba (LIP6 laboratory, Paris), Nicolas Brisebarre and Jean-Michel Muller 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. They provide an implementation of several variants of our algorithm, and compare them [26].

7.2. Lattices: algorithms and cryptology

7.2.1. Linearly Homomorphic Encryption from DDH

We design a linearly homomorphic encryption scheme whose security relies on the hardness of the decisional Diffie-Hellman problem. Our approach requires some special features of the underlying group. In particular, its order is unknown and it contains a subgroup in which the discrete logarithm problem is tractable. Therefore, our instantiation holds in the class group of a non maximal order of an imaginary quadratic field. Its algebraic structure makes it possible to obtain such a linearly homomorphic scheme whose message space is the whole set of integers modulo a prime p and which supports an unbounded number of additions modulo p from the ciphertexts. A notable difference with previous works is that, for the first time, the security does not depend on the hardness of the factorization of integers. As a consequence, under some conditions, the prime p can be scaled to fit the application needs. [13]

7.2.2. Secure Efficient History-Hiding Append-Only Signatures in the Standard Model

As formalized by Kiltz et al. (ICALP’05), append-only signatures (AOS) are digital signature schemes where anyone can publicly append extra message blocks to an already signed sequence of messages. This property is useful, e.g., in secure routing, in collecting response lists, reputation lists, or petitions. Bethencourt, Boneh and Waters (NDSS’07) suggested an interesting variant, called history-hiding append-only signatures (HH-AOS), which handles messages as sets rather than ordered tuples. This HH-AOS primitive is useful when the exact order of signing needs to be hidden. When free of subliminal channels (i.e., channels that can tag elements in an undetectable fashion), it also finds applications in the storage of ballots on an electronic voting terminals or in other archival applications (such as the record of petitions, where we want to hide the influence among messages). However, the only subliminal-free HH-AOS to date only provides heuristic arguments in terms of security: Only a proof in the idealized (non-realizable) random oracle model is given. This paper provides the first HH-AOS construction secure in the standard model. Like the system of Bethencourt et al., our HH-AOS features constant-size public keys, no matter how long messages to be signed are, which is atypical (we note that secure constructions often suffer from a space penalty when compared to their random-oracle-based counterpart). As a second result, we show that, even if we use it to sign ordered vectors as in an ordinary AOS (which is always possible with HH-AOS), our system provides considerable advantages over existing realizations. As a third result, we show that HH-AOS schemes provide improved identity-based ring signatures (i.e., in prime order groups and with a better efficiency than the state-of-the-art schemes). [17]

7.2.3. Compactly Hiding Linear Spans: Tightly Secure Constant-Size Simulation-Sound QA-NIZK Proofs and Applications

Quasi-adaptive non-interactive zero-knowledge (QA-NIZK) proofs is a powerful paradigm, suggested recently by Jutla and Roy (Asiacrypt’13), which is motivated by the Groth-Sahai seminal techniques for efficient non-interactive zero-knowledge (NIZK) proofs. In this paradigm, the common reference string may depend on specific language parameters, a fact that allows much shorter proofs in important cases. It even makes certain standard model applications competitive with the Fiat-Shamir heuristic in the Random Oracle idealization (such QA-NIZK proofs were recently optimized to constant size by Jutla and Roy (Crypto’14) and Libert et al. (Eurocrypt’14) for the important case of proving that a vector of group elements belongs to a linear subspace). While, e.g., the QA-NIZK arguments of Libert et al. provide unbounded simulation-soundness and constant proof length, their simulation-soundness is only loosely related to the underlying assumption (with a gap proportional to the number of adversarial queries) and it is unknown how to alleviate this limitation without sacrificing efficiency. Here, we deal with the basic question of whether and to what extent we can simultaneously optimize the proof size and the tightness of security reductions, allowing for important applications with tight security (which are typically to date quite lengthy) to be of shorter size. In this paper, we resolve this question by describing a novel simulation-sound QA-NIZK argument showing that a vector v ∈ G n belongs to a subspace of rank t < n using a constant number of group elements. Unlike previous constant-size QA-NIZK proofs of such statements, the unbounded simulation-soundness of our system is nearly tightly related (i.e., the reduction only loses a factor proportional to the security parameter) to the standard Decision Linear assumption. To show simulation-soundness in the constrained context of tight reductions, we employ a number of techniques, and explicitly point at a technique – which may be of independent interest – of hiding the linear span of a structure-preserving homomorphic signature (which is part of an OR proof). As an application, we design a public-key cryptosystem with almost tight CCA2-security in the multi-challenge, multiuser setting with improved length (asymptotically optimal for long messages). We also adapt our scheme to provide CCA security in the key-dependent message scenario (KDM-CCA2) with ciphertext length reduced by 75% when compared to the best known tightly secure KDM-CCA2 system so far. [18]

7.2.4. Short Group Signatures via Structure-Preserving Signatures: Standard Model Security from Simple Assumptions

Group signatures are a central cryptographic primitive which allows users to sign messages while hiding their identity within a crowd of group members. In the standard model (without the random oracle idealization), the most efficient constructions rely on the Groth-Sahai proof systems (Eurocrypt'08). The structure-preserving signatures of Abe et al. (Asiacrypt'12) make it possible to design group signatures based on well-established, constant-size number theoretic assumptions (a.k.a. "simple assumptions") like the Symmetric eXternal Diffie-Hellman or Decision Linear assumptions. While much more efficient than group signatures built on general assumptions, these constructions incur a significant overhead w.r.t. constructions secure in the idealized random oracle model. Indeed, the best known solution based on simple assumptions requires 2.8 kB per signature for currently recommended parameters. Reducing this size and presenting techniques for shorter signatures are thus natural questions. In this paper, our first contribution is to significantly reduce this overhead. Namely, we obtain the first fully anonymous group signatures based on simple assumptions with signatures shorter than 2 kB at the 128-bit security level. In dynamic (resp. static) groups, our signature length drops to 1.8 kB (resp. 1 kB). This improvement is enabled by two technical tools. As a result of independent interest, we first construct a new structure-preserving signature based on simple assumptions which shortens the best previous scheme by 25%. Our second tool is a new method for attaining anonymity in the strongest sense using a new CCA2-secure encryption scheme which is simultaneously a Groth-Sahai commitment. [19]

7.2.5. Implementing Candidate Graded Encoding Schemes from Ideal Lattices

Multilinear maps have become popular tools for designing cryptographic schemes since a first approximate realisation candidate was proposed by Garg, Gentry and Halevi (GGH). This construction was later improved by Langlois, Stehlé and Steinfeld who proposed GGHLite which offers smaller parameter sizes. In this work, we provide the first implementation of such approximate multilinear maps based on ideal lattices. Implementing GGH-like schemes naively would not allow instantiating it for non-trivial parameter sizes. We hence propose a strategy which reduces parameter sizes further and several technical improvements to allow for an efficient implementation. In particular, since finding a prime ideal when generating instances is an expensive operation, we show how we can drop this requirement. We also propose algorithms and implementations for sampling from discrete Gaussians, for inverting in some Cyclotomic number fields and for computing norms of ideals in some Cyclotomic number rings. Due to our improvements we were able to compute a multilinear jigsaw puzzle for $\kappa = 52$ (resp. $\kappa = 38$) and $\lambda = 52$ (resp. $\lambda = 80$). [10]

7.2.6. Improved security proofs in lattice-based cryptography: using the Rényi divergence rather than the statistical distance

The Rényi divergence is a mean to measure the closeness of two distributions. We show that it can often be used as an alternative to the statistical distance in security proofs for lattice-based cryptography. Using the Rényi divergence is particularly suited for security proofs of primitives in which the attacker is required to solve a search problem (e.g., forging a signature). We show that it may also be used in the case of distinguishing problems (e.g., semantic security of encryption schemes), when they enjoy a public sampleability property. The techniques lead to security proofs for schemes with smaller parameters. [11]

7.2.7. *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 effient realizations of the primitive for the computation of linear functions on encrypted data: given an encryption of a vector y over some specific base ring, a secret key SK_x for the vector x allows computing $< x, y >$. 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 this paper, 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. Our constructions 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, we obtain 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. We finally propose a solution based on Paillier's composite residuosity assumption that enables evaluation of inner products modulo an RSA integer $N = pq$. We demonstrate that the functionality of inner products over a prime field is very powerful and can be used to construct bounded collusion FE for all circuits. [23]

7.2.8. *Fully Homomophic Encryption over the Integers Revisited*

Two main computational problems serve as security foundations of current fully homomorphic encryption schemes: Regev's Learning With Errors problem (LWE) and Howgrave-Graham's Approximate Greatest Common Divisor problem (AGCD). Our first contribution is a reduction from LWE to AGCD. As a second contribution, we describe a new AGCD-based fully homomorphic encryption scheme, which outperforms all prior AGCD-based proposals: its security does not rely on the presumed hardness of the so-called Sparse Subset Sum problem, and the bit-length of a ciphertext is only $\widetilde{O}\lambda$, where λ refers to the security parameter. [15]

7.2.9. *Cryptanalysis of the Multilinear Map over the Integers*

We describe a polynomial-time cryptanalysis of the (approximate) multilinear map of Coron, Lepoint and Tibouchi (CLT). The attack relies on an adaptation of the so-called zeroizing attack against the Garg, Gentry and Halevi (GGH) candidate multilinear map. Zeroizing is much more devastating for CLT than for GGH. In the case of GGH, it allows to break generalizations of the Decision Linear and Subgroup Membership problems from pairing-based cryptography. For CLT, this leads to a total break: all quantities meant to be kept secret can be efficiently and publicly recovered. [14]

7.2.10. *Cryptanalysis of Gu's ideal multilinear map*

In March, 2015 Gu Chunsheng proposed a candidate ideal multilinear map [eprint 2015/269]. An ideal multilinear map allows to perform as many multiplications as desired, while in k-multilinear maps like GGH [EC 2013] or CLT [CR2013, CR2015] one we canperform at most a predetermined number k of multiplications. In this note, we show that the extraction Multilinear Computational Diffie-Hellman problem (ext-MCDH) associated to Gu's map can be solved in polynomial-time: this candidate ideal multilinear map is insecure. We also give intuition on why we think that the two other ideal multilinear maps proposed by Gu in [eprint 2015/269] are not secure either. [39]

7.2.11. Worst-case to average-case reductions for module lattices

Most lattice-based cryptographic schemes are built upon the assumed hardness of the Short Integer Solution (SIS) and Learning With Errors (LWE) problems. Their efficiencies can be drastically improved by switching the hardness assumptions to the more compact Ring-SIS and Ring-LWE problems. However, this change of hardness assumptions comes along with a possible security weakening: SIS and LWE are known to be at least as hard as standard (worst-case) problems on euclidean lattices, whereas Ring-SIS and Ring-LWE are only known to be as hard as their restrictions to special classes of ideal lattices, corresponding to ideals of some polynomial rings. In this work, we define the Module-SIS and Module-LWE problems, which bridge SIS with Ring-SIS, and LWE with Ring-LWE, respectively. We prove that these average-case problems are at least as hard as standard lattice problems restricted to module lattices (which themselves generalize arbitrary and ideal lattices). As these new problems enlarge the toolbox of the lattice-based cryptographer, they could prove useful for designing new schemes. Importantly, the worst-case to average-case reductions for the module problems are (qualitatively) sharp, in the sense that there exist converse reductions. This property is not known to hold in the context of Ring-SIS/Ring-LWE: Ideal lattice problems could reveal easy without impacting the hardness of Ring-SIS/Ring-LWE. [6]

7.2.12. Reducing Communication Overhead of the Subset Difference Scheme

In Broadcast Encryption (BE) systems like Pay-TV, AACS, online content sharing and broadcasting, reducing the header length (communication overhead per session) is of practical interest. The Subset Difference (SD) scheme due to Naor-Naor-Lotspiech (NNL) is the most popularly used BE scheme. This work introduced the (a,b,γ) augmented binary tree subset difference ((a,b,γ)-ABTSD) scheme which is a generalization of the NNL-SD scheme. By varying the parameters (a,b,γ), it is possible to obtain $O(n \log n)$ different schemes. In addition to the underlying binary tree structure of the NNL-SD scheme, the new scheme uses an additional binary tree structure of height a augmented with each internal node. The SD subsets in this scheme arise due to nodes that are at a distance at most b from each other. In the augmented tree of height a, at most c leaves are considered together in creating the SD subsets for the scheme. The average header length achieved by the new schemes is smaller than all known schemes having the same decryption time as that of the NNL-SD scheme and achieving non-trivial trade-offs between the user storage and the header size. The amount of key material that a user is required to store increases. For the earlier mentioned applications, reducing header size and achieving fast decryption is perhaps more of a concern than the user storage

7.3. Algebraic computing and high performance kernels

7.3.1. Complexity of the F5 Gröbner basis algorithm

We study the complexity of Gröbner bases computation, in particular in the generic situation where the variables are in simultaneous Noether position with respect to the system. We give a bound on the number of polynomials of degree d in a Gröbner basis computed by Faugère's F5 algorithm (2002) in this generic case for the grevlex ordering (which is also a bound on the number of polynomials for a reduced Gröbner basis, independently of the algorithm used). Next, we analyse more precisely the structure of the polynomials in the Gröbner bases with signatures that F5 computes and use it to bound the complexity of the algorithm. Our estimates show that the version of F5 we analyse, which uses only standard Gaussian elimination techniques, outperforms row reduction of the Macaulay matrix with the best known algorithms for moderate degrees, and even for degrees up to the thousands if Strassen's multiplication is used. The degree being fixed, the factor of improvement grows exponentially with the number of variables. [1]

7.3.2. Faster Algorithms for Multivariate Interpolation with Multiplicities and Simultaneous Polynomial Approximations

The interpolation step in the Guruswami-Sudan algorithm is a bivariate interpolation problem with multiplicities commonly solved in the literature using either structured linear algebra or basis reduction of polynomial lattices. This problem has been extended to three or more variables; for this generalization, all fast algorithms proposed so far rely on the lattice approach. In this work, we reduce this multivariate interpolation problem to a problem of simultaneous polynomial approximations, which we solve using fast structured linear algebra. This improves the best known complexity bounds for the interpolation step of the list-decoding of Reed-Solomon codes, Parvaresh-Vardy codes, and folded Reed-Solomon codes. In particular, for Reed-Solomon list-decoding with re-encoding, our approach has complexity $\widetilde{O}(\ell^{\omega-1}m^2(n-k))$, where ℓ, m, n, k are the list size, the multiplicity, the number of sample points and the dimension of the code, and ω is the exponent of linear algebra; this accelerates the previously fastest known algorithm by a factor of ℓ/m. [3]

7.3.3. Recursion based parallelization of exact dense linear algebra routines for Gaussian elimination

We present block algorithms and their implementation for the parallelization of sub-cubic Gaussian elimination on shared memory architectures. Contrarily to the classical cubic algorithms in parallel numerical linear algebra, we focus here on recursive algorithms and coarse grain parallelization. Indeed, sub-cubic matrix arithmetic can only be achieved through recursive algorithms making coarse grain block algorithms perform more efficiently than fine grain ones. This work is motivated by the design and implementation of dense linear algebra over a finite field, where fast matrix multiplication is used extensively and where costly modular reductions also advocate for coarse grain block decomposition. We incrementally build efficient kernels, for matrix multiplication first, then triangular system solving, on top of which a recursive PLUQ decomposition algorithm is built. We study the parallelization of these kernels using several algorithmic variants: either iterative or recursive and using different splitting strategies. Experiments show that recursive adaptive methods for matrix multiplication, hybrid recursive-iterative methods for triangular system solve and tile recursive versions of the PLUQ decomposition, together with various data mapping policies, provide the best performance on a 32 cores NUMA architecture. Overall, we show that the overhead of modular reductions is more than compensated by the fast linear algebra algorithms and that exact dense linear algebra matches the performance of full rank reference numerical software even in the presence of rank deficiencies. [4]

7.3.4. Computing the Rank Profile Matrix

The row (resp. column) rank profile of a matrix describes the staircase shape of its row (resp. column) echelon form. In an ISSAC'13 paper, we proposed a recursive Gaussian elimination that can compute simultaneously the row and column rank profiles of a matrix as well as those of all of its leading sub-matrices, in the same time as state of the art Gaussian elimination algorithms. Here we first study the conditions making a Gaus-sian elimination algorithm reveal this information. Therefore, we propose the definition of 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 also explore the conditions for a Gaussian elimination algorithm to compute all or part of this invariant, through the corresponding PLUQ decomposition. As a consequence, we show that the classical iterative CUP decomposition algorithm can actually be adapted to compute the rank profile matrix. Used, in a Crout variant, as a base-case to our ISSAC'13 implementation, it delivers a significant improvement in efficiency. Second, the row (resp. column) echelon form of a matrix are usually computed via different dedicated triangular decompositions. We show here that, from some PLUQ decompositions, it is possible to recover the row and column echelon forms of a matrix and of any of its leading sub-matrices thanks to an elementary post-processing algorithm. [16]

7.3.5. Formulas for Continued Fractions. An Automated Guess and Prove Approach

We describe a simple method that produces automatically closed forms for the coefficients of continued fractions expansions of a large number of special functions. The function is specified by a non-linear differential equation and initial conditions. This is used to generate the first few coefficients and from there a conjectured formula. This formula is then proved automatically thanks to a linear recurrence satisfied by some remainder terms. Extensive experiments show that this simple approach and its straightforward generalization to difference and q-difference equations capture a large part of the formulas in the literature on continued fractions. [20]

7.3.6. Algebraic Diagonals and Walks

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 $\mathrm{Diag}\, F$. Generically, it is its minimal polynomial and is obtained in time quasi-linear in its size. We show that this minimal polynomial has an exponential size with respect to 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. [12]

8. Bilateral Contracts and Grants with Industry

8.1. 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.
- Within the program Nano 2017, we collaborate with the Compilation Expertise Center of STMicroelectronics on the theme of floating-point arithmetic for embedded processors.

9. Partnerships and Cooperations

9.1. Regional Initiatives

- ARC6 PhD Programme. The PhD grant of Valentina Popescu is funded since Sep. 2014 by Région Rhône-Alpes through the “ARC6” programme.
- PALSE Project. Benoît Libert was awarded a 500keur (from July 2014 to November 2016) grant for his PALSE (Programme d’Avenir Lyon Saint-Etienne) project *Towards practical enhanced asymmetric encryption schemes*.

9.2. National Initiatives

9.2.1. ANR HPAC Project

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

“High-performance Algebraic Computing” (HPAC) is a four year ANR project that started in January 2012. The Web page of the project is http://hpac.gforge.inria.fr/. HPAC is headed by Jean-Guillaume Dumas (CASYS team, LJK laboratory, Grenoble); it involves 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 is 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 is 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 conducts 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.

9.2.2. 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 http://www.liafa.univ-paris-diderot.fr/dyna3s/. It is headed by Valérie Berthé (U. Paris 7) and involves also the University of Caen.

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

9.2.3. ANR FastRelax Project

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

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

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

9.2.4. 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.

9.3. European Initiatives

9.3.1. 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.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

9.4.1.1. Visiting Scientists

- Jung Hee Cheon from July to August;
- Arnold Neumaier from August to December;
- Khoa Ta Toa Nguyen until October;
- Peter Tang, from June to July;
- Yong Sue Song from July to August.

9.4.1.2. Internships

Fabrice Mouhartem

Date: February 2015–July 2015
Institution: ENS de Lyon
Supervisor: Benoît Libert

Alice Pellet-Mary

Date: February 2015–July 2015
Institution: ENS de Lyon
Supervisor: Damien Stehlé

Andrada Popa

Date: July 2015–September 2015
Institution: Technical University of Cluj-Napoca (Roumanie)
Supervisor: Nicolas Brisebarre

Pablo Rotondo

Date: March 2015–June 2015
Institution: Universidad de la Republica Uruguay (Uruguay)
Supervisor: Bruno Salvy

Weiqiang Wen

Date: February 2015–July 2015
Institution: SCNU, China
Supervisor: Damien Stehlé

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific events organisation

10.1.1.1. General chair, scientific chair

Jean-Michel Muller was the General Chair of ARITH'22, Lyon.

10.1.1.2. Member of the organizing committees

Bruno Salvy is a co-organizer with Alin Bostan of Alea'2016, Luminy.

10.1.2. Scientific events selection

10.1.2.1. Member of the conference program committees

Fabien Laguillaumie was a member of the program committee of WCC'15.

Benoît Libert was a member of the program committees of ACM-CCS'15, Eurocryp'15, PKC'15 and '16, Africacrypt'16.

Jean-Michel Muller was a member of the program committee of ASAP'2015.

Nathalie Revol was a member of the program committee of NRE1 at SuperComputing'15.

Bruno Salvy is a member of program committee of AofA'2016, Warsaw, Poland.

Damien Stehlé was member of the program committees of Latincrypt'15, Asiacrypt'15, PQCrypto'16, PKC'15 and '16. He is a member of the program committee of ANTS'16 and SCN'16.

10.1.3. Journal

10.1.3.1. 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*.

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 collections *Texts and Monographs in Symbolic Computation* (Springer) and *Mathématiques et Applications* (SMAI-Springer).

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

10.1.4. Invited talks

Claude-Pierre Jeannerod was an invited speaker at the MACIS conference (Sixth International Conference on Mathematical Aspects of Computer and Information Sciences, Berlin, November 2015).

Damien Stehlé gave two invited talks at the HEAT workshop on fully homomorphic encryption and multilinear maps, held in Paris in October. He gave an invited talk at a Sloan Foundation workshop on the mathematics of modern cryptography, which was held in Berkeley in July. He gave two invited talks at the summer school on real-world crypto and privacy that was held in Sibenik in June.

10.1.5. 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).

Claude-Pierre Jeannerod is a member 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 general standard has been published in July 2015 (IEEE 1788-2015) and the work now addresses the set-based model (IEEE P1788.1). She was a member of a hiring committee at U. Montpellier 2 (MCF position). She is a member of the Equality-Parity Committee at Inria.

10.1.6. 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.

10.1.7. 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.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master: Nicolas Brisebarre, *Introduction to Effective Approximation Theory* (24h), Hanoi Institute of Mathematics (Vietnam).

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: Fabien Laguillaumie, Cryptography, Error Correcting Codes, 150h, Université Claude Bernard Lyon 1.

Master: Vincent Lefèvre, *Arithmétique des ordinateurs* (20h), M2 ISFA (Institut de Science Financière et d'Assurances), Université Claude Bernard Lyon 1.

Master: Benoît Libert, Advanced cryptographic protocols, 24h, ENS de Lyon; Computer science and privacy, 12h, ENS de Lyon; Cryptography, 12h, ENS de Lyon; Public-key cryptology, (21h), M2 ISFA (Institut de Science Financière et d'Assurances), Université Claude Bernard Lyon 1.

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

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

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

Master: Damien Stehlé, Cryptography, 24h, ENS de Lyon.

Master: Nicolas Louvet, *Compilation* (24h), Lyon 1.

Bachelor: Nicolas Louvet, *Algorithmique*, *Architecture des ordinateurs*, *Unix*, ..., (170h), Lyon 1.

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

Divers: Bruno Salvy, Introduction à la D-finitude (2h), *Leçons de mathématiques d'aujourd'hui*, Bordeaux.

10.2.2. Supervision

- 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: Silviu Filip, *Filtroptim : tools for an optimal synthesis of numerical filters*, since September 2013, co-supervised by Nicolas Brisebarre and Guillaume Hanrot.
- 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, co-supervised by Benoît Libert (95%) and Damien Stehlé (5%).
- PhD in progress: Vincent Neiger, *Multivariate interpolation in computer algebra: efficient algorithms ans applications*, since September 2013, co-supervised by Claude-Pierre Jeannerod and Gilles Villard (together with Éric Schost (Western University, London, Canada)).
- 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 : Serge Torres, *Some tools for the design of efficient and reliable function evaluation libraries*, since September 2010, co-supervised by Nicolas Brisebarre and Jean-Michel Muller.
- PhD in progress: Weiqiang Wen, *Hard problems on lattices*, since September 2015, supervised by Damien Stehlé.

10.2.3. Juries

Nicolas Brisebarre was in the PhD committee of Catherine Lelay (LRI, Inria Saclay, Université Paris-Sud) and Esteban Segura Ugalde (XLIM, Université de Limoges).

Fabien Laguillaumie was in the PhD committee of Oliver Sanders (DI, ENS Paris, Orange Labs).

Benoît Libert was a reviewer and a member of the PhD committee for the PhD thesis of Olivier Sanders (DI, ENS Paris, Orange Labs).

Nathalie Revol was in the PhD committee of Qiaochu Li (Université de Technologie de Compiègne).

Bruno Salvy was a reviewer for the PhD thesis of Amaury Pouly (LIX, École polytechnique). He was in the PhD committees of Simone Naldi (LAAS, Toulouse) and Romain Serra (LAAS, Toulouse).

Damien Stehlé was a reviewer for the PhD theses of Thomas Prest (DI, ENS Paris), Zheng Wang (Imperial College, UK), Rina Zeitoun (LIP6, UPMC) and Cheng Shantian (NTU, Singapore). He is in the PhD committee of Thijs Laarhoven (TU Eindhoven, The Netherlands) and in the Habilitation thesis of Ludovic Perret (LIP6, UPMC).

10.3. Popularization

Nicolas Brisebarre co-organizes scientific conferences, called «Éclats de sciences», at Maison du Livre, de l'Image et du Son in Villeurbanne. Around three conferences take place per year.

Nathalie Revol is a member of the steering committee of the MMI: Maison des Mathématiques et de l'Informatique. She led a "Coding morning" for Inria assistants at Montbonnot (February 2015). She gave two conferences for high-school teachers (Montbonnot, February and Grenoble, May 2015). As an incentive for high-school pupils, and especially girls, to choose scientific careers, she gave talks at Lycée Simone Veil (Châtillon d'Azergues) and Mondial des Métiers (both in March 2015). She gave conferences for Rallye des Maths (May 2015) and during the Science Fair (2 high-school classes, October 2015). During the Science Fair, she was also present one afternoon at Médiathèque du Bachut - Lyon 8e. She presented computer science unplugged for primary school pupils (CM1, École Guilloux, St-Genis-Laval: 8 lectures of 45mn each) and computer science plugged (CM2, École Guilloux, St-Genis-Laval: 10 lectures of 1h in 2015-2016, 2 classes). She presented this work during Forum Maths Vivantes (October 2015). She also met people from Ébulliscience and FERS (Fondation Entreprise Réussite Scolaire) to give advice on their projects of popularization of computer science towards primary schools and high school pupils.

11. Bibliography

Publications of the year

Articles in International Peer-Reviewed Journals

[1] M. Bardet, J.-C. Faugère, B. Salvy. *On the complexity of the F5 Gröbner basis algorithm*, in "Journal of Symbolic Computation", September 2015, vol. 70, pp. 49–70 [*DOI :* 10.1016/j.jsc.2014.09.025], https://hal.inria.fr/hal-01064519

[2] S. BHATTACHERJEE, P. SARKAR. *Reducing Communication Overhead of the Subset Difference Scheme*, in "IEEE Transactions on Computers", 2015, https://hal.archives-ouvertes.fr/hal-01241138

[3] M. F. I. CHOWDHURY, C.-P. JEANNEROD, V. NEIGER, E. SCHOST, G. VILLARD. *Faster Algorithms for Multivariate Interpolation with Multiplicities and Simultaneous Polynomial Approximations*, in "IEEE Transactions on Information Theory", 2015, pp. 2370-2387 [*DOI :* 10.1109/TIT.2015.2416068], https://hal.inria.fr/hal-00941435

[4] 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", November 2015, https://hal.archives-ouvertes.fr/hal-01084238

[5] S. GRAILLAT, V. LEFÈVRE, J.-M. MULLER. *On the maximum relative error when computing integer powers by iterated multiplications in floating-point arithmetic*, in "Numerical Algorithms", November 2015, vol. 70, n^{o} 3, pp. 653-667 [*DOI :* 10.1007/S11075-015-9967-8], https://hal-ens-lyon.archives-ouvertes.fr/ensl-00945033

[6] A. LANGLOIS, D. STEHLÉ. *Worst-case to average-case reductions for module lattices*, in "Designs, Codes and Cryptography", 2015 [*DOI :* 10.1007/S10623-014-9938-4], https://hal.archives-ouvertes.fr/hal-01240452

[7] É. MARTIN-DOREL, G. HANROT, M. MAYERO, L. THÉRY. *Formally verified certificate checkers for hardest-to-round computation*, in "Journal of Automated Reasoning", 2015, vol. 54, n^{o} 1, pp. 1-29 [*DOI :* 10.1007/s10817-014-9312-2], https://hal.inria.fr/hal-00919498

[8] J.-M. MULLER. *On the error of Computing ab + cd using Cornea, Harrison and Tang's method*, in "ACM Transactions on Mathematical Software", January 2015, vol. 41, n^{o} 2, 8 p. , https://hal-ens-lyon.archives-ouvertes.fr/ensl-00862910

[9] S. M. RUMP, F. BÜNGER, C.-P. JEANNEROD. *Improved error bounds for floating-point products and Horner's scheme*, in "BIT Numerical Mathematics", March 2015, 14 p. [*DOI :* 10.1007/S10543-015-0555-Z], https://hal.inria.fr/hal-01137652

International Conferences with Proceedings

[10] M. R. ALBRECHT, C. COCIS, F. LAGUILLAUMIE, A. LANGLOIS. *Implementing Candidate Graded Encoding Schemes from Ideal Lattices*, in "Asiacrypt 2015", Auckland, New Zealand, T. IWATA, J. H. CHEON (editors), Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II, Springer, November 2015, vol. 9453 [*DOI :* 10.1007/978-3-662-48800-3_31], https://hal.inria.fr/hal-01237355

[11] *Best Paper*
S. BAI, A. LANGLOIS, T. LEPOINT, D. STEHLÉ, R. STEINFELD. *Improved security proofs in lattice-based cryptography: using the Rényi divergence rather than the statistical distance*, in "ASIACRYPT", Auckland, New Zealand, 2015, https://hal.archives-ouvertes.fr/hal-01240434.

[12] A. BOSTAN, L. DUMONT, B. SALVY. *Algebraic Diagonals and Walks*, in "ISSAC'15 International Symposium on Symbolic and Algebraic Computation", Bath, United Kingdom, ACM Press, July 2015, pp. 77–84 [*DOI :* 10.1145/2755996.2756663], https://hal.archives-ouvertes.fr/hal-01240729

[13] G. CASTAGNOS, F. LAGUILLAUMIE. *Linearly Homomorphic Encryption from DDH*, in "The Cryptographer's Track at the RSA Conference 2015", San Francisco, United States, Topics in Cryptology — CT-RSA 2015, April 2015, n^{o} 9048 [*DOI :* 10.1007/978-3-319-16715-2_26], https://hal.archives-ouvertes.fr/hal-01213284

[14] *Best Paper*
J. H. CHEON, K. HAN, C. LEE, H. RYU, D. STEHLÉ. *Cryptanalysis of the Multilinear Map over the Integers*, in "EUROCRYPT", Sofia, Bulgaria, 2015, https://hal.archives-ouvertes.fr/hal-01240445.

[15] J. H. CHEON, D. STEHLÉ. *Fully Homomophic Encryption over the Integers Revisited*, in "EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques", Sofia, Bulgaria, April 2015, pp. 513-536 [*DOI :* 10.1007/978-3-662-46800-5_20], https://hal.archives-ouvertes.fr/hal-01240437

[16] *Best Paper*
J.-G. DUMAS, C. PERNET, Z. SULTAN. *Computing the Rank Profile Matrix*, in "ISSAC", Bath, United Kingdom, K. YOKOYAMA (editor), ISSAC 2015, ACM, July 2015, pp. 146–153 [*DOI :* 10.1145/2755996.2756682], https://hal.archives-ouvertes.fr/hal-01107722.

[17] B. LIBERT, M. JOYE, M. YUNG, T. PETERS. *Secure Efficient History-Hiding Append-Only Signatures in the Standard Model*, in "Public Key Cryptography 2015 (PKC 2015)", Washington DC, United States, Public Key Cryptography 2015 (PKC 2015), Springer, March 2015, vol. 9020 [*DOI :* 10.1007/978-3-662-46447-2_20], https://hal.inria.fr/hal-01225344

[18] B. LIBERT, T. PETERS, M. JOYE, M. YUNG. *Compactly Hiding Linear Spans: Tightly Secure Constant-Size Simulation-Sound QA-NIZK Proofs and Applications*, in "Advances in Cryptology - Asiacrypt 2015", Auckland, New Zealand, Advances in Cryptology - Asiacrypt 2015, IACR, November 2015, https://hal.inria.fr/hal-01225363

[19] B. LIBERT, T. PETERS, M. YUNG. *Short Group Signatures via Structure-Preserving Signatures: Standard Model Security from Simple Assumptions*, in "Advances in Cryptology - Crypto 2015", Santa Barbara, United States, Advances in Cryptology - Crypto 2015, Springer, August 2015, vol. 9216 [*DOI :* 10.1007/978-3-662-48000-7_15], https://hal.inria.fr/hal-01225353

[20] S. MAULAT, B. SALVY. *Formulas for Continued Fractions. An Automated Guess and Prove Approach*, in "ISSAC'15", Bath, United Kingdom, ACM Press, July 2015 [*DOI :* 10.1145/2755996.2756660], https://hal.inria.fr/hal-01227259

Scientific Books (or Scientific Book chapters)

[21] *Proceedings of IEEE 22nd Symposium on Computer Arithmetic*, IEEE, Lyon, France, June 2015 [*DOI :* 10.1109/ARITH.2015.1], https://hal.inria.fr/hal-01233867

Research Reports

[22] R. Serra, D. Arzelier, M. Joldes, J.-B. Lasserre, A. Rondepierre, B. Salvy. *A Power Series Expansion based Method to compute the Probability of Collision for Short-term Space Encounters*, LAAS-CNRS, March 2015, Rapport LAAS n° 15072, https://hal.archives-ouvertes.fr/hal-01131384

Other Publications

[23] S. Agrawal, B. Libert, D. Stehlé. *Fully Secure Functional Encryption for Linear Functions from Standard Assumptions*, November 2015, working paper or preprint, https://hal.inria.fr/hal-01228559

[24] A. Bostan, L. Dumont, B. Salvy. *Algebraic Diagonals and Walks: Algorithms, Bounds, Complexity*, October 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01244914

[25] A. Bostan, P. Lairez, B. Salvy. *Multiple binomial sums*, October 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01220573

[26] N. Brisebarre, C. Lauter, M. Mezzarobba, J.-M. Muller. *Comparison between binary and decimal floating-point numbers*, June 2015, working paper or preprint [*DOI :* 10.1109/TC.2015.2479602], https://hal.archives-ouvertes.fr/hal-01021928

[27] J.-G. Dumas, C. Pernet, Z. Sultan. *Fast Computation of the Rank Profile Matrix and the Generalized Bruhat Decomposition*, December 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01251223

[28] S.-I. Filip. *A robust and scalable implementation of the Parks-McClellan algorithm for designing FIR filters*, March 2015, Preliminary version submitted for publication, https://hal.inria.fr/hal-01136005

[29] C.-P. Jeannerod. *A radix-independent error analysis of the Cornea-Harrison-Tang method*, 2015, To appear in ACM Trans. Math. Software, https://hal.inria.fr/hal-01050021

[30] C.-P. Jeannerod. *Exploiting structure in floating-point arithmetic*, December 2015, Invited paper - MACIS 2015 (Sixth International Conference on Mathematical Aspects of Computer and Information Sciences), https://hal.inria.fr/hal-01247059

[31] C.-P. Jeannerod, P. Kornerup, N. Louvet, J.-M. Muller. *Error bounds on complex floating-point multiplication with an FMA*, 2015, working paper or preprint, https://hal.inria.fr/hal-00867040

[32] C.-P. Jeannerod, N. Louvet, J.-M. Muller, A. Plet. *A Library for Symbolic Floating-Point Arithmetic*, November 2015, working paper or preprint, https://hal.inria.fr/hal-01232159

[33] C.-P. Jeannerod, N. Louvet, J.-M. Muller, A. Plet. *Sharp error bounds for complex floating-point inversion*, September 2015, working paper or preprint, https://hal-ens-lyon.archives-ouvertes.fr/ensl-01195625

[34] C.-P. Jeannerod, V. Neiger, E. Schost, G. Villard. *Computing minimal interpolation bases*, December 2015, working paper or preprint, https://hal.inria.fr/hal-01241781

[35] C.-P. JEANNEROD, S. M. RUMP. *On relative errors of floating-point operations: optimal bounds and applications*, December 2015, working paper or preprint, https://hal.inria.fr/hal-00934443

[36] M. JOLDES, O. MARTY, J.-M. MULLER, V. POPESCU. *Arithmetic algorithms for extended precision using floating-point expansions*, June 2015, Rapport LAAS n° 15016, https://hal.archives-ouvertes.fr/hal-01111551

[37] J. LE MAIRE, N. BRUNIE, F. DE DINECHIN, J.-M. MULLER. *Computing floating-point logarithms with fixed-point operations*, November 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01227877

[38] V. LEFÈVRE. *Correctly Rounded Arbitrary-Precision Floating-Point Summation*, 2015, working paper or preprint, https://hal.inria.fr/hal-01242127

[39] A. PELLET-MARY, D. STEHLÉ. *Cryptanalysis of Gu's ideal multilinear map*, 2015, Non, https://hal.archives-ouvertes.fr/hal-01240457

[40] R. SERRA, D. ARZELIER, M. JOLDES, J.-B. LASSERRE, A. RONDEPIERRE, B. SALVY. *A Fast and Accurate Method to Compute the Probability of Collision for Short-term Space Encounters*, 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01132149

[41] L. THÉVENOUX, P. LANGLOIS, M. MARTEL. *Automatic source-to-source error compensation of floating-point programs: code synthesis to optimize accuracy and time*, December 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01236919