IN PARTNERSHIP WITH:
CNRS

Université Claude Bernard (Lyon 1)

Ecole normale supérieure de Lyon

Activity Report 2014

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

Keywords: Computer Arithmetic, Computer Algebra, Cryptology, Interval Analysis

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

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]
Weiqiang Wen [ENS Lyon, until Jul 2014]

Faculty Members

Stef Graillat [Univ. Paris VI, Associate Professor, until Aug 2014, HdR]
Guillaume Hanrot [ENS Lyon, Professor, HdR]
Fabien Laguillaumie [Univ. Lyon I, Professor]
Nicolas Louvet [Univ. Lyon I, Associate Professor]
Clément Pernet [Univ. Grenoble I, Associate Professor, HdR]
Damien Stehlé [ENS Lyon, Professor, HdR]

Engineer

Serge Torres [ENS Lyon]

PhD Students

Nicolas Brunie [CIFRE grant (Kalray), until Apr 2014]
Silviu Filip [ENS Lyon]
Adeline Langlois [ENS Cachan, until Oct 2014]
Sébastien Maulat [ENS Lyon, from Sep 2014]
Vincent Neiger [ENS Lyon and Western University (London, Canada), international co-direction]
Marie Paindavoine [ENS Lyon and Orange Labs]
Antoine Plet [ENS Lyon, from Sep 2014]
Valentina Popescu [ENS Lyon, from Sep 2014]
Philippe Théveny [ENS Lyon, until Oct 2014]
Stephen Melczer [NSERC, from Sep 2014]

Post-Doctoral Fellows

Shi Bai [ENS Lyon, from Dec 2014]
Rishiraj Bhattacharyya [ENS Lyon, until Mar 2014]
Benoît Libert [ENS Lyon]

Visiting Scientists

Jie Chen [ECNU (China), Nov 2014]
Jung Hee Cheon [SNU (South Korea), Aug 2014]
Changmin Lee [SNU (South Korea), Aug 2014]

Administrative Assistants

Chiraz Benamor [CNRS, from Nov 2014]
Damien Séon [ENS Lyon, until Nov 2014]

Others

Laura-Roxana Chira [ENS Lyon, L3 Intern Student, from Jul 2014 until Sep 2014]
Catalin Cocis [Inria, M2 Intern Student, from Feb 2014 until Jun 2014]
François Colas [ENS Lyon, M2 Intern Student, from Feb 2014 until Jun 2014]
Thomas Gregoire [ENS Lyon, M2 Intern Student, from Feb 2014 until Jul 2014]
Valentin Le Fèvre [ENS Lyon, L3 Intern Student, from Jun 2014 until Jul 2014]
Mihai-Ioan Popescu [ENS Lyon, M2 Intern Student, from May 2014 until Aug 2014]
Saurabh Yadav [Inria, L3 Intern Student, from Jul 2014 until Aug 2014]

2. Overall Objectives

2.1. Overview

The overall objective of AriC is, through computer arithmetic, to improve computing at large, in terms of performance, efficiency, and reliability. We work on arithmetic algorithms (integer and floating-point arithmetic, complex arithmetic, multiple-precision arithmetic, finite-field arithmetic) and their implementation, approximation methods, Euclidean lattices and cryptology, certified computing and computer algebra. Specifically, we focus on the following domains:

1. **Floating-point arithmetic:** The IEEE 754-2008 standard specifies the behavior of floating-point arithmetic. We are interested in preparing future evolutions of the standard, in implementing it efficiently on embedded processors, in exploring its "low level" properties for better numerical analysis (for instance by finding certified and tight error bounds of numerical algorithms), and in building correctly rounded mathematical function programs. We are also interested in designing efficient algorithms and software for multiple-precision arithmetic and complex arithmetic.
2. **Certified computing and computer algebra:** We are interested in computing certified approximations using computer algebra and formal proof systems, in analyzing the fundamental algorithms of semi-numerical computation, in finding best or nearly best approximations under special constraints, and in designing efficient algorithms for exact linear algebra. Also, we are working on the development and standardization of interval arithmetic.
3. **Cryptography and lattices:** Lattice-based cryptography (LBC) is a fast developing field, raising fascinating questions both on cryptography and lattices. Lattice algorithmics is an established research area that is being revived by the amazing application that is LBC and by the new tools and concepts that it introduced. We aim at contributing to a major technological switch, from conventional to lattice-based cryptography. This will help suppress the main limitation to the expansion of the cloud economy that are the privacy concerns. Further, thanks to the ubiquity of lattices, our work may significantly impact several other fields, including coding, computer algebra, and computer arithmetic.

3. Research Program

3.1. Lattice-based cryptography

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 will work on three directions, detailed now.

3.1.1. 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).

3.1.2. 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 last section). 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.

3.1.3. 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 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/)

3.2. Efficient approximation methods

3.2.1. 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.

3.2.2. 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 first important challenge that we want to address 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.

3.2.3. 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-tound cases are a precious help for building libraries of correctly rounded mathematical functions. The current code, based on Lefèvre 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.

3.3. High-performance reliable 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. Algorithmic design and analysis of symbolic or numerical algorithms.

On the symbolic side, we have so far obtained fast algorithms for basic operations on both polynomial matrices and structured matrices, but in a rather independent way. Both types turn out to have much in common, but this is sometimes not reflected by the complexities obtained, especially for applications in cryptology and coding theory. Our long term goal in this area is thus to explore these connections further, to provide a more unified treatment and bridge these complexity gaps, and to produce associated efficient implementations. A first step towards this goal will be the design and implementation of enhanced algorithms for various generalizations of Hermite-Padé approximation; in the context of list decoding, this should in particular make it possible to improve over the structured-matrix approach, which is so far the fastest known.

On the numerical side, we will continue to revisit and improve the classical error bounds of numerical analysis in the light of all the subtleties of IEEE floating-point arithmetic. These aspects will be developed jointly with the "symbolic floating-point" approach presented in the next paragraph. A complementary approach will also be studied, based on the estimation (possibly via automatic differentiation) of condition numbers in order to identify inputs leading to large backward errors. Finally, concerning interval arithmetic, a thorough analysis of the accuracy of several representations, such as mid-rad, is also to be done.

3.3.2. Symbolic floating-point arithmetic.

Our work 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. A long-term goal here is 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. This is a completely new direction, whose main outcome will be a “symbolic floating-point toolbox” distributed in computer algebra systems like Sage and or Maple. In particular, such a toolbox will provide a way to check automatically the certificates of optimality we have obtained on the error bounds of various numerical algorithms. A PhD student has started on this subject in September 2014.

3.3.3. High-performance multiple precision arithmetic libraries.

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 is 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. We are in close contact with Warwick Tucker (Uppsala University, Sweden) and Mioara Joldes (LAAS, Toulouse) on this topic. A PhD student funded by a Région Rhône-Alpes grant has started on this topic in September 2014.

3.3.4. Interactions between arithmetics.

We will work on the interplay between floating-point and integer arithmetics, and especially on how to make the best use of both integer and floating-point basic operations when designing floating-point numerical kernels for embedded devices. This will be done in the context of the Metalibm ANR project and of our collaboration with STMicroelectronics. In addition, 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 using the fixed-precision hardware available for IEEE 754-2008 floating-point arithmetic. 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.

3.3.5. Adequation algorithms/architectures.

So far, we have investigated how specific instructions like the fused multiply-add (FMA) impact the accuracy of computations, and have proposed several highly accurate FMA-based algorithms. The FMA being available on several recent architectures, we now want to understand its impact on such algorithms in terms of practical performances. This should be a medium term project, leading to FMA-based algorithms with best speed/accuracy/robustness tradeoff. On the other hand (and on the long term), a major issue is how to exploit the various levels of parallelism of recent and upcoming architectures to ensure simultaneously high performance and reliability. A first direction will be to focus on SIMD parallelism, offered by instruction sets via vector instructions. This kind of parallelism should be key for small numerical kernels like elementary functions, complex arithmetic, or low-dimensional matrix computations. A second direction will be at the multi-core processor level, especially for larger numerical or algebraic problems (and in conjunction with SIMD parallelism when handling sub-problems of small enough dimension). Finally, we will work on aspects of automatic adaptation (auto-tuning) to such architectural features, not only for speed, but also for accuracy. This could be done via the design and implementation of heuristics capable of inserting more accurate codes, based for example on error-free transforms, whenever needed.

4. Application Domains

4.1. Hardware Arithmetic

The application domains of hardware arithmetic operators are

- digital signal processing;
- image processing;
- embedded applications;
- reconfigurable computing;
- cryptography.

4.2. 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.

4.3. Cryptography, Cryptology, Communication Theory

Lattice reduction algorithms have direct applications in

- public-key cryptography.

Another interesting field of application is

- communications theory.

5. New Software and Platforms

5.1. Overview

AriC software realizations are accessible from the web page http://www.ens-lyon.fr/LIP/AriC/ware. We describe below only those which progressed in 2014.

5.2. GNU MPFR

Participant: Vincent Lefèvre [correspondant].

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.

MPFR was one of the main pieces of software developed by the old SPACES team at Loria. Since late 2006, with the departure of Vincent Lefèvre to Lyon, it has become a joint project between the Caramel (formerly SPACES then CACAO) and the AriC (formerly Arénaire) project-teams. MPFR has been a GNU package since 26 January 2009.

An MPFR-MPC developers meeting took place from 20 to 22 January 2014 in Nancy. There was no new release this year, but various developments were done in the trunk.

The main work done in the AriC project-team:

- Changed the behavior of the `mpfr_set_exp` function to avoid undefined behavior in some cases (this change mainly impacted the internal usage).
- Bug fixes and various improvements (portability, efficiency, etc.).
- The `mpfr_sum` function is being rewritten (`new-sum` branch); see Section 6.2.8.

URL: http://www.mpfr.org/

GNU MPFR is on the Black Duck Open Hub community platform for free and open source software: https://www.openhub.net/p/gnu-mpfr

- ACM: D.2.2 (Software libraries), G.1.0 (Multiple precision arithmetic), G.4 (Mathematical software).
- AMS: 26-04 Real Numbers, Explicit machine computation and programs.
- APP: no longer applicable (copyright transferred to the Free Software Foundation).
- License: LGPL version 3 or later.
- Type of human computer interaction: C library, callable from C or other languages via third-party interfaces.
- OS/Middleware: any OS, as long as a C compiler is available.
- Required library or software: GMP.
- Programming language: C.
- Documentation: API in texinfo format (and other formats via conversion); algorithms are also described in a separate document.

5.3. 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 Perl scripts have been improved (in particular, for the interaction with Grid Engine).

5.4. FPLLL: A Lattice Reduction Library

Participant: Damien Stehlé [correspondant].

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 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.

This year, several improvements to the BKZ (block Korkine Zolotarev) algorithm have been implemented. Further, the library is now hosted on `github`.

URL: https://github.com/dstehle/fplll

- ACM: D.2.2 (Software libraries), G.4 (Mathematical software)
- APP: Procedure started
- License: LGPL v2.1
- Type of human computer interaction: C++ library callable, from any C++ program.
- OS/Middleware: any, as long as a C++ compiler is available.
- Required library or software: MPFR and GMP.
- Programming language: C++.
- Documentation: available in html format on **URL:** https://github.com/dstehle/fplll

5.5. Sipe

Participant: Vincent Lefèvre.

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.

New in 2014:

- `sipe_to_mpfr` function;
- support for `__float128` from GCC/libquadmath (implementing the binary128 format);
- some corrections.

URL: https://www.vinc17.net/research/sipe/

- ACM: D.2.2 (Software libraries), G.4 (Mathematical software).
- AMS: 26-04 Real Numbers, Explicit machine computation and programs.
- License: LGPL version 2.1 or later.
- Type of human computer interaction: C header file.
- OS/Middleware: any OS.
- Required library or software: GCC compiler.
- Programming language: C.
- Documentation: comment at the beginning of the code and Research report Inria RR-7832.

5.6. Gfun

Participant: Bruno Salvy.

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. This year, the implementation effort was focused on speeding up the guessing routines in the case of sequences with symbolic parameters that come up in general hypergeometric identities.

6. New Results

6.1. Arithmetic operators

6.1.1. A table-based method to evaluate trigonometric functions

Linear (order-one) function evaluation schemes, such as bipartite and multipartite tables, are usually effective for low precision approximations. For high output precision, the lookup table size is often too large for practical use. Dong Wang and Milos Ercegovac (UC Los Angeles) and Nicolas Brisebarre and Jean-Michel Muller investigate the so-called (M, p, k) scheme that reduces the range of input argument to a very small interval so that trigonometric functions can be approximated with very small lookup tables and a few additions/subtractions. An optimized hardware architecture is proposed and implemented in both FPGA device and standard cell based technology. Experimental results show that the proposed scheme achieves more than 50% reduction in total chip area compared with the best linear approach for 24-bit evaluation [14].

6.2. Floating-Point arithmetic

6.2.1. On the computation of the reciprocal of floating point expansions using an adapted Newton-Raphson iteration

Many numerical problems require a higher computing precision than that offered by common floating point (FP) formats. One common way of extending the precision is to represent numbers in a *multiple component* format. With so-called *floating point expansions*, numbers are represented as the unevaluated sum of standard machine precision FP numbers. This format offers the simplicity of using directly available and highly optimized FP operations and is used by multiple-precisions libraries such as Bailey's 'Q'D or the analogue Graphics Processing Units tuned version, GQD. Mioara Joldes (LAAS), Jean-Michel Muller, and Valentina Popescu introduced a new algorithm for computing the reciprocal FP expansion a^{-1} of a FP expansion a. Their algorithm is based on using an adapted Newton-Raphson iteration where "truncated" operations (additions, multiplications) involving FP expansions are used. The error analysis given shows that their algorithm allows for computations of very accurate quotients. Precisely, after $i \geq 0$ iterations, the computed FP expansion $x = x_0 + \cdots + x_{2^i - 1}$ satisfies the relative error bound $|\frac{x-a^{-1}}{a^{-1}}| \leq 2^{-2^i(p-3)-1}$, where $p > 4$ is the precision of the FP representation used ($p = 24$ for single precision and $p = 53$ for double precision) [19].

6.2.2. Error bounds on complex floating-point multiplication with a fused-multiply add

The accuracy analysis of complex floating-point multiplication done by Brent, Percival, and Zimmermann [*Math. Comp.*, 76:1469–1481, 2007] is extended by Peter Kornerup (Odense Univ. Denmark), Claude-Pierre Jeannerod, Nicolas Louvet, and Jean-Michel Muller [42] to the case where a fused multiply-add (FMA) operation is available. Considering floating-point arithmetic with rounding to nearest and unit roundoff u, they show that the bound $\sqrt{5}\,u$ on the normwise relative error $|\widehat{z}/z - 1|$ of a complex product z can be decreased further to $2u$ when using the FMA in the most naive way. Furthermore, they prove that the term $2u$ is asymptotically optimal not only for this naive FMA-based algorithm, but also for two other algorithms, which use the FMA operation as an efficient way of implementing rounding error compensation. Thus, although highly accurate in the componentwise sense, these two compensated algorithms bring no improvement to the normwise accuracy $2u$ already achieved using the FMA naively. Asymptotic optimality is established for each algorithm thanks to the explicit construction of floating-point inputs for which it is proven that the normwise relative error then generated satisfies $|\widehat{z}/z - 1| \to 2u$ as $u \to 0$. All these results hold for IEEE floating-point arithmetic, with radix $\beta \geq 2$, precision $p \geq 2$, and rounding to nearest; it is only assumed that underflows and overflows do not occur and, when bounding errors from below, that $\beta^{p-1} \geq 12$.

6.2.3. Refined error analysis of the Cornea-Harrison-Tang method for $ab + cd$

In their book *Scientific Computing on Itanium-based Systems*, Cornea, Harrison, and Tang introduced an accurate algorithm for evaluating expressions of the form $ab + cd$ in binary floating-point arithmetic, assuming a fused-multiply add instruction is available. They showed 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. Jean-Michel Muller improved 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 $2u$, he proved that this error bound is asymptotically optimal [11]. Claude-Pierre Jeannerod then showed in [41] that an error bound of the form $2u + 2u^2 + O(u^3)$ in fact holds for any radix $\beta \geq 2$, with $u = \frac{1}{2}\beta^{1-p}$. He also showed that the possibility of removing the $O(u^2)$ term from this bound depends on 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 $2u + \frac{1}{\beta}u^2$.

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

Stef Graillat (Paris 6 University), Vincent Lefèvre and Jean-Michel Muller improved 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. They also discussed the more general problem of computing the product of n terms [7].

6.2.5. Improved error bounds for numerical linear algebra

When computing matrix factorizations and solving linear systems in floating-point arithmetic, classical rounding error analyses provide backward error bounds whose leading terms have the form $\gamma_n = nu/(1 - nu)$ for suitable values of n and with u the unit roundoff. With Siegfried M. Rump (Hamburg University of Technology), Claude-Pierre Jeannerod showed in [13] that for LU and Cholesky factorizations as well as for triangular system solving, γ_n can be replaced by the $O(u^2)$-free and unconditional constant nu. To get these new bounds the main ingredient is a general framework for bounding expressions of the form $|\rho - s|$, where s is the exact sum of a floating-point number and $n - 1$ real numbers, and where ρ is a real number approximating the computed sum $\widehat{s}$.

6.2.6. On relative errors of floating-point operations

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 RN and barring underflow and overflow, such models bound the relative errors $E_1(t) = |t - \mathrm{RN}(t)|/|t|$ and $E_2(t) = |t - \mathrm{RN}(t)|/|\mathrm{RN}(t)|$ by the unit roundoff u. In [34] Claude-Pierre Jeannerod and Siegfried M. Rump (Hamburg University of Technology) investigated the possibility 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. They provided explicit and attainable bounds on $E_1(t)$, which are all less than or equal to $u/(1 + u)$ and, therefore, smaller than u. For $E_2(t)$ the bound u is attainable whenever $t = x \pm y$ or $t = xy$ or, in base > 2, $t = x/y$ with x, y two floating-point numbers. However, for division in base 2 as well as for square root, smaller bounds are derived, which are also shown to be attainable. This set of sharp bounds was then applied to the rounding error analysis of various numerical algorithms: in all cases, they obtained either much shorter proofs of the best-known error bounds for such algorithms, or improvements on these bounds themselves.

6.2.7. 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 [37].

6.2.8. Correctly rounded sum of floating-point numbers in GNU MPFR

Vincent Lefèvre has designed a new algorithm to compute the correctly rounded sum of several floating-point numbers, each having its own precision and the output having its own precision, as in GNU MPFR. At the same time, the `mpfr_sum` function is being reimplemented (not finished yet). While the old algorithm was just an application of Ziv's method, thus with exponential time and memory complexity in the worst case such as the sum of a huge number and a tiny number, the new algorithm does the sum by blocks (reiterations being needed only in case of cancellations), taking such holes between numbers into account.

6.3. Certified computing and computer algebra

6.3.1. Standardization of interval arithmetic

The IEEE 1788 working group is devoted to the standardization of interval arithmetic. V. Lefèvre and N. Revol are very active in this group. This year has been devoted to a ballot on the whole text of the standard [28], and to editorial work to make it compliant with IEEE rules. The final, remaining step, is the so-called "Sponsor ballot" and it should be completed in 2015.

6.3.2. Interval linear algebra on multi-core processors

For the product of matrices with interval coefficients, fast approximate algorithms have been developed by Philippe Théveny: they compute an enclosure of the exact product. These algorithms rely on the representation of intervals by their midpoints and radii. This representation allows one to use optimized routines for the multiplication of matrices with floating-point coefficients. In [4], the quality of the approximation of several algorithms is established, which accounts for roundoff errors and not only method's errors. A new algorithm is proposed, which requires even less (only 2) calls to a floating-point routine and still offers a good approximation quality, for a well specified type of input matrices. Three of the studied algorithms are implemented on a multi-core architecture. To avoid problems listed in [12] and to offer good performances, Philippe Théveny developed optimizations. The resulting implementations exhibit good performances: guaranteed results are obtained with an overhead less than 3, high numerical intensity and good scalability.

6.3.3. Numerical reproducibility

What is called *numerical reproducibility* is the problem of getting the same result when the scientific computation is run several times, either on the same machine or on different machines. In [12], the focus is on interval computations using floating-point arithmetic: Nathalie Revol and Philippe Théveny identified implementation issues that may invalidate the inclusion property, and presented several ways to preserve this inclusion property. This work has also been replaced in the larger context of numerical validation [15].

6.3.4. Faster multivariate interpolation with multiplicities

Muhammad Chowdhury (U. Western Ontario), Claude-Pierre Jeannerod, Vincent Neiger (ENS de Lyon), Éric Schost (U. Western Ontario), and Gilles Villard proposed in [38] a fast algorithm for interpolating multivariate polynomials with multiplicities. This algorithm relies on the reduction to a problem of simultaneous polynomial approximations, which is then solved using fast structured linear algebra techniques. This algorithm leads to the best known complexity bounds for the interpolation step of the list-decoding of Reed-Solomon codes, Parvaresh-Vardy codes or folded Reed-Solomon codes. In the special case of Reed-Solomon codes, it allows to accelerate the interpolation step of Guruswami and Sudan's list-decoding by a factor (list size)/(multiplicity).

6.3.5. Polynomial system solving

M. Bardet (U. Rouen), J.-C. Faugère (PolSys team) and B. Salvy studied 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. They gave a bound on the number of polynomials of each degree in a Gröbner basis computed by Faugère's F_5 algorithm 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) and used it to bound the complexity of the F_5 algorithm [5].

6.3.6. Linear differential equations

In [6], A. Bostan (SpecFun team), K. Raschel (U. Tours) and B. Salvy proved that the sequence $(e_n^{\mathfrak{S}})_{n\geq 0}$ of excursions in the quarter plane corresponding to a nonsingular step set $\mathfrak{S} \subseteq \{0, \pm 1\}^2$ with infinite group does not satisfy any nontrivial linear recurrence with polynomial coefficients. Accordingly, in those cases, the trivariate generating function of the numbers of walks with given length and prescribed ending point is not D-finite. Moreover, they displayed the asymptotics of $e_n^{\mathfrak{S}}$. This completes the classification of these walks.

Colleagues from the LAAS (Toulouse) and B. Salvy provided a new method for computing the probability of collision between two spherical space objects involved in a short-term encounter. In this specific framework of conjunction, classical assumptions reduce the probability of collision to the integral of a 2-D normal distribution over a disk shifted from the peak of the corresponding Gaussian function. Both integrand and domain of integration directly depend on the nature of the short-term encounter. Thus the inputs are the combined sphere radius, the mean relative position in the encounter plane at reference time as well as the relative position covariance matrix representing the uncertainties. The method they presented is based on an analytical expression for the integral. It has the form of a convergent power series whose coefficients verify a linear recurrence. It is derived using Laplace transform and properties of D-finite functions. The new method has been intensively tested on a series of test-cases and compares favorably to other existing works [29].

6.4. Lattices and cryptography

6.4.1. 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 RingLWE 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. Adeline Langlois and Damien Stehlé defined the Module-SIS and Module-LWE problems, which bridge SIS with Ring-SIS, and LWE with Ring-LWE, respectively. They proved that these average-case problems are at least as hard as standard lattice problems restricted to module lattices (which themselves bridge 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 [8].

6.4.2. Semantically Secure Lattice Codes for the Gaussian Wiretap Channel

Cong Ling (Imperial College, UK), Laura Luzzi (ENSEA), Jean-Claude Belfiore (Telecom ParisTech) and Damien Stehlé proposed a new scheme of wiretap lattice coding that achieves semantic security and strong secrecy over the Gaussian wiretap channel. The key tool in their security proof is the flatness factor which characterizes the convergence of the conditional output distributions corresponding to different messages and leads to an upper bound on the information leakage. They not only introduced the notion of secrecy-good lattices, but also proposed the flatness factor as a design criterion of such lattices. Both the modulo-lattice

Gaussian channel and the genuine Gaussian channel are considered. In the latter case, they proposed a novel secrecy coding scheme based on the discrete Gaussian distribution over a lattice, which achieves the secrecy capacity to within a half nat under mild conditions. No a priori distribution of the message is assumed, and no dither is used in their proposed schemes [9].

6.4.3. GGHLite: More Efficient Multilinear Maps from Ideal Lattices

The Garg-Gentry-Halevi (GGH) Graded Encoding Scheme, based on ideal lattices, is the first plausible approximation to a cryptographic multilinear map. Unfortunately, the scheme requires very large parameters to provide security for its underlying encoding re-randomization process. Adeline Langlois, Damien Stehlé and Ron Steinfeld (Monash University, Australia) formalized, simplified and improved the efficiency and the security analysis of the re-randomization process in the GGH construction. This results in a new construction that they called GGHLite. In particular, they first lowered the size of a standard deviation parameter of the GGH re-randomization process from exponential to polynomial in the security parameter. This first improvement is obtained via a finer security analysis of the so-called drowning step of re-randomization, in which they applied the Rényi divergence instead of the conventional statistical distance as a measure of distance between distributions. Their second improvement is to reduce the number of randomizers needed to 2, independently of the dimension of the underlying ideal lattices. These two contributions allowed them to decrease the bit size of the public parameters to $O(\lambda \log^2 \lambda)$ in GGHLite, with respect to the security parameter λ (for a constant multilinearity parameter κ) [22].

6.4.4. LLL reducing with the most significant bits

Let B be a basis of a Euclidean lattice, and $\widetilde{B}$ an approximation thereof. Saruchi (IIT Delhi, India), Ivan Morel, Damien Stehlé and Gilles Villard gave a sufficient condition on the closeness between $\widetilde{B}$ and B so that an LLL-reducing transformation U for $\widetilde{B}$ remains valid for B. Further, they analysed an efficient reduction algorithm when B is itself a small deformation of an LLL-reduced basis. Applications include speeding-up reduction by keeping only the most significant bits of B, reducing a basis that is only approximately known, and efficiently batching LLL reductions for closely related inputs [30].

6.4.5. Hardness of k-LWE and Applications in Traitor Tracing

San Ling (NTU, Singapore), Duong Hieu Phan (LAGA), Damien Stehlé and Ron Steinfeld (Monash University, Australia) introduced the k-LWE problem, a Learning With Errors variant of the k-SIS problem. The Boneh-Freeman reduction from SIS to k-SIS suffers from an exponential loss in k. Ling *et al.* improved and extended it to an LWE to k-LWE reduction with a polynomial loss in k, by relying on a new technique involving trapdoors for random integer kernel lattices. Based on this hardness result, they presented the first algebraic construction of a traitor tracing scheme whose security relies on the worstcase hardness of standard lattice problems. The proposed LWE traitor tracing is almost as efficient as the LWE encryption. Further, it achieves public traceability, i.e., allows the authority to delegate the tracing capability to untrusted parties. To this aim, Ling *et al.* introduced the notion of projective sampling family in which each sampling function is keyed and, with a projection of the key on a well chosen space, one can simulate the sampling function in a computationally indistinguishable way. The construction of a projective sampling family from k-LWE allows us to achieve public traceability, by publishing the projected keys of the users [27].

6.4.6. Lattice-Based Group Signatures Scheme with Verifier-local Revocation

Support of membership revocation is a desirable functionality for any group signature scheme. Among the known revocation approaches, verifier-local revocation (VLR) seems to be the most flexible one, because it only requires the verifiers to possess some up-to-date revocation information, but not the signers. All of the contemporary VLR group signatures operate in the bilinear map setting, and all of them will be insecure once quantum computers become a reality. Adeline Langlois, San Ling, Khoa Nguyen and Huaxiong Wang (NTU, Singapore) introduced the first lattice-based VLR group signature [21], and thus, the first such scheme that is believed to be quantum-resistant. In comparison with existing lattice-based group signatures, this scheme has several noticeable advantages: support of membership revocation, logarithmic-size signatures, and weaker security assumption. In the random oracle model, our scheme is proved to be secure based on the hardness of the Shortest Independent Vector Problem with approximation factor $\gamma = \widetilde{O}(n^{1.5})$ - an assumption that is as weak as those of state-of-the-art lattice-based standard signatures. Moreover, this construction works without relying on encryption schemes, which is an intriguing feature for group signatures.

6.4.7. Proxy Re-Encryption Scheme Supporting a Selection of Delegatees

Julien Devigne (Orange Labs), Eleonora Guerrini (Univ. Montpellier 2, LIRMM) and Fabien Laguillaumie adapt the primitive of proxy re-encryption which allows a user to decide that in case of unavailability, one (or several) particular user, the delegatee, will be able to read his confidential messages. They modify it so that a sender can choose who among many potential delegatees will be able to decrypt his messages, and propose a simple and efficient scheme which is secure under chosen plaintext attack under standard algorithmic assumption in a bilinear setting. They also investigate the possibility to add a traceability of the proxy so that one can detect if it has leaked some re-encryption keys [17].

6.4.8. Practical validation of several fault attacks against the Miller algorithm

Ronan Lashermes (SAS-ENSMSE, PRISM), Marie Paindavoine, Nadia El Mrabet (Univ. P8, LIASD), Jacques Fournier (SAS-ENSMSE) and Louis Goubin (UVSQ, PRISM) describe practical implementations of fault attacks against the Miller algorithm, which computes pairing evaluations on algebraic curves. These implementations validate common fault models used against pairings. In the light of the implemented fault attacks, they show that some blinding techniques proposed to protect the algorithm against Side-Channels Analyses cannot be used as countermeasures against the implemented fault attacks [23].

6.4.9. Non-Malleability from Malleability: Simulation-Sound Quasi-Adaptive NIZK Proofs and CCA2-Secure Encryption from Homomorphic Signatures

Verifiability is central to building protocols and systems with integrity. Initially, efficient methods employed the Fiat-Shamir heuristics. Since 2008, the Groth-Sahai techniques have been the most efficient in constructing non-interactive witness indistinguishable and zero-knowledge proofs for algebraic relations in the standard model. For the important task of proving membership in linear subspaces, Jutla and Roy (Asiacrypt 2013) gave significantly more efficient proofs in the quasi-adaptive setting (QA-NIZK). For membership of the row space of a $t \times n$ matrix, their QA-NIZK proofs save $\Omega(t)$ group elements compared to Groth-Sahai. In [26], Benoît Libert, Thomas Peters (UCL, Belgique), Marc Joye (Technicolor, USA) and Moti Yung (Google and Columbia U, USA) gave QA-NIZK proofs made of a *constant* number group elements – regardless of the number of equations or the number of variables – and additionally proved them *unbounded* simulation-sound. Unlike previous unbounded simulation-sound Groth-Sahai-based proofs, their construction does not involve quadratic pairing product equations and does not rely on a chosen-ciphertext-secure encryption scheme. Instead, they built on structure-preserving signatures with homomorphic properties. They applied their methods to design new and improved CCA2-secure encryption schemes. In particular, they built the first efficient threshold CCA-secure keyed-homomorphic encryption scheme (*i.e.*, where homomorphic operations can only be carried out using a dedicated evaluation key) with publicly verifiable ciphertexts.

6.4.10. 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 [24], Benoît Libert, Marc Joye (Technicolor, USA) and Moti Yung (Google and Columbia U, USA) constructed 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). Their schemes 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, their schemes are erasure-free (reliable erasure is a hard to assure and hard to administer property in actual systems). 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).

6.4.11. Concise Multi-challenge CCA-Secure Encryption and Signatures with Almost Tight Security

To gain strong confidence in the security of a public-key scheme, it is most desirable for the security proof to feature a tight reduction between the adversary and the algorithm solving the under-lying hard problem. Recently, Chen and Wee (Crypto '13) described the first Identity-Based Encryption scheme with almost tight security under a standard assumption. Here, "almost tight" means that the security reduction only loses a factor $O(\lambda)$ – where λ is the security parameter – instead of a factor proportional to the number of adversarial queries. Chen and Wee also gave the shortest signatures whose security almost tightly relates to a simple assumption in the standard model. Also recently, Hofheinz and Jager (Crypto '12) constructed the first CCA-secure public-key encryption scheme in the multi-user setting with tight security. These constructions give schemes that are significantly less efficient in length (and thus, processing) when compared with the earlier schemes with loose reductions in their proof of security. Hofheinz and Jager's scheme has a ciphertext of a few hundreds of group elements, and they left open the problem of finding truly efficient constructions. Likewise, Chen and Wee's signatures and IBE schemes are somewhat less efficient than previous constructions with loose reductions from the same assumptions.

In [25], Benoît Libert, Thomas Peters (UCL, Belgique), Marc Joye (Technicolor, USA) and Moti Yung (Google and Columbia U, USA) considered space-efficient schemes with security almost tightly related to standard assumptions. As a step in solving the open question by Hofheinz and Jager, they constructed an efficient CCA-secure public-key encryption scheme whose chosen-ciphertext security in the multi-challenge, multi-user setting almost tightly relates to the DLIN assumption (in the standard model). Quite remarkably, the ciphertext size decreases to 69 group elements under the DLIN assumption whereas the best previous solution required about 400 group elements. Their scheme is obtained by taking advantage of a new almost tightly secure signature scheme (in the standard model) they developed and which is based on the recent concise proofs of linear subspace membership in the quasi-adaptive non-interactive zero-knowledge setting (QA-NIZK) defined by Jutla and Roy (Asiacrypt '13). The new signature scheme reduces the length of the previous such signatures (by Chen and Wee) by 37% under the Decision Linear assumption, by almost 50% under the K-LIN assumption, and it becomes only 3 group elements long under the Symmetric eXternal Diffie-Hellman assumption. Our signatures are obtained by carefully combining the proof technique of Chen and Wee and the above mentioned QA-NIZK proofs.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. Contracts with Bosch.

Two studies were conducted for Bosch (Stuttgart) on the numerical aspects of embedded computing. In the first one, Florent de Dinechin and Jean-Michel Muller dealt with the issue of the choice of an adequate representation of numbers (fixed-point or floating-point) for embedded systems. In the second one, Claude-Pierre Jeannerod reported on the stability and accuracy issues of linear system solving in finite-precision arithmetic.

7.1.2. Collaboration with Intel.

INTEL made a $20000 donation in recognition of our work on the correct rounding of functions.

7.2. Bilateral Grants with Industry

7.2.1. Collaboration with Kalray.

Nicolas Brunie has been supported by a CIFRE PhD grant (from 15/04/2011 to 14/04/2014) from Kalray. The purpose was the study of a tightly coupled reconfigurable accelerator to be embedded in the Kalray multicore processor.

7.2.2. Orange Labs PhD Grant.

Marie Paindavoine is supported by an Orange Labs PhD Grant (from October 2013 to November 2016). She works on privacy-preserving encryption mechanisms.

8. Partnerships and Cooperations

8.1. Regional Initiatives

The PhD grant of Valentina Popescu is funded by Région Rhône-Alpes through the ARC6 programme.

8.2. National Initiatives

8.2.1. ANR HPAC Project

Participants: Claude-Pierre Jeannerod, Nicolas Louvet, Clément Pernet, Nathalie Revol, Philippe Théveny, 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.

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 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.

8.2.3. 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.

8.2.4. PEPS Quarenum

Participants: Nicolas Louvet, Nathalie Revol.

“Quarenum” is an abbreviation for *Qualité et Reproductibilité Numériques dans le Calcul Scientifique Haute Performance*. This project focuses on the numerical quality of scientific software, more precisely of high-performance numerical codes. Numerical validation is one aspect of the project, the second one regards numerical reproducibility.

8.3. International Initiatives

8.3.1. Inria Associate Teams

QOLAPS (Quantifier elimination, Optimization, Linear Algebra and Polynomial Systems) is an Associate Team between the Symbolic Computation Group at North Carolina State University (USA), the PolSys team at LIP6, Paris 6, and the AriC team. Participants: Clément Pernet, Nathalie Revol, Gilles Villard.

8.3.2. Inria International Partners

8.3.2.1. Informal International Partners

Our international academic collaborators are from Courant Institute of Mathematical Sciences (USA), Hamburg University of Technology (Germany), Imperial College (UK), Macquarie University (Australia), Mc Gill University (Canada), Monash University (Australia), Nanyang Technological University (Singapore), North Carolina State University (USA), Technical University of Cluj-Napoca (Romania), University of California, Los Angeles (USA), University of Delaware (USA), University of Southern Denmark (Denmark), University of Western Ontario (Canada), University of Waterloo (Canada), Uppsala University (Sweden).

We also collaborate with Intel (Portland, USA).

8.3.3. Participation In other International Programs

- PICS CANTaL (Cryptography, Algorithmic Number Theory and Lattices). This is a collaborative project involving several AriC members (Nicolas Brisebarre, Guillaume Hanrot, Fabien Laguillaumie, Adeline Langlois and Damien Stehlé), and collaborators in several Australian universities: Christophe Doche (Macquarie University), Igor Shparlinski (UNSW) and Ron Steinfeld (Monash University). It was funded by the International office of the CNRS, for 2012, 2013 and 2014.
- IEEE P1788 working group for the standardization of interval arithmetic. We contributed to the creation in 2008 of this working group http://grouper.ieee.org/groups/1788/ and Nathalie Revol chairs this group since its creation. In 2014, the final draft text has been approved upon by the working group in June. The rest of the year was devoted to editorial polishing, before submitting the text to the “Sponsor ballot”, which constitutes the final step and should be completed in 2015. The annual in-person meeting, chaired by Nathalie Revol, took place at the end of the SCAN 2014 conference in Würzburg, Germany, the 26 September.

  Vincent Lefèvre actively participated in various discussions, either in the mailing-list or in small subgroups.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Many colleagues from all other the world visit us regularly for seminars and collaborations. We list only long visits here.

Jie Chen (assistant professor at ECNU, China) visited us for a month, in November. He collaborated with Fabien Laguillaumie, Benoît Libert and Damien Stehlé on functional encryption.

Jung Hee Cheon (professor at SNU, South Korea) and Changmin Lee (PhD student at SNU, South Korea) visited us for a month, in August. They collaborated with Damien Stehlé on the approximate greatest common divisor problem and its applications in homomorphic cryptography.

8.4.1.1. Internships

Mihai-Ioan Popescu (ENS de Lyon) did a Master 1 internship from May to July, under the supervision of Damien Stehlé. He worked on heuristic algorithms for short lattice vector enumeration.

François Colas (U. Grenoble) did a Master 2 internship from March to June, under the supervision of Damien Stehlé. He worked on lattice-based homomorphic encryption.

Catalin Cocis (ENS de Lyon) did a Master 2 internship from February to June under the supervision of Fabien Laguillaumie. He worked on the implementation of multilinear maps.

Laura Chira (Technological U. of Cluj, Romania) did an L3 Summer internship from July to September 2014. This internship was supervised by Benoît Libert and devoted to the implementation of pseudo-random functions based on hard algorithmic problems in lattices.

Thomas Grégoire (ENS de Lyon) did a Master 2 internship from February to June under the supervision of Nicolas Brisebarre. He designed some tools for the certified approximation of functions in various orthogonal bases.

Saurabh Yadav (2nd year student, Indian Institute of Technology Delhi, India) did a Summer internship supervised by Benoît Libert in July and August 2014. The goal was to study and survey the applications of a cryptographic primitive built on top of multi-linear maps and called “indistinguishability obfuscation.”

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific animation

- Guillaume Hanrot is director of the LIP laboratory (Laboratoire de l'Informatique du Parallélisme) since April 1, 2014. He was deputy director of the LIP before;
- Jean-Michel Muller is co-director of the Groupement de Recherche (GDR) *Informatique Mathématique* of CNRS;
- Gilles Villard has been director of the LIP laboratory until April 1, 2014.

9.1.2. Scientific events organisation

9.1.2.1. general chair, scientific chair

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).

9.1.2.2. member of the organizing committee

Bruno Salvy was one of the organizers of a workshop "Challenges in 21st Century Experimental Mathematical Computation", at ICERM, Providence, Rhode Island.

Nicolas Brisebarre and Jean-Michel Muller organized a one week workshop "Formal Proof, Symbolic Computation and Computer Arithmetic" which took place from February 3 to February 7 (50 participants), in the framework of a whole month devoted to "Mathematical Structures of Computation" in Lyon.

9.1.3. Scientific events selection

9.1.3.1. member of the conference program committee

Jean-Michel Muller was a member of the program committees of ASAP'2014 and ARITH'2015.

Damien Stehlé was a member of the program committees of LATINCRYPT'14, PQCrypto'14, and ACISP'14.

Bruno Salvy was a member of the program committee of AofA'2014.

Fabien Laguillaumie was a member of the program committee of Africacrypt'14.

Benoît Libert was a member of the program committee of ACM-CCS'14.

9.1.4. Journal

9.1.4.1. member of the editorial board

- 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*. He was co-guest editor of a special issue of the journal *Science of Computer Programming* [32].
- 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*.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master: Jean-Michel Muller, *Floating-Point Arithmetic and Formal Proof* (8h + coordination of the 24h course), ENS de Lyon.

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

Master: Claude-Pierre Jeannerod, Nicolas Louvet, 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* (20h), M2 ISFA (Institut de Science Financière et d'Assurances), Université Claude Bernard Lyon 1.

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

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

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

Master: Benoît Libert, Advances cryptographic protocols, 24h, ENS de Lyon.

Research school: Adeline Langlois, Fabien Laguillaumie, Damien Stehlé, *Chiffrement avancé à partir du problème Learning With Errors* (4h30), École de printemps Codes et Crypto, Université de Grenoble.

Research school: Adeline Langlois, Fabien Laguillaumie, Damien Stehlé, *Chiffrement avancé à partir du problème Learning With Errors* (4h30), École Jeunes Chercheurs en Informatique Mathématique, Université de Caen.

Research school: Damien Stehlé, *Cryptographie reposant sur les réseaux euclidiens* (3h), Colloque Jeunes Chercheurs en Théorie des Nombres.

9.2.2. Supervision

PhD : Nicolas Brunie, *Contribution à l'arithmétique des ordinateurs et applications aux systèmes embarqués*, ENS Lyon, May 2014, co-supervised by Florent de Dinechin (and Renaud Ayrignac).

PhD : Adeline Langlois, *Lattice - Based Cryptography - Security Foundations and Constructions*, ENS Lyon, October 2014, supervised by Damien Stehlé.

PhD : Philippe Théveny, *Numerical quality and high performance in interval linear algebra on multi-core Processors*, ENS Lyon, October 2014, supervised by Nathalie Revol.

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: 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: Louis Dumont, *Algorithmique efficace pour les diagonales, applications en combinatoire, physique et théorie des nombres*, co-supervised by Alin Bostan (SpecFun team) and Bruno Salvy.

PhD in progress: Sébastien Maulat, *Évaluation efficace et certifiée de fonctions différentiellement finies en précision modérée*, since september 2014, supervised by Bruno Salvy.

PhD in progress: Stephen Melczer, *Effective analytic combinatorics in one and several variables*, co-supervised by George Labahn (U. Waterloo, Canada) and Bruno Salvy.

9.2.3. Juries

In 2014, Jean-Michel Muller was vice-chair of the "Comité d'évaluation scientifique mathématiques–informatique théorique" of the ANR (the French national research agency). He participated to the PhD committees for the defenses of Laurent Thévenoux (Univ. Perpignan) and Karim Bigou (Univ. Rennes 1). He participated to the Habilitation committees for the defenses of Christophe Denis (Univ. Perpignan), Sylvie Boldo (Paris Sud Univ.) and David Defour (Univ. Perpignan). He was a member of the Scientific Council of ENS de Lyon until june 2014, and he is a member of the Scientific Council of CERFACS (Toulouse).

Bruno Salvy was a member of the PhD committees of Julien Courtien (Bordeaux), Jules Svartz (UPMC), and Pierre Lairez (École polytechnique).

Nathalie Revol was a member of the PhD committee of Olivier Mullier (École polytechnique). Nathalie Revol was in the hiring committee for junior researchers (CR) of Inria Grenoble - Rhône-Alpes and in the hiring committee for an assistant professor position at Université Paris Sud.

Damien Stehlé was reviewer of the PhD theses of Robert Fitzpatrick (Royal Holloway, UK), Tancrède Lepoint (ENS Paris, Univ. du Luxembourg and CryptoExperts) and Nicola di Pietro (Univ. Bordeaux).

Fabien Laguillaumie was reviewer for the PhD thesis of Alain Patey (Telecom ParisTech). He was part of the HDR committee of Damien Vergnaud (ENS).

Nicolas Louvet was a member of a hiring committee for an associate professor position at the university Montpellier 2.

9.3. Invited Conferences

- Damien Stehlé gave an invited talk *Secure lattice codes for the gaussian wiretap channel*, at the Algebra, Codes and Networks symposium, Bordeaux, France, in June 2014;
- Damien Stehlé gave an invited talk *The Learning with Errors problem*, at the Oberwolfach workshop on combinatorial optimization, Oberwolfach, Germany, in November 2014;
- Jean-Michel Muller gave two invited talks, *On the maximum relative error when computing x^n in floating-point arithmetic* (in Tokyo) and *On complex multiplication and division with an FMA* (in Kyoto), for the conference INVA 2014, Japan, in March 2014;
- Jean-Michel Muller gave an invited talk *Getting tight error bounds in floating-point arithmetic: illustration with complex functions, and the real x^n function*, at the workshop *NSV'2014: Numerical Software Verification*, Vienna, in July 2014.
- Bruno Salvy gave an invited talk *Algorithmic variations on linear differential equations* at the MBM2014 day organized in Bordeaux in October when Mireille Bousquet-Mélou received the silver medal of the CNRS. He was also invited to give a talk in Oberwolfach, for their meeting on Enumerative Combinatorics in March, where he talked about *Multiple Binomial Sums*, of which he had given a previous version in February at the "Holonomy days" where he had been invited in Grenoble.
- Nathalie Revol gave invited talks at the workshop "Challenges in 21st Century Experimental Mathematical Computation" at ICERM, Providence, Rhode Island, and at French seminars: CEA-LIST, Inria comité des projets, Aristote.
- Fabien Laguillaumie gave an invited scientific committee talk *Anonymity-oriented Signatures based on Lattices* at the YACC'14 conference, Porquerolles, France, in June 2014.

9.4. Popularization

- Sylvie Boldo (Proval project) and Jean-Michel Muller wrote a popular science paper *Des ordinateurs capables de calculer plus juste* in the journal *La Recherche* [36].
- 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 gave talks for pupils at collèges and lycées, as an incentive to choose scientific careers: lycée Camille Vernet (Valence, Drôme), lycée Jérémie de la Ville (Charlieu, Loire), lycée Gabriel Fauré (Annecy, Haute-Savoie), collège Jean Renoir (Neuville-sur-Saône, Rhône). During the "Week of mathematics", she gave a 2-hour talk at lycée de la Côtière (La Boisse, Ain). She gave the inaugural conference of the congress "Math en Jean's" in Lyon and the conference for the scientific camp "Math C2+" in Montbonnot. She was present for the "Mondial des Métiers" (Eurexpo Lyon, Chassieu, Rhône). For the Science Fair, she gave 2 talks at MMI, ENS de Lyon. In 2014, she met over 1000 pupils.

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] N. BRUNIE. *Contributions to computer arithmetic and applications to embedded systems*, Ecole Normale Supérieure de Lyon, May 2014, https://tel.archives-ouvertes.fr/tel-01078204

[2] A. LANGLOIS. *Lattice-Based Cryptography: Security Foundations and Constructions*, ENS Lyon, October 2014, https://hal.archives-ouvertes.fr/tel-01092130

[3] C. PERNET. *High Performance and Reliable Algebraic Computing*, Université Joseph Fourier, Grenoble 1, November 2014, Habilitation à diriger des recherches, https://tel.archives-ouvertes.fr/tel-01094212

[4] P. THÉVENY. *Numerical Quality and High Performance in Interval Linear Algebra on Multi-Core Processors*, ENS Lyon, October 2014, https://hal.inria.fr/tel-01107447

Articles in International Peer-Reviewed Journals

[5] M. BARDET, J.-C. FAUGÈRE, B. SALVY. *On the complexity of the F5 Gröbner basis algorithm*, in "Journal of Symbolic Computation", September 2014, pp. 1-24 [*DOI :* 10.1016/J.JSC.2014.09.025], https://hal.inria.fr/hal-01064519

[6] A. BOSTAN, K. RASCHEL, B. SALVY. *Non-D-finite excursions in the quarter plane*, in "Journal of Combinatorial Theory, Series A", January 2014, vol. 121, pp. 45-63 [*DOI :* 10.1016/J.JCTA.2013.09.005], https://hal.archives-ouvertes.fr/hal-00697386

[7] 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", 2015, 15 p. , forthcoming, https://hal-ens-lyon.archives-ouvertes.fr/ensl-00945033

[8] A. LANGLOIS, D. STEHLÉ. *Worst-case to average-case reductions for module lattices*, in "Designs, Codes and Cryptography", 2014, 35 p. , https://hal.archives-ouvertes.fr/hal-01091291

[9] C. LING, L. LUZZI, J.-C. BELFIORE, D. STEHLÉ. *Semantically Secure Lattice Codes for the Gaussian Wiretap Channel*, in "Information Theory, IEEE Transactions on", 2014, 18 p. , https://hal.archives-ouvertes.fr/hal-01091295

[10] 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

[11] 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

[12] N. REVOL, P. THÉVENY. *Numerical Reproducibility and Parallel Computations: Issues for Interval Algorithms*, in "IEEE Transactions on Computers", 2014, vol. 63, n^o 8, pp. 1915-1924, forthcoming [*DOI :* 10.1109/TC.2014.2322593], https://hal.inria.fr/hal-00916931

[13] S. M. RUMP, C.-P. JEANNEROD. *Improved backward error bounds for LU and Cholesky factorizations*, in "SIAM Journal on Matrix Analysis and Applications", 2014, vol. 35, n^o 2, pp. 684-698 [*DOI :* 10.1137/130927231], https://hal.inria.fr/hal-00841361

[14] D. WANG, J.-M. MULLER, N. BRISEBARRE, M. ERCEGOVAC. *(M, p, k)-Friendly Points: A Table-based Method to Evaluate Trigonometric Function*, in "IEEE Transactions on Circuits and Systems. Part II, Express Briefs", September 2014, vol. 61, n^o 9, pp. 711-715 [*DOI :* 10.1109/TCSII.2014.2331094], https://hal-ens-lyon.archives-ouvertes.fr/ensl-01001673

Articles in National Peer-Reviewed Journals

[15] F. JÉZÉQUEL, P. LANGLOIS, N. REVOL. *First steps towards more numerical reproducibility*, in "ESAIM: Proceedings", September 2014, vol. 45, pp. 229-238 [*DOI :* 10.1051/PROC/201445023], http://hal-lirmm.ccsd.cnrs.fr/lirmm-00872562

International Conferences with Proceedings

[16] B. BOYER, J.-G. DUMAS, P. GIORGI, C. PERNET, B. D. SAUNDERS. *Elements of Design for Containers and Solutions in the LinBox Library*, in "4th International Congress on Mathematical Software", Seoul, South Korea, Springer, August 2014, vol. 8592, 8 pages, https://hal.archives-ouvertes.fr/hal-01015138

[17] J. DEVIGNE, E. GUERRINI, F. LAGUILLAUMIE. *Proxy Re-Encryption Scheme Supporting a Selection of Delegatees*, in "7th International Conference on Cryptology AFRICACRYPT 2014", Marrakech, Morocco, LNCS, Springer, May 2014, https://hal.inria.fr/hal-00982549

[18] J.-G. DUMAS, T. GAUTIER, C. PERNET, Z. SULTAN. *Parallel computation of echelon forms*, in "EuroPar-2014", Porto, Portugal, August 2014, 12 p. , https://hal.archives-ouvertes.fr/hal-00947013

[19] M. JOLDES, J.-M. MULLER, V. POPESCU. *On the computation of the reciprocal of floating point expansions using an adapted Newton-Raphson iteration*, in "25th IEEE International Conference on Application-specific Systems, Architectures and Processors, ASAP", Zurich, Switzerland, June 2014, 8 p. , forthcoming, https://hal.archives-ouvertes.fr/hal-00957379

[20] E. L. KALTOFEN, C. PERNET. *Sparse Polynomial Interpolation Codes and their decoding beyond half the minimal distance*, in "ISSAC - 39th International Symposium on Symbolic and Algebraic Computation", Kobe, Japan, July 2014, In Proceedings of the International Symposium on Symbolic and Algebraic Computation 2014 (ISSAC'14) [*DOI :* 10.1145/2608628.2608660], https://hal.inria.fr/hal-01068308

[21] A. LANGLOIS, S. LING, K. NGUYEN, H. WANG. *Lattice-based Group Signature Scheme with Verifier-local Revocation*, in "Public-Key Cryptography - PKC2014", Buenos Aires, Argentina, H. KRAWCZYK (editor), Lecture Notes in Computer Science, Springer, March 2014, vol. 8383, pp. 345-361 [*DOI :* 10.1007/978-3-642-54631-0], https://hal.archives-ouvertes.fr/hal-00983084

[22] A. LANGLOIS, D. STEHLÉ, R. STEINFELD. *GGHLite: More Efficient Multilinear Maps from Ideal Lattices*, in "EUROCRYPT 2014", Copenhague, Denmark, May 2014, https://hal.archives-ouvertes.fr/hal-00983179

[23] R. LASHERMES, M. PAINDAVOINE, N. EL MRABET, J. FOURNIER, L. GOUBIN. *Practical validation of several fault attacks against the Miller algorithm*, in "FDTC - Workshop on Fault Diagnosis and Tolerance in Cryptography", Busan, South Korea, September 2014 [*DOI :* 10.1109/FDTC.2014.21], https://hal.archives-ouvertes.fr/hal-01100813

[24] B. LIBERT, M. JOYE, M. YUNG. *Born and Raised Distributively: Fully Distributed Non-Interactive Adaptively-Secure Threshold Signatures with Short Shares*, in "ACM Symposium on Principles of Distributed Computing (PODC 2014)", Paris, France, S. DOLEV (editor), ACM, July 2014, https://hal.inria.fr/hal-00983149

[25] B. LIBERT, M. JOYE, M. YUNG, T. PETERS. *Concise Multi-challenge CCA-Secure Encryption and Signatures with Almost Tight Security*, in "Asiacrypt 2014", Kaohsiung, Taiwan, Advances in Cryptology - Lecture Notes in Computer Science, Springer, December 2014, vol. 2, n^{o} 8874, pp. 1 - 21 [*DOI :* 10.1007/978-3-662-45608-8_1], https://hal.inria.fr/hal-01088108

[26] B. LIBERT, T. PETERS, M. JOYE, M. YUNG. *Non-Malleability from Malleability: Simulation-Sound Quasi-Adaptive NIZK Proofs and CCA2-Secure Encryption from Homomorphic Signatures*, in "Eurocrypt 2014", Copenhagen, Denmark, P. NGUYEN, E. OSWALD (editors), May 2014, https://hal.inria.fr/hal-00983147

[27] S. LING, D. H. PHAN, D. STEHLÉ, R. STEINFELD. *Hardness of k-LWE and Applications in Traitor Tracing*, in "CRYPTO", Santa Barbara, CA, United States, 2014, https://hal.archives-ouvertes.fr/hal-01091300

[28] N. REVOL. *Latest Developments on the IEEE 1788 Effort for the Standardization of Interval Arithmetic*, in "ICVRAM & ISUMA - Second International Conference on Vulnerability and Risk Analysis and Management & Sixth International Symposium on Uncertainty Modelling and Analysis", Liverpool, United Kingdom, ASCE: American Society of Civil Engineers, July 2014, pp. 1-10, (Standardization effort supported by the Inria D2T.), https://hal.inria.fr/hal-00920662

[29] R. SERRA, D. ARZELIER, M. JOLDES, J.-B. LASSERRE, A. RONDEPIERRE, B. SALVY. *A New Method to Compute the Probability of Collision for Short-term Space Encounters*, in "AIAA/AAS Astrodynamics Specialist Conference", San Diego, United States, August 2014 [*DOI :* 10.2514/6.2014-4366], https://hal.inria.fr/hal-01092420

[30] D. STEHLÉ, G. VILLARD, I. MOREL, G. SARUSHI. *LLL reducing with the most significant bits*, in "ISSAC'14 - International symposium on Symbolic and algebraic computation", Kobe, Japan, ACM proceedings, July 2014 [*DOI :* 10.1145/2608628.2608645], https://hal-ens-lyon.archives-ouvertes.fr/ensl-00993445

Scientific Books (or Scientific Book chapters)

[31] F. DE DINECHIN, J.-M. MULLER. *Evaluating Elementary Functions*, in "Princeton Companion to Applied Mathematics", N. HIGHAM (editor), Princeton University Press, 2014, 2 p. , https://hal.inria.fr/ensl-00989001

[32] A. GIL, J.-M. MULLER, J. SEGURA. *Edition d'un numéro spécial "Numerical Software: Design, Analysis and Verification"*, Elsevier, September 2014, vol. 90 part A, 1 p. , https://hal-ens-lyon.archives-ouvertes.fr/ensl-01070771

[33] F. LAGUILLAUMIE, A. LANGLOIS, D. STEHLÉ. *Chiffrement avancé à partir du problème Learning With Errors*, in "Informatique Mathématique : une photographie en 2014", S. PEYRONNET (editor), Presses universitaires de Perpignan, March 2014, https://hal.inria.fr/hal-00984055

Research Reports

[34] C.-P. JEANNEROD, S. M. RUMP. *On relative errors of floating-point operations: optimal bounds and applications*, January 2014, 15 p. , https://hal.inria.fr/hal-00934443

[35] M. JOLDES, O. MARTY, J.-M. MULLER, V. POPESCU. *Arithmetic algorithms for extended precision using floating-point expansions*, LIP - ENS Lyon ; LAAS-CNRS ; ENS Cachan, January 2015, Rapport LAAS n° 15016, https://hal.archives-ouvertes.fr/hal-01111551

Scientific Popularization

[36] J.-M. MULLER, S. BOLDO. *Des ordinateurs capables de calculer plus juste*, in "La Recherche", October 2014, pp. 46-53, https://hal-ens-lyon.archives-ouvertes.fr/ensl-01069744

Other Publications

[37] N. BRISEBARRE, C. LAUTER, M. MEZZAROBBA, J.-M. MULLER. *Comparison between binary and decimal floating-point numbers*, July 2014, https://hal.archives-ouvertes.fr/hal-01021928

[38] M. F. I. CHOWDHURY, C.-P. JEANNEROD, V. NEIGER, E. SCHOST, G. VILLARD. *Faster Algorithms for Multivariate Interpolation with Multiplicities and Simultaneous Polynomial Approximations*, February 2014, https://hal.inria.fr/hal-00941435

[39] J.-G. DUMAS, T. GAUTIER, C. PERNET, J.-L. ROCH, Z. SULTAN. *Recursion based parallelization of exact dense linear algebra routines for Gaussian elimination*, November 2014, https://hal.archives-ouvertes.fr/hal-01084238

[40] J.-G. DUMAS, C. PERNET, Z. SULTAN. *Computing the Rank Profile Matrix* *, January 2015, https://hal.archives-ouvertes.fr/hal-01107722

[41] C.-P. JEANNEROD. *A rounding error analysis of the Cornea-Harrison-Tang method in radix β*, July 2014, Preprint submitted on April 5, 2014 and revised on July 15, 2014, https://hal.inria.fr/hal-01050021

[42] C.-P. JEANNEROD, P. KORNERUP, N. LOUVET, J.-M. MULLER. *Error bounds on complex floating-point multiplication with an FMA*, July 2014, https://hal.inria.fr/hal-00867040