RESEARCH CENTRE

Inria Lyon Centre

IN PARTNERSHIP WITH:

CNRS, Université Claude Bernard (Lyon 1), Ecole normale supérieure de Lyon

2024

ACTIVITY REPORT

Project-Team

ARIC

Arithmetic and Computing

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

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Algorithmics, Computer Algebra and Cryptology

Inria

Contents

Project-Team ARIC 1

1 Team members, visitors, external collaborators 2

2 Overall objectives 3

3 Research program 3
3.1 Efficient and certified approximation methods . . . 3
3.1.1 Safe numerical approximations . . . 3
3.1.2 Floating-point computing . . . 4
3.2 Lattices: algorithms and cryptology . . . 4
3.2.1 Hardness foundations . . . 4
3.2.2 Cryptanalysis . . . 5
3.2.3 Advanced cryptographic primitives . . . 5
3.3 Algebraic computing and high performance kernels . . . 5

4 Application domains 6
4.1 Floating-point and Validated Numerics . . . 6
4.2 Cryptography, Cryptology, Communication Theory . . . 6

5 Highlights of the year 6
5.1 Awards . . . 6

6 New software, platforms, open data 6
6.1 New software . . . 6
6.1.1 FPLLL . . . 6
6.1.2 Gfun . . . 7
6.1.3 GNU-MPFR . . . 7
6.1.4 MPFI . . . 7

7 New results 8
7.1 Efficient approximation methods . . . 8
7.1.1 Efficient and Validated Numerical Evaluation of Abelian Integrals . . . 8
7.1.2 A path-norm toolkit for modern networks: consequences, promises and challenges 8
7.1.3 Path-metrics, pruning, and generalization . . . 8
7.1.4 Fast inference with Kronecker-sparse matrices . . . 8
7.1.5 Fast and reliable computation of the instantaneous orbital collision probability . . . 9
7.1.6 An Exchange Algorithm for Optimizing both Approximation and Finite-Precision Evaluation Errors in Polynomial Approximations . . . 9
7.2 Floating-point and Validated Numerics . . . 9
7.2.1 Useful applications of correctly-rounded operators of the form ab + cd + e . . . 9
7.2.2 Towards a correctly-rounded and fast power function in binary64 arithmetic, with formal proofs . . . 9
7.2.3 Error in ulps of the multiplication or division by a correctly-rounded function or constant in binary floating-point arithmetic . . . 10
7.2.4 Correctly-rounded evaluation of a function: why, how, and at what cost? . . . 10
7.2.5 An Emacs-Cairo scrolling bug due to floating-point inaccuracy . . . 10
7.3 Cryptography . . . 10
7.3.1 Quantum Oblivious LWE Sampling and Insecurity of Standard Model Lattice-Based SNARKs . . . 10
7.3.2 Fast Public-Key Silent OT and More from Constrained Naor-Reingold . . . 10
7.3.3 HAETAE: Shorter Lattice-Based Fiat-Shamir Signatures . . . 11
7.4 Algebraic Computing and High-performance Kernels . . . 11
7.4.1 Minimization of differential equations and algebraic values of E-functions . . . 11
7.4.2 Reduction-Based Creative Telescoping for Definite Summation of D-Finite Functions 11

7.4.3 Positivity certificates for linear recurrences . . . 11
7.4.4 Faster modular composition . . . 12
7.4.5 Explicit maximal totally real embeddings . . . 12
7.4.6 High-order lifting for polynomial Sylvester matrices . . . 12
7.4.7 Elimination ideal and bivariate resultant over finite fields . . . 12
7.4.8 Computing Krylov iterates in the time of matrix multiplication . . . 13

8 Bilateral contracts and grants with industry **13**
8.1 Bilateral contracts with industry . . . 13

9 Partnerships and cooperations **13**
9.1 International initiatives . . . 13
9.1.1 Inria associate team not involved in an IIL or an international program . . . 13
9.2 National initiatives . . . 14
9.2.1 ANR NuSCAP Project . . . 14

10 Dissemination **14**
10.1 Promoting scientific activities . . . 14
10.1.1 Scientific events: organisation . . . 14
10.1.2 Members of editorial boards . . . 14
10.1.3 Seminars and Workshops . . . 14
10.1.4 Scientific expertise . . . 15
10.1.5 Research administration . . . 15
10.2 Teaching - Supervision - Juries . . . 15
10.2.1 Teaching . . . 15
10.2.2 Juries . . . 16
10.3 Popularization . . . 16
10.3.1 Specific official responsibilities in science outreach structures . . . 16
10.3.2 Participation in Live events . . . 16
10.3.3 Others science outreach relevant activities . . . 17

11 Scientific production **17**
11.1 Publications of the year . . . 17

Project-Team ARIC

Creation of the Project-Team: 2013 January 01

Keywords

Computer sciences and digital sciences

A2.4. – Formal method for verification, reliability, certification

A4.3. – Cryptography

A7.1. – Algorithms

A8. – Mathematics of computing

A8.1. – Discrete mathematics, combinatorics

A8.4. – Computer Algebra

A8.5. – Number theory

A8.10. – Computer arithmetic

Other research topics and application domains

B6.6. – Embedded systems

B9.5. – Sciences

B9.10. – Privacy

1 Team members, visitors, external collaborators

Research Scientists

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

Faculty Member

- Nicolas Louvet [UNIV LYON I, Associate Professor]

PhD Students

- Calvin Abou Haidar [INRIA, until Jan 2024]
- Pouria Fallahpour [ENS DE LYON, until Aug 2024]
- Joel Felderhoff [INRIA]
- Louis Gaillard [ENS DE LYON, from Sep 2024]
- Antoine Gonon [ENS DE LYON, until Nov 2024]
- Tom Hubrecht [ENS DE LYON, from Sep 2024]
- Alaa Ibrahim [INRIA]
- Mahshid Riahinia [ENS DE LYON, until Sep 2024]

Technical Staff

- Joris Picot [ENS DE LYON, Engineer]

Interns and Apprentices

- Tom Hubrecht [ENS PARIS-SACLAY, until Mar 2024]
- Hugo Passe [ENS DE LYON, Intern, from Feb 2024 until Jul 2024]

Administrative Assistant

- Chiraz Benamor [ENS DE LYON]

2 Overall objectives

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

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

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

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

- **Efficient approximation methods (§3.1).** Here lies the question of interleaving formal proofs, computer arithmetic and computer algebra, for significantly extending the range of functions whose reliable evaluation can be optimized.
- **Lattices: algorithms and cryptography (§3.2).** Long term goals are to go beyond the current design paradigm in basis reduction, and to demonstrate the superiority of lattice-based cryptography over contemporary public-key cryptographic approaches.
- **Algebraic computing and high performance kernels (§3.3).** The problem is to keep the algorithm and software designs in line with the scales of computational capabilities and application needs, by simultaneously working on the structural and the computer arithmetic levels.

3 Research program

3.1 Efficient and certified approximation methods

3.1.1 Safe numerical approximations

The last twenty years have seen the advent of computer-aided proofs in mathematics and this trend is getting more and more important. They request: fast and stable numerical computations; numerical results with a guarantee on the error; formal proofs of these computations or computations with a proof assistant. One of our main long-term objectives is to develop a platform where one can study a computational problem on all (or any) of these three levels of rigor. At this stage, most of the necessary

routines are not easily available (or do not even exist) and one needs to develop *ad hoc* tools to complete the proof. We plan to provide more and more algorithms and routines to address such questions. Possible applications lie in the study of mathematical conjectures where exact mathematical results are required (e.g., stability of dynamical systems); or in more applied questions, such as the automatic generation of efficient and reliable numerical software for function evaluation. On a complementary viewpoint, numerical safety is also critical in robust space mission design, where guidance and control algorithms become more complex in the context of increased satellite autonomy. We will pursue our collaboration with specialists of that area whose questions bring us interesting focus on relevant issues.

3.1.2 Floating-point computing

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

Floating-point algorithms, properties, and standardization One of our targets is the design of building blocks of computing (e.g., algorithms for the basic operations and functions, and algorithms for complex or double-word arithmetic). Establishing properties of these building blocks (e.g., the absence of "spurious" underflows/overflows) is also important. The IEEE 754 standard on floating-point arithmetic (which has been revised slightly in 2019) will have to undergo a major revision within a few years: first because advances in technology or new needs make some of its features obsolete, and because new features need standardization. We aim at playing a leading role in the preparation of the next standard.

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

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

3.2 Lattices: algorithms and cryptology

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

3.2.1 Hardness foundations

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

of standard ones) from which we could derive much more efficient constructions. Furthermore, it could open the way to completely different constructions of advanced primitives based on new hardness assumptions.

3.2.2 Cryptanalysis

Lattice-based cryptography has come much closer to maturity in the recent past. In particular, NIST has started a standardization process for post-quantum cryptography, and lattice-based proposals are numerous and competitive. This dramatically increases the need for cryptanalysis:

Do the underlying hard problems suffer from structural weaknesses? Are some of the problems used easy to solve, e.g., asymptotically?

Are the chosen concrete parameters meaningful for concrete cryptanalysis? In particular, how secure would they be if all the known algorithms and implementations thereof were pushed to their limits? How would these concrete performances change in case (full-fledged) quantum computers get built?

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

3.2.3 Advanced cryptographic primitives

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

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

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

3.3 Algebraic computing and high performance kernels

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

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

4 Application domains

4.1 Floating-point and Validated Numerics

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

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

Much of our work, in particular the development of correctly rounded elementary functions, is critical to the reproducibility of floating-point computations.

4.2 Cryptography, Cryptology, Communication Theory

Lattice reduction algorithms have direct applications in

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

5 Highlights of the year

5.1 Awards

- Best paper award at ARITH 2024 for the paper *Useful applications of correctly-rounded operators of the form ab + cd + e* by Tom Hubrecht, Claude-Pierre Jeannerod, and Jean-Michel Muller [14].
- Best paper award at ISSAC 2024 for the article *Computing Krylov iterates in the time of matrix multiplication* by Vincent Neiger, Clément Pernet and Gilles Villard [17].

6 New software, platforms, open data

6.1 New software

6.1.1 FPLLL

Keywords: Euclidean Lattices, Computer algebra system (CAS), Cryptography

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

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

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

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

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

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

Contact: Damien Stehlé

6.1.2 Gfun

Name: generating functions package

Keyword: Symbolic computation

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

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

Contact: Bruno Salvy

6.1.3 GNU-MPFR

Functional Description: GNU MPFR is an efficient arbitrary-precision floating-point library with well-defined semantics (copying the good ideas from the IEEE 754 standard), in particular correct rounding in 5 rounding modes. It provides about 100 mathematical functions, in addition to utility functions (assignments, conversions...). Special data (Not a Number, infinities, signed zeros) are handled like in the IEEE 754 standard. GNU MPFR is based on the mpn and mpz layers of the GMP library.

URL: https://www.mpfr.org/

Publications: hal-01394289, hal-01502326, inria-00069930, inria-00070174, inria-00103655, inria-00000026

Contact: Vincent Lefèvre

Participants: Guillaume Hanrot, Paul Zimmermann, Philippe Theveny, Vincent Lefèvre

6.1.4 MPFI

Name: Multiple Precision Floating-point Interval

Keyword: Arithmetic

Functional Description: MPFI is a C library based on MPFR and GMP for arbitrary precision interval arithmetic.

Release Contributions: Updated for the autoconf installation. New functions added: rev_sqrt, exp10, exp2m1, exp10m1, log2p1, log10p1.

URL: https://gitlab.inria.fr/mpfi/mpfi

Contact: Nathalie Revol

7 New results

Participants: Calvin Abou Haidar, Nicolas Brisebarre, Pouria Fallahpour, Joel Felderhoff, Louis Gaillard, Antoine Gonon, Tom Hubrecht, Alaa Ibrahim, Claude-Pierre Jeannerod, Vincent Lefèvre, Nicolas Louvet, Jean-Michel Muller, Joris Picot, Nathalie Revol, Mahshid Riahinia, Bruno Salvy, Gilles Villard.

7.1 Efficient approximation methods

7.1.1 Efficient and Validated Numerical Evaluation of Abelian Integrals

Abelian integrals play a key role in the infinitesimal version of Hilbert's 16th problem. Being able to evaluate such integrals - with guaranteed error bounds - is a fundamental step in computer-aided proofs aimed at this problem. Using interpolation by trigonometric polynomials and quasi-Newton-Kantorovitch validation, we develop a validated numerics method for computing Abelian integrals in a quasi-linear number of arithmetic operations. Our approach is both effective, as exemplified on two practical perturbed integrable systems, and amenable to an implementation in a formal proof assistant, which is key to provide fully reliable computer-aided proofs [2].

7.1.2 A path-norm toolkit for modern networks: consequences, promises and challenges

This work introduces the first toolkit around path-norms that is fully able to encompass general DAG ReLU networks with biases, skip connections and any operation based on the extraction of order statistics: max pooling, GroupSort etc. This toolkit notably allows us to establish generalization bounds for modern neural networks that are not only the most widely applicable path-norm based ones, but also recover or beat the sharpest known bounds of this type. These extended path-norms further enjoy the usual benefits of path-norms: ease of computation, invariance under the symmetries of the network, and improved sharpness on feedforward networks compared to the product of operators' norms, another complexity measure most commonly used. The versatility of the toolkit and its ease of implementation allow us to challenge the concrete promises of path-norm-based generalization bounds, by numerically evaluating the sharpest known bounds for ResNets on ImageNet [13].

7.1.3 Path-metrics, pruning, and generalization

Analyzing the behavior of ReLU neural networks often hinges on understanding the relationships between their parameters and the functions they implement. This paper proves a new bound on function distances in terms of the so-called path-metrics of the parameters. Since this bound is intrinsically invariant with respect to the rescaling symmetries of the networks, it sharpens previously known bounds. It is also, to the best of our knowledge, the first bound of its kind that is broadly applicable to modern networks such as ResNets, VGGs, U-nets, and many more. In contexts such as network pruning and quantization, the proposed path-metrics can be efficiently computed using only two forward passes. Besides its intrinsic theoretical interest, the bound yields not only novel theoretical generalization bounds, but also a promising proof of concept for rescaling-invariant pruning [25].

7.1.4 Fast inference with Kronecker-sparse matrices

This paper benchmarks and improves existing GPU matrix multiplication algorithms specialized for Kronecker-sparse matrices, whose sparsity patterns are described by Kronecker products. These matrices have recently gained popularity as replacements for dense matrices in neural networks because they preserve accuracy while using fewer parameters. We present the first energy and time benchmarks for the multiplication with such matrices, helping users identify scenarios where Kronecker-sparse matrices are more time- and energy-efficient than their dense counterparts. Our benchmark also reveals that specialized implementations spend up to 50% of their total runtime on memory rewriting operations. To address the challenge of reducing memory transfers, we introduce a new so-called tiling strategy adapted

to the Kronecker-sparsity structure, which reduces reads and writes between levels of GPU memory. We implement this tiling strategy in a new CUDA kernel that achieves a median speed-up of x1.4, while also cutting energy consumption by 15%. We further demonstrate the broader impact of our results by applying the new kernel to accelerate transformer inference [26].

7.1.5 Fast and reliable computation of the instantaneous orbital collision probability

Due to the increasing number of objects in Low Earth orbit, the fast and reliable estimation of the collision risk is an important challenge for spacecraft owners/operators. Among the available risk indicators, we focus on computing the instantaneous probability of collision, which can be modeled as the integral of a three-dimensional Gaussian probability density function over a Euclidean ball. We propose an efficient and accurate method for evaluating this integral. It is based on the combination of two complementary strategies. For the first one, convergent series and numerical error bounds are computed. These bounds provide a tradeoff between the accuracy needed and the number of terms to compute. The second one, using divergent series, approximates the value of the integral with a good accuracy in most cases with only a few terms computed. Based on those two methods, a hybrid algorithm is tested on cases borrowed from the literature and compared against existing methods. Several numerical results and comparisons confirm both the efficiency and robustness of our approach [5].

7.1.6 An Exchange Algorithm for Optimizing both Approximation and Finite-Precision Evaluation Errors in Polynomial Approximations

The finite precision implementation of mathematical functions frequently depends on polynomial approximations. A key characteristic of this approach is that rounding errors occur both when representing the coefficients of the polynomial on a finite number of bits, and when evaluating it in finite precision arithmetic. Hence, to find a best polynomial, for a given fixed degree, norm and interval, it is necessary to account for both the approximation error and the floating-point evaluation error. While efficient algorithms were already developed for taking into account the approximation error, the evaluation part is usually a posteriori handled, in an ad-hoc manner. Here, we formulate a semi-infinite linear optimization problem whose solution is a best polynomial with respect to the supremum norm of the sum of both errors. This problem is then solved with an iterative exchange algorithm, which can be seen as an extension of the well-known Remez exchange algorithm. An open-source C implementation using the Sollya library is presented and tested on several examples, which are then analyzed and compared against state-of-the-art Sollya routines [23].

7.2 Floating-point and Validated Numerics

7.2.1 Useful applications of correctly-rounded operators of the form ab + cd + e

We show that the availability of fused arithmetic operators that evaluate expressions of the form $ab+cd$ (FD2 instruction) or $ab+cd+e$ (FD2A instruction) in floating-point arithmetic with one final rounding only would significantly facilitate many calculations that are hard to perform with high accuracy at small cost using only the traditional operations $+$, $-$, $\times$, $\div$, $\sqrt{}$, and fused multiply-add (FMA) [14].

7.2.2 Towards a correctly-rounded and fast power function in binary64 arithmetic, with formal proofs

We design algorithms for the correct rounding of the power function x^y in the binary64 IEEE 754 format, for all rounding modes, modulo the knowledge of hardest-to-round cases. Our implementation of these algorithms largely outperforms previous correctly-rounded implementations and is not far from the efficiency of current mathematical libraries, which are not correctly-rounded. Still, we expect our algorithms can be further improved for speed. The proofs of correctness are fully detailed and have been formally verified. We hope this work will motivate the next IEEE 754 revision committee to require correct rounding for mathematical functions [27].

7.2.3 Error in ulps of the multiplication or division by a correctly-rounded function or constant in binary floating-point arithmetic

Assume we use a binary floating-point arithmetic and that RN is the round-to-nearest function. Also assume that c is a constant or a real function of one or more variables, and that we have at our disposal a correctly rounded implementation of c, say $\hat{c} = \mathrm{RN}(c)$. For evaluating $x \cdot c$ (resp. x/c or c/x), the natural way is to replace it by $\mathrm{RN}(x \cdot \hat{c})$ (resp. $\mathrm{RN}(x/\hat{c})$ or $\mathrm{RN}(\hat{c}/x)$), that is, to call function $\hat{c}$ and to perform a floating-point multiplication or division. This can be generalized to the approximation of n/d by $\mathrm{RN}(\hat{n}/\hat{d})$ and the approximation of $n \cdot d$ by $\mathrm{RN}(\hat{n} \cdot \hat{d})$, where $\hat{n} = \mathrm{RN}(n)$ and $\hat{d} = \mathrm{RN}(d)$, and n and d are functions for which we have at our disposal a correctly rounded implementation. We discuss tight error bounds in ulps of such approximations. From our results, one immediately obtains tight error bounds for calculations such as `x*pi`, `ln(2)/x`, `x/(y+z)`, `(x+y)*z`, `x/sqrt(y)`, `sqrt(x)/y`, `(x+y)(z+t)`, `(x+y)/(z+t)`, `(x+y)/(zt)`, etc. in floating-point arithmetic [3].

7.2.4 Correctly-rounded evaluation of a function: why, how, and at what cost?

The goal of this paper is to give a survey on the various computational and mathematical issues and progress related to the problem of providing efficient correctly-rounded elementary functions in floating-point arithmetic. We also aim at convincing the reader that a future standard for floating-point arithmetic should require the availability of a correctly-rounded version of a well-chosen core set of elementary functions. We discuss the interest and feasibility of this requirement. We also give answers to common objections we have received over the last 10 years [24].

7.2.5 An Emacs-Cairo scrolling bug due to floating-point inaccuracy

We study a bug that we found in the GNU Emacs text editor when built against the Cairo graphics library. We analyze both the Emacs code and the Cairo code, and we suggest what can be done to avoid unexpected results. This involves a particular case with a computation that can be reduced to the equivalent floating-point expression $((1/s) \cdot b) \cdot s$, where s and b are small positive integers such that $b < s$ and the basic operations are rounded to nearest. The analysis takes into account the values of s and b that can occur in practice, and the suggestions for workarounds must avoid handling this particular case in a separate branch or breaking the structure of the Cairo library (so that just returning b is not possible)[16].

7.3 Cryptography

7.3.1 Quantum Oblivious LWE Sampling and Insecurity of Standard Model Lattice-Based SNARKs

The Learning With Errors (LWE) problem asks to find s from an input of the form $(A, b = As + e) \in (\mathbb{Z}/q\mathbb{Z})^{m \times n} \times (\mathbb{Z}/q\mathbb{Z})^m$, for a vector e that has small-magnitude entries. In this work, we do not focus on solving LWE but on the task of sampling instances. As these are extremely sparse in their range, it may seem plausible that the only way to proceed is to first create s and e and then set $b = As + e$. In particular, such an instance sampler knows the solution. This raises the question whether it is possible to obliviously sample $(A, As + e)$, namely, without knowing the underlying s. A variant of the assumption that oblivious LWE sampling is hard has been used in a series of works to analyze the security of candidate constructions of Succinct Non-interactive Arguments of Knowledge (SNARKs). As the assumption is related to LWE, these SNARKs have been conjectured to be secure in the presence of quantum adversaries. Our main result is a quantum polynomial-time algorithm that samples well-distributed LWE instances while provably not knowing the solution, under the assumption that LWE is hard. Moreover, the approach works for a vast range of LWE parametrizations, including those used in the above-mentioned SNARKs. This invalidates the assumptions used in their security analyses, although it does not yield attacks against the constructions themselves.[12]

7.3.2 Fast Public-Key Silent OT and More from Constrained Naor-Reingold

Pseudorandom Correlation Functions (PCFs) allow two parties, given correlated evaluation keys, to locally generate arbitrarily many pseudorandom correlated strings, e.g. Oblivious Transfer (OT) correlations, which can then be used by the two parties to jointly run secure computation protocols. In this work, we

provide a novel and simple approach for constructing PCFs for OT correlation, by relying on constrained pseudorandom functions for a class of constraints containing a weak pseudorandom function (wPRF). We then show that tweaking the Naor-Reingold pseudorandom function and relying on low-complexity pseudorandom functions allow us to instantiate our paradigm. We further extend our ideas to obtain efficient public-key PCFs, which allow the distribution of correlated keys between parties to be non-interactive: each party can generate a pair of public/secret keys, and any pair of parties can locally derive their correlated evaluation key by combining their secret key with the other party's public key. In addition to these theoretical contributions, we detail various optimizations and provide concrete instantiations of our paradigm relying on the Boneh-Ishai-Passelègue-Sahai-Wu wPRF and the Goldreich-Applebaum-Raykov wPRF. Putting everything together, we obtain public-key PCFs with a throughput of 15k-40k OT/s, which is of a similar order of magnitude to the state-of-the-art interactive PCFs and about 4 orders of magnitude faster than state-of-the-art public-key PCFs. As a side result, we also show that public-key PCFs can serve as a building block to construct reusable designated-verifier non-interactive zero-knowledge proofs (DV-NIZK) for NP. Combined with our instantiations, this yields simple and efficient reusable DV-NIZKs for NP in pairing-free groups. [10]

7.3.3 HAETAE: Shorter Lattice-Based Fiat-Shamir Signatures

We present HAETAE (Hyperball bimodAl modulE rejecTion signAture schemE), a new lattice-based signature scheme. Like the NIST-selected Dilithium signature scheme, HAETAE is based on the Fiat-Shamir with Aborts paradigm, but our design choices target an improved complexity/compactness compromise that is highly relevant for many space-limited application scenarios. We primarily focus on reducing signature and verification key sizes so that signatures fit into one TCP or UDP datagram while preserving a high level of security against a variety of attacks. As a result, our scheme has signature and verification key sizes up to 39% and 25% smaller, respectively, compared than Dilithium. We provide a portable, constanttime reference implementation together with an optimized implementation using AVX2 instructions and an implementation with reduced stack size for the Cortex-M4. Moreover, we describe how to efficiently protect HAETAE against implementation attacks such as side-channel analysis, making it an attractive candidate for use in IoT and other embedded systems. [11]

7.4 Algebraic Computing and High-performance Kernels

7.4.1 Minimization of differential equations and algebraic values of E-functions

A power series being given as the solution of a linear differential equation with appropriate initial conditions, minimization consists in finding a non-trivial linear differential equation of minimal order having this power series as a solution. This problem exists in both homogeneous and inhomogeneous variants; it is distinct from, but related to, the classical problem of factorization of differential operators. Recently, minimization has found applications in Transcendental Number Theory, more specifically in the computation of non-zero algebraic points where Siegel's E-functions take algebraic values. We present algorithms for these questions and discuss implementation and experiments [1].

7.4.2 Reduction-Based Creative Telescoping for Definite Summation of D-Finite Functions

Creative telescoping is an algorithmic method initiated by Zeilberger to compute definite sums by synthesizing summands that telescope, called certificates. We describe a creative telescoping algorithm that computes telescopers for definite sums of D-finite functions as well as the associated certificates in a compact form. The algorithm relies on a discrete analogue of the generalized Hermite reduction, or equivalently, a generalization of the Abramov-Petkovšek reduction. We provide a Maple implementation with good timings on a variety of examples [4].

7.4.3 Positivity certificates for linear recurrences

We show that for solutions of linear recurrences with polynomial coefficients of Poincaré type and with a unique simple dominant eigenvalue, positivity reduces to deciding the genericity of initial conditions in a precisely defined way. We give an algorithm that produces a certificate of positivity that is a data-structure

for a proof by induction. This induction works by showing that an explicitly computed cone is contracted by the iteration of the recurrence [15].

7.4.4 Faster modular composition

A new Las Vegas algorithm is presented for the composition of two polynomials modulo a third one, over an arbitrary field. When the degrees of these polynomials are bounded by n, the algorithm uses $O(n^{1.43})$ field operations, breaking through the 3/2 barrier in the exponent for the first time. The previous fastest algebraic algorithms, due to Brent and Kung in 1978, require $O(n^{1.63})$ field operations in general, and $n^{3/2+o(1)}$ field operations in the particular case of power series over a field of large enough characteristic. If using cubic-time matrix multiplication, the new algorithm runs in $n^{5/3+o(1)}$ operations, while previous ones run in $O(n^2)$ operations. Our approach relies on the computation of a matrix of algebraic relations that is typically of small size. Randomization is used to reduce arbitrary input to this favorable situation [6].

7.4.5 Explicit maximal totally real embeddings

An explicit canonical construction is given for a maximal totally real embedding for real analytic manifolds equipped with a covariant derivative operator acting on the real analytic sections of its tangent bundle or of its complexified tangent bundle. The existence of maximal totally real embeddings for real analytic manifolds is known from previous celebrated works by Bruhat-Whitney and Grauert. Their construction is based on the use of analytic continuation of local frames and local coordinates that are far from being canonical or explicit. As a consequence, the form of the corresponding complex structure has been a mystery since the very beginning. A quite simple recursive expression for such complex structures has been provided in Pali's work "On maximal totally real embeddings". In our series of articles we focus on the case of torsion free connections. In the present article we give a fiberwise Taylor expansion of the canonical complex structure which is expressed in terms of symmetrization of curvature monomials and a rather simple and explicit expression of the coefficients of the expansion. We explain also a rather simple geometric characterization of such canonical complex structures. Our main result and argument can be useful for the study of open questions in the theory of the embeddings in consideration such as their moduli space [7].

7.4.6 High-order lifting for polynomial Sylvester matrices

A new algorithm is presented for computing the resultant of two "sufficiently generic" bivariate polynomials over an arbitrary field. For such p and q in $\mathsf{K}[x,y]$ of degree d in x and n in y, the resultant with respect to y is computed using $O(n^{1.458}d)$ arithmetic operations as long as $d = O(n^{1/3})$. For $d = 1$, the complexity estimate is therefore essentially reconciled with the best known estimates of [6] for the related problems of modular composition and characteristic polynomial in a univariate quotient algebra. This allows to cross the 3/2 barrier in the exponent of n for the first time in the case of the resultant. More generally, our algorithm improves on best previous algebraic ones as long as $d = O(n^{0.47})$ [8].

7.4.7 Elimination ideal and bivariate resultant over finite fields

Given two polynomials a and b in $\mathbb{F}_q[x,y]$ which have no non-trivial common divisors, we prove that a generator of the elimination ideal $\langle a,b\rangle \cap \mathbb{F}_q[x]$ can be computed in quasi-linear time. To achieve this, we propose a randomized algorithm of the Monte Carlo type which requires $(de\log q)^{1+o(1)}$ bit operations, where d and e bound the input degrees in x and in y respectively.

The same complexity estimate applies to the computation of the largest degree invariant factor of the Sylvester matrix associated with a and b (with respect to either x or y), and of the resultant of a and b if they are sufficiently generic, in particular such that the Sylvester matrix has a unique non-trivial invariant factor.

Our approach is to exploit reductions to problems of minimal polynomials in quotient algebras of the form $\mathbb{F}_q[x,y]/\langle a,b\rangle$. By proposing a new method based on structured polynomial matrix division for computing with the elements of the quotient, we succeed in improving the best-known complexity bounds [9].

7.4.8 Computing Krylov iterates in the time of matrix multiplication

Krylov methods rely on iterated matrix-vector products $A^k u_j$ for an $n \times n$ matrix A and vectors $u_1, \ldots, u_m$. The space spanned by all iterates $A^k u_j$ admits a particular basis — the *maximal Krylov basis* — which consists of iterates of the first vector $u_1, Au_1, A^2u_1, \ldots$, until reaching linear dependency, then iterating similarly the subsequent vectors until a basis is obtained. Finding minimal polynomials and Frobenius normal forms is closely related to computing maximal Krylov bases. The fastest way to produce these bases was, until this paper, Keller-Gehrig's 1985 algorithm whose complexity bound $O(n^\omega \log n)$ comes from repeated squarings of A and logarithmically many Gaussian eliminations. Here $\omega > 2$ is a feasible exponent for matrix multiplication over the base field. We present an algorithm computing the maximal Krylov basis in $O(n^\omega \log\log n)$ field operations when $m \in O(n)$, and even $O(n^\omega)$ as soon as $m \in O(n/\log(n)^c)$ for some fixed real $c > 0$. As a consequence, we show that the Frobenius normal form together with a transformation matrix can be computed deterministically in $O(n^\omega (\log\log n)^2)$, and therefore matrix exponentiation A^k can be performed in the latter complexity if $\log k \in O(n^{\omega-1-\varepsilon})$ for some fixed $\varepsilon > 0$. A key idea for these improvements is to rely on fast algorithms for $m \times m$ polynomial matrices of average degree n/m, involving high-order lifting and minimal kernel bases [17].

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

Bosch (Stuttgart) ordered from us two studies:

- (in collaboration with the Emeraude team) some support for the design and implementation of accurate functions in binary32 floating-point arithmetic (exponential and sigmoid functions) and the emulation of binary64 floating-point arithmetic;
- (in collaboration with the Avalon team) some advice on the implementation of numerics in the cloud, both from a performance point of view (Avalon) and from a numerical reliability point of view (AriC).

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

9 Partnerships and cooperations

9.1 International initiatives

9.1.1 Inria associate team not involved in an IIL or an international program

Symbolic

Title: Symbolic matrices and polynomials and their application in combinatorics: new trends in complexity, algorithms and software

Duration: 2022-2024

Coordinator: Éric Schost (eschost@uwaterloo.ca)

Partners:

- University of Waterloo Waterloo (Canada)

Inria contact: Gilles Villard

Summary: The Symbolic Computation Group (U. Waterloo) and the AriC project team (ENS de Lyon) will expand already established collaborations, in order to design and implement algorithms for linear and non-linear symbolic algebra.

9.2 National initiatives

9.2.1 ANR NuSCAP Project

Participants: Nicolas Brisebarre, Jean-Michel Muller, Joris Picot, Bruno Salvy.

NuSCAP (Numerical Safety for Computer-Aided Proofs) is a four-year project started in February 2021. See the web page of the project. It is headed by Nicolas Brisebarre and, besides AriC, involves people from LIP lab, Galinette, Lfant, Stamp and Toccata INRIA teams, LAAS (Toulouse), LIP6 (Sorbonne Université), LIPN (Univ. Sorbonne Paris Nord) and LIX (École Polytechnique). Its goal is to develop theorems, algorithms and software, that will allow one to study a computational problem on all (or any) of the desired levels of numerical rigor, from fast and stable computations to formal proofs of the computations.

10 Dissemination

Participants: Nicolas Brisebarre, Claude-Pierre Jeannerod, Vincent Lefèvre, Nicolas Louvet, Jean-Michel Muller, Nathalie Revol, Bruno Salvy, Gilles Villard.

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

- Bruno Salvy has been chair of the steering committee of the conference AofA for several years until June 2024.

10.1.2 Members of editorial boards

- Jean-Michel Muller is Associate Editor in Chief of the journal IEEE Transactions on Emerging Topics in Computing.
- Nathalie Revol is Associate Editor of the journal IEEE Transactions on Computers.
- Bruno Salvy is a member of the editorial board of the *Journal of Symbolic Computation*, of *Annals of Combinatorics*, and of the collection *Texts and Monographs in Symbolic Computation* (Springer).

10.1.3 Seminars and Workshops

- Nicolas Brisebarre gave an invited talk at the workshop Computer-assisted proofs in nonlinear analysis, Montréal, Canada, 9-13/9/2024.
- Nathalie Revol has given a scientific talk to the Canari team in Bordeaux and a shorter talk for the opening ceremony of this team. She has also given a lecture about interval arithmetic during the winter school Set4MOST (Modelling, Estimation and Control using Set-Based Methods: Theory and Applications).
- Bruno Salvy gave a talk at the workshop 'Functional Equations and Interactions' in Anglet, in the 'Séminaire de Mathématiques accessibles' in St-Étienne, and in the seminar 'Research in Mathematics, Interactions and Applications' in Strasbourg.

10.1.4 Scientific expertise

- Nicolas Brisebarre is a member of the scientific council of "Journées Nationales de Calcul Formel".
- Claude-Pierre Jeannerod is a member of "Comité des Moyens Incitatifs" of the Lyon Inria research center.
- Vincent Lefèvre participated in the revision of the ISO C standard via the C Floating Point Study Group.
- Vincent Lefèvre is an editor for the next revision of the IEEE 754 standard.
- Jean-Michel Muller chaired the evaluation committee of the CRIStAL Laboratory (UMR 9189, Lille, oct. 2024).
- Jean-Michel Muller was a member of the jury for a full professor recruitment et ENS de Lyon (may 2024).
- Nathalie Revol was a member of the Inria hiring committees for junior researchers for Bordeaux, Lyon and Nancy. She reviewed other application files for the Inria's "Commission d'Évaluation".
- Nathalie Revol was a member of the hiring committee for an assistant professor for the University of Nantes.
- Nathalie Revol acted as an expert for the "Jeunes Talents L'Oréal" prize.
- Nathalie Revol acted as an expert for the MSCA postdoctoral fellowships of the European Union.

10.1.5 Research administration

- Nicolas Brisebarre is co-head of GT ARITH (GDR IM).
- Nathalie Revol is member of the board of the GDR Calcul.
- Bruno Salvy was a member of the scientific council of the CIRM until May. He is a member of the scientific council of the GDR IFM.
- Jean-Michel Muller is a member of the steering committee of GDR IFM.

10.2 Teaching - Supervision - Juries

10.2.1 Teaching

Master: Nicolas Brisebarre, Approximation Theory and Proof Assistants: Certified Computations, 15h, M2, ENS de Lyon, France.

Master: Claude-Pierre Jeannerod, Computer Algebra, 30h, M2, ISFA, France.

Master: Vincent Lefèvre, Computer Arithmetic, 10.5h, M2, ISFA, France.

Master: Bruno Salvy and Gilles Villard, Computer Algebra, 20h, M1, ENS de Lyon, France

Master: Bruno Salvy and Gilles Villard, with Alin Bostan, Modern Algorithms in Symbolic Summation and Integration, 32h, M2, ENS de Lyon, France

10.2.2 Juries

- Nicolas Brisebarre was a member of the PhD committees of Antoine Gonon (AriC and Ockham) and Théo Beuzeville (IRIT, Toulouse) for whom he was a reviewer.
- Jean-Michel Muller was member (reviewer) of the Habilitation Committee of Thibault Hilaire (Paris Sorbonne) and of the PhD committee of Morganne Vollmer (Université de Bretagne Occidentale).
- Nathalie Revol was a member of the M2 jury of ENS de Lyon.
- Bruno Salvy was a member of the PhD committees of Calvin Abou Haidar and Joël Felderhoff (AriC), Eric Pichon (Polytechnique); of the Habilitation committees of Édouard Bonnet (Ens Lyon) and Guillaume Moroz (for whom he was a reviewer).

10.3 Popularization

10.3.1 Specific official responsibilities in science outreach structures

- Nathalie Revol is the scientific editor of Interstices. With Joanna Jongwane, they presented Interstices during the JSI (Journées Scientifiques Inria).

10.3.2 Participation in Live events

- Nicolas Brisebarre has been a scientific consultant for “Les maths et moi”, a one-man show by Bruno Martins since 2020. He also takes part to Q & A sessions with the audience after some shows.
- Nathalie Revol took part in the "Binôme" project and was present for the presentation of the result of this project in Avignon (July) and Paris (December).
- Nathalie Revol was present during the festival "Double Science" in Paris, 8-9 June, in particular performing magic tricks related to computer science.
- Claude-Pierre Jeannerod and Nathalie Revol were supervisors of 3 pupils from lycée (2nde) during their 2-week stay, in June.
- Nathalie Revol was in charge of 3 workshops (half a day each - with the help of Simon Delamare) for the complete group of 12 pupils from lycée (2nde), in June.
- Nathalie Revol was in charge of 4 workshops (half a day each - with the help of Simon Delamare) for a group of 6 pupils from collège (3e), in November.
- Nathalie Revol and Joris Picot hosted a group of pupils from Lycée Le Valentin (Bourg-les-Valence) during half a day, in March.
- Nathalie Revol was a member of the animation team for the "Facto" scientific camp in Saint-Paul-en-Jarez in October, for 14 pupils from lycée (2nde).
- Nathalie Revol and Anne Benoit went twice to the primary school Guilloux (Saint-Genis-Laval), during 2 hours, to introduce computer science (programming and robotics) for 2 classes of 9-10 years old pupils, in December.
- Nathalie Revol and Natacha Portier organized the visit and hosted 3 groups of girl pupils in the lab during half a day, for March 8th.
- Nathalie Revol and Natacha Portier were in charge of workshops during the "Journées Filles et Math-Info" at lycée Condorcet of Saint-Priest in February, University Clermont-Ferrand in April and ENS de Lyon in November.
- Nathalie Revol was a panelist during a café about "Femmes et numérique" organized by the association "Regards de Femmes", in May.
- Nathalie Revol and Aude Lemar-Verrier were in charge of a workshop about women in computer science for Agile Lyon, in June.

10.3.3 Others science outreach relevant activities

- Nathalie Revol has taught "Scientific outreach" to 3 groups of 12 to 15 (4th year) students of ENS de Lyon, 12h per group.
- Nathalie Revol and Natacha Portier organized a "Journée Filles et Info-Maths" at ENS de Lyon for 90 girl pupils in November, as an incentive to choose a scientific career.

11 Scientific production

11.1 Publications of the year

International journals

[1] A. Bostan, T. Rivoal and B. Salvy. 'Minimization of differential equations and algebraic values of E-functions'. In: *Mathematics of Computation* 93 (2024), pp. 1427–1472. DOI: 10.1090/mcom/3912. URL: https://hal.science/hal-03771150 (cit. on p. 11).

[2] F. Bréhard, N. Brisebarre, M. Joldeş and W. Tucker. 'Efficient and Validated Numerical Evaluation of Abelian Integrals'. In: *ACM Transactions on Mathematical Software* 50.1 (Mar. 2024), pp. 1–38. DOI: 10.1145/3637550. URL: https://hal.science/hal-03561096 (cit. on p. 8).

[3] N. Brisebarre, J.-M. Muller and J. Picot. 'Error in ulps of the multiplication or division by a correctly-rounded function or constant in binary floating-point arithmetic'. In: *IEEE Transactions on Emerging Topics in Computing* 12.2 (2024), pp. 656–666. DOI: 10.1109/TETC.2023.3294986. URL: https://hal.science/hal-04044716 (cit. on p. 10).

[4] H. Brochet and B. Salvy. 'Reduction-Based Creative Telescoping for Definite Summation of D-Finite Functions'. In: *Journal of Symbolic Computation* 125 (Nov. 2024), p. 102329. DOI: 10.1016/j.jsc.2024.102329. URL: https://hal.science/hal-04295759 (cit. on p. 11).

[5] M. Masson, D. Arzelier, F. Bréhard, M. Joldes and B. Salvy. 'Fast and reliable computation of the instantaneous orbital collision probability'. In: *Journal of Guidance, Control, and Dynamics* (13th May 2024), pp. 1–14. DOI: 10.2514/1.G008102. URL: https://laas.hal.science/hal-04134188 (cit. on p. 9).

[6] V. Neiger, B. Salvy, É. Schost and G. Villard. 'Faster Modular Composition'. In: *Journal of the ACM (JACM)* 71.2 (Apr. 2024), pp. 1–79. DOI: 10.1145/3638349. URL: https://hal.science/hal-03380258 (cit. on p. 12).

[7] N. Pali and B. Salvy. 'Explicit maximal totally real embeddings'. In: *Advances in Mathematics* 459.110031 (Dec. 2024). DOI: 10.1016/j.aim.2024.110031. URL: https://hal.science/hal-04266729 (cit. on p. 12).

[8] C. Pernet, H. Signargout and G. Villard. 'High-order lifting for polynomial Sylvester matrices'. In: *Journal of Complexity* 80 (Feb. 2024), p. 101803. DOI: 10.1016/j.jco.2023.101803. URL: https://hal.science/hal-03740320 (cit. on p. 12).

[9] G. Villard. 'Bivariate polynomial reduction and elimination ideal over finite fields'. In: *Journal of Symbolic Computation* 127 (2024), p. 102367. DOI: 10.1016/j.jsc.2024.102367. URL: https://hal.science/hal-04542799. In press (cit. on p. 12).

International peer-reviewed conferences

[10] D. Bui, G. Couteau, P. Meyer, A. Passelègue and M. Riahinia. 'Fast Public-Key Silent OT and More from Constrained Naor-Reingold'. In: EUROCRYPT 2024. Vol. 14656. Lecture Notes in Computer Science. Santa Barbara (CA), France: Springer Nature Switzerland, 29th Apr. 2024, pp. 88–118. DOI: 10.1007/978-3-031-58751-1_4. URL: https://hal.science/hal-04770536 (cit. on p. 11).

[11] J. H. Cheon, H. Choe, J. Devevey, T. Güneysu, D. Hong, M. Krausz, G. Land, M. Möller, D. Stehlé and M. Yi. 'HAETAE: Shorter Lattice-Based Fiat-Shamir Signatures'. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems*. Conference on Cryptographic Hardware and Embedded Systems - CHES2024. Vol. 2024. 3. Halifax, Canada, 18th July 2024, pp. 25–75. DOI: 10.46586/tches.v2024.i3.25-75. URL: https://hal.science/hal-04909666 (cit. on p. 11).

[12] T. Debris-Alazard, P. Fallahpour and D. Stehlé. 'Quantum Oblivious LWE Sampling and Insecurity of Standard Model Lattice-Based SNARKs'. In: STOC 2024 - 56th Annual ACM Symposium on Theory of Computing. Vancouver BC, Canada: ACM, 11th June 2024, pp. 423–434. DOI: 10.1145/3618260.3649766. URL: https://hal.science/hal-04891122 (cit. on p. 10).

[13] A. Gonon, N. Brisebarre, E. Riccietti and R. Gribonval. 'A path-norm toolkit for modern networks: consequences, promises and challenges'. In: *International Conference on Learning Representations*. International Conference on Learning Representations. Wien, Austria, 2024. URL: https://hal.science/hal-04225201 (cit. on p. 8).

[14] T. Hubrecht, C.-P. Jeannerod and J.-M. Muller. 'Useful applications of correctly-rounded operators of the form ab + cd + e'. In: 2024 IEEE 31st Symposium on Computer Arithmetic (ARITH 2024). Vol. 2024 IEEE 31st Symposium on Computer Arithmetic (ARITH). Málaga, Spain, 2024. URL: https://inria.hal.science/hal-04461089 (cit. on pp. 6, 9).

[15] A. Ibrahim and B. Salvy. 'Positivity certificates for linear recurrences'. In: *Proceedings of the Thirty-Fifth Annual ACM-SIAM Symposium on DiscreteAlgorithms (SODA 2024)*. SODA 2024 - ACM-SIAM Symposium on Discrete Algorithms. Alexandria, Virginia, United States: Society for Industrial and Applied Mathematics, 2024, pp. 982–994. DOI: 10.1137/1.9781611977912.37. URL: https://inria.hal.science/hal-04271203 (cit. on p. 12).

[16] V. Lefèvre. 'An Emacs-Cairo Scrolling Bug due to Floating-Point Inaccuracy'. In: 2024 IEEE 31st Symposium on Computer Arithmetic (ARITH). Proceedings of the 2024 IEEE 31st Symposium on Computer Arithmetic (ARITH). Málaga, Spain: IEEE, June 2024, pp. 76–79. DOI: 10.1109/ARITH61463.2024.00022. URL: https://inria.hal.science/hal-04566768 (cit. on p. 10).

[17] V. Neiger, C. Pernet and G. Villard. 'Computing Krylov iterates in the time of matrix multiplication'. In: *Proceedings of the 2024 International Symposium on Symbolic and Algebraic Computation*. ISSAC '24: International Symposium on Symbolic and Algebraic Computation. ISSAC '24. Raleigh, NC, United States: ACM, 16th July 2024, pp. 419–428. DOI: 10.1145/3666000.3669715. URL: https://cnrs.hal.science/hal-04445355 (cit. on pp. 6, 13).

Doctoral dissertations and habilitation theses

[18] C. Abou Haidar. 'Updatable Public Key Encryption in the context of Secure Messaging'. École Normale Supérieure de LYON, 9th Feb. 2024. URL: https://theses.hal.science/tel-04902577.

[19] P. Fallahpour. 'Lattice-based cryptography in a quantum setting : security proofs and attacks'. Ecole normale supérieure de lyon - ENS LYON, 5th July 2024. URL: https://theses.hal.science/tel-04700564.

[20] J. Felderhoff. 'Hardness of Structured Lattices Problems for Post-Quantum Cryptography'. Ecole normale supérieure de lyon - ENS LYON, 26th Nov. 2024. URL: https://hal.science/tel-04842326.

[21] A. Gonon. 'Harnessing symmetries for modern deep learning challenges : a path-lifting perspective'. Ecole normale supérieure de lyon - ENS LYON, 12th Nov. 2024. URL: https://theses.hal.science/tel-04784426.

[22] M. Riahinia. 'Constrained Pseudorandom Functions : New Constructions and Connections with Secure Computation'. Ecole normale supérieure de lyon - ENS LYON, 8th July 2024. URL: https://theses.hal.science/tel-04727070.

Reports & preprints

[23] D. Arzelier, F. Bréhard, T. Hubrecht and M. Joldes. *An Exchange Algorithm for Optimizing both Approximation and Finite-Precision Evaluation Errors in Polynomial Approximations*. Aug. 2024. URL: https://hal.science/hal-04709615 (cit. on p. 9).

[24] N. Brisebarre, G. Hanrot, J.-M. Muller and P. Zimmermann. *Correctly-rounded evaluation of a function: why, how, and at what cost?* 31st May 2024. URL: https://hal.science/hal-04474530 (cit. on p. 10).

[25] A. Gonon, N. Brisebarre, E. Riccietti and R. Gribonval. *A rescaling-invariant Lipschitz bound based on path-metrics for modern ReLU network parameterizations*. 11th Jan. 2025. URL: https://hal.science/hal-04584311 (cit. on p. 8).

[26] A. Gonon, L. Zheng, P. Carrivain and Q.-T. Le. *Fast inference with Kronecker-sparse matrices*. 3rd Nov. 2024. URL: https://hal.science/hal-04584450 (cit. on p. 9).

[27] T. Hubrecht, C.-P. Jeannerod, P. Zimmermann, L. Rideau and L. Théry. *Towards a correctly-rounded and fast power function in binary64 arithmetic*. 8th Feb. 2024. URL: https://inria.hal.science/hal-04159652 (cit. on p. 9).

Software

[28] [SW] A. Gonon, N. Brisebarre, E. Riccietti and R. Gribonval, *Code for reproducible research - A path-norm toolkit for modern networks: consequences, promises and challenges* version 1.0.0, 11th Mar. 2024. LIC: BSD 3-Clause "New" or "Revised" License. HAL: ⟨hal-04498597⟩, URL: https://hal.science/hal-04498597, VCS: https://github.com/agonon/pathnorm_toolkit, SWHID: ⟨swh:1:dir:119d3f903d3b6e0a776bd64c71317331839390d4;origin=https://hal.archives-ouvertes.fr/hal-04498597;visit=swh:1:snp:3b7c23b687511f3d2e4673d222c3ba96195bb004;anchor=swh:1:rel:7c123216ebb2018ea3290cbdb4cf4f4b8ddea964;path=/⟩.