RESEARCH CENTRE

Inria Lyon Centre

IN PARTNERSHIP WITH:

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

2023

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

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]
- Alain Passelègue [INRIA, Researcher, until Aug 2023]
- Nathalie Revol [INRIA, Researcher]
- Gilles Villard [CNRS, Senior Researcher, HDR]

Faculty Members

- Guillaume Hanrot [ENS DE LYON, Professor, until Aug 2023, HDR]
- Nicolas Louvet [UNIV LYON I, Associate Professor]
- Damien Stehlé [ENS DE LYON, Professor, until Mar 2023, HDR]

PhD Students

- Calvi Abou Haidar [INRIA]
- Orel Cosseron [ZAMA SAS, until Aug 2023]
- Julien Devevey [ENS DE LYON, until Sep 2023]
- Pouria Fallahpour [ENS DE LYON]
- Joel Felderhoff [INRIA]
- Alaa Ibrahim [INRIA]
- Mahshid Riahinia [ENS DE LYON]
- Hippolyte Signargout [ENS DE LYON, until Oct 2023]

Technical Staff

- Joris Picot [ENS DE LYON, Engineer]

Interns and Apprentices

- Louis Gaillard [ENS DE LYON, Intern, from Feb 2023 until Jul 2023]
- Tom Hubrecht [ENS PARIS-SACLAY, from Sep 2023]

Administrative Assistant

- Chiraz Benamor [ENS DE LYON]

Visiting Scientist

- Warwick Tucker [Monash University, Australia]

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 2023 for the article 'Towards Machine-Efficient Rational L^∞-Approximations of Mathematical Functions', by Silviu-Ioan Filip and Nicolas Brisebarre [12].

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

Keywords: Multiple-Precision, Floating-point, Correct Rounding

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 Théveny, 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

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 [4].

7.1.2 Towards Machine-Efficient Rational L^∞-Approximations of Mathematical Functions

Software implementations of mathematical functions often use approximations that can be either polynomial or rational in nature. While polynomials are the preferred approximation in most cases, rational approximations are nevertheless an interesting alternative when dealing with functions that have a pronounced "nonpolynomial behavior" (such as poles close to the approximation domain, asymptotes or finite limits at $\pm\infty$). The major challenge is that of computing good rational approximations with machine number coefficients (e.g. floatingpoint or fixed-point) with respect to the supremum norm, a key step in most procedures for evaluating a mathematical function. This is made more complicated by the fact that even when dealing with real-valued coefficients, optimal supremum norm solutions are sometimes difficult to obtain. Here, we introduce flexible and fast algorithms for computing such rational approximations with both real and machine number coefficients. Their effectiveness is explored on several examples [12].

7.1.3 Approximation speed of quantized vs. unquantized ReLU neural networks and beyond

We deal with two complementary questions about approximation properties of ReLU networks. First, we study how the uniform quantization of ReLU networks with real-valued weights impacts their approximation properties. We establish an upper-bound on the minimal number of bits per coordinate needed for uniformly quantized ReLU networks to keep the same polynomial asymptotic approximation speeds as unquantized ones. We also characterize the error of nearest-neighbour uniform quantization of ReLU networks. This is achieved using a new lower-bound on the Lipschitz constant of the map that associates the parameters of ReLU networks to their realization, and an upper-bound generalizing classical results. Second, we investigate when ReLU networks can be expected, or not, to have better approximation properties than other classical approximation families. Indeed, several approximation families share the following common limitation: their polynomial asymptotic approximation speed of any set is bounded from above by the encoding speed of this set. We introduce a new abstract property of approximation families, called infinite-encodability, which implies this upper-bound. Many classical approximation families, defined with dictionaries or ReLU networks, are shown to be infinite-encodable. This unifies and generalizes several situations where this upper-bound is known [7].

7.1.4 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 [28].

7.1.5 Can sparsity improve the privacy of neural networks?

Sparse neural networks are mainly motivated by ressource efficiency since they use fewer parameters than their dense counterparts but still reach comparable accuracies. This article empirically investigates whether sparsity could also improve the privacy of the data used to train the networks. The experiments show positive correlations between the sparsity of the model, its privacy, and its classification error. Simply comparing the privacy of two models with different sparsity levels can yield misleading conclusions on the role of sparsity, because of the additional correlation with the classification error. From this perspective, some caveats are raised about previous works that investigate sparsity and privacy [23].

7.2 Floating-point and Validated Numerics

7.2.1 Floating-point arithmetic: invited survey for *Acta Numerica*

Floating-point numbers have an intuitive meaning when it comes to physics-based numerical computations, and they have thus become the most common way of approximating real numbers in computers. The IEEE-754 Standard has played a large part in making floating-point arithmetic ubiquitous today, by specifying its semantics in a strict yet useful way as early as 1985. In particular, floating-point operations should be performed as if their results were first computed with an infinite precision and then rounded to the target format. A consequence is that floating-point arithmetic satisfies the 'standard model' that is often used for analysing the accuracy of floating-point algorithms. But that is only scraping the surface, and floating-point arithmetic offers much more. In the survey [2] we recall the history of floating-point arithmetic as well as its specification mandated by the IEEE-754 Standard. We also recall what properties it entails and what every programmer should know when designing a floating-point algorithm. We provide various basic blocks that can be implemented with floating-point arithmetic. In particular, one can actually compute the rounding error caused by some floating-point operations, which paves the way to designing more accurate algorithms. More generally, properties of floating-point arithmetic make it possible to extend the accuracy of computations beyond working precision.

7.2.2 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 [5].

7.2.3 Testing The Sharpness of Known Error Bounds on The Fast Fourier Transform

The computation of Fast Fourier Transforms (FFTs) in floating-point arithmetic is inexact due to roundings, and for some applications it can prove very useful to know a tight bound on the final error. Although it can be almost attained by specifically built input values, the best known error bound for the Cooley-Tukey FFT seems to be much larger than most actually obtained errors. Also, interval arithmetic can be used to compute a bound on the error committed with a given set of input values, but it is in general considered hampered with large overestimation. We report results of intensive computations to test the two approaches, in order to estimate the numerical performance of state-of-the-art bounds. Surprisingly enough, we observe that while interval arithmetic-based bounds are overestimated, they remain, in our computations, tighter than general known bounds [13].

7.2.4 Affine Iterations and Wrapping Effect: Various Approaches

Affine iterations of the form $x_{n+1} = Ax_n + b$ converge, using real arithmetic, if the spectral radius of the matrix A is less than 1. However, substituting interval arithmetic to real arithmetic may lead to divergence of these iterations, in particular if the spectral radius of the absolute value of A is greater than 1. In [11], we review different approaches to limit the overestimation of the iterates, when the components of the initial vector x_0 and b are intervals. We compare, both theoretically and experimentally, the widths of the iterates computed by these different methods: the naive iteration, methods based on the QR-and SVD-factorization of A, and Lohner's QR-factorization method. The method based on the SVD-factorization is computationally less demanding and gives good results when the matrix is poorly scaled, it is superseded either by the naive iteration or by Lohner's method otherwise.

7.2.5 A framework to test interval arithmetic libraries and their IEEE 1788-2015 compliance

As developers of libraries implementing interval arithmetic, we faced the same difficulties when it comes to testing our libraries. What must be tested? How can we devise relevant test cases for unit testing? How can we ensure a high (and possibly 100%) test coverage? In [1], before considering these questions, we briefly recall the main features of interval arithmetic and of the IEEE 1788-2015 standard for interval arithmetic. After listing the different aspects that, in our opinion, must be tested, we contribute a first step towards offering a test suite for an interval arithmetic library. First we define a format that enables the exchange of test cases, so that they can be read and tried easily. Then we offer a first set of test cases, for a selected set of mathematical functions. Next, we examine how the Julia interval arithmetic library, IntervalArithmetic.jl, actually performs to these tests. As this is an ongoing work, we list extra tests that we deem important to perform.

7.2.6 About the "accurate mode" of the IEEE 1788-2015 standard for interval arithmetic

The IEEE 1788-2015 standard for interval arithmetic defines three accuracy modes for the so-called set-based flavor: tightest, accurate and valid. This work in progress [30] focuses on the accurate mode. First, an introduction to interval arithmetic and to the IEEE 1788-2015 standard is given, then the accurate mode is defined. How can this accurate mode be tested, when a library implementing interval arithmetic claims to provide this mode? The chosen approach is unit testing, and the elaboration of testing pairs for this approach is developed. A discussion closes this paper: how can the tester be tested? And if we go to the roots of the subject, is the accurate mode really relevant or should it be dropped off in the next version of the standard?

7.2.7 Towards a correctly-rounded and fast power function in binary64 arithmetic

In [16] 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 in an extended version of this paper, with the goal to enable a formal proof of these algorithms. We hope this work will motivate the next IEEE 754 revision committee to require correct rounding for mathematical functions.

7.2.8 Accurate calculation of Euclidean norms

This work was done with Laurence Rideau (STAMP Team, Sophia). In [8], we consider the computation of the Euclidean (or L2) norm of an n-dimensional vector in floating-point arithmetic. We review the classical solutions used to avoid spurious overflow or underflow and/or to obtain very accurate results. We modify a recently published algorithm (that uses double-word arithmetic) to allow for a very accurate solution, free of spurious overflows and underflows. To that purpose, we use a double-word square-root algorithm of which we provide a tight error analysis. The returned L2 norm will be within very slightly more than 0.5 ulp from the exact result, which means that we will almost always provide correct rounding.

7.3 Lattices: Algorithms and Cryptology

7.3.1 Constrained Pseudorandom Functions from Homomorphic Secret Sharing

We propose and analyze a simple strategy for constructing 1-key constrained pseudorandom functions (CPRFs) from homomorphic secret sharing. In the process, we obtain the following contributions. First, we identify desirable properties for the underlying HSS scheme for our strategy to work. Second, we show that (most) recent existing HSS schemes satisfy these properties, leading to instantiations of CPRFs for various constraints and from various assumptions. Notably, we obtain the first (1-key selectively secure, private) CPRFs for inner-product and (1-key selectively secure) CPRFs for NC 1 from the DCR assumption, and more. Lastly, we revisit two applications of HSS, equipped with these additional properties, to secure computation: we obtain secure computation in the silent preprocessing model with one party being able to precompute its whole preprocessing material before even knowing the other party, and we construct one-sided statistically secure computation with sublinear communication for restricted forms of computation. This is a joint by Geoffroy Couteau, Pierre Meyer, Alain Passelègue, and Mahshid Riahinia, published at Eurocrypt 2023 [22].

7.3.2 A Detailed Analysis of Fiat-Shamir with Aborts

Lyubashevky's signatures are based on the Fiat-Shamir with Aborts paradigm. It transforms an interactive identification protocol that has a non-negligible probability of aborting into a signature by repeating executions until a loop iteration does not trigger an abort. Interaction is removed by replacing the challenge of the verifier by the evaluation of a hash function, modeled as a random oracle in the analysis. The access to the random oracle is classical (ROM), resp. quantum (QROM), if one is interested in security against classical, resp. quantum, adversaries. Most analyses in the literature consider a setting with a bounded number of aborts (i.e., signing fails if no signature is output within a prescribed number of loop iterations), while practical instantiations (e.g., Dilithium) run until a signature is output (i.e., loop iterations are unbounded).

In this work, we emphasize that combining random oracles with loop iterations induces numerous technicalities for analyzing correctness, run-time, and security of the resulting schemes, both in the bounded and unbounded case. As a first contribution, we put light on errors in all existing analyses. We then provide two detailed analyses in the QROM for the bounded case, adapted from Kiltz et al. [EUROCRYPT'18] and Grilo et al. [ASIACRYPT'21]. In the process, we prove the underlying -protocol to achieve a stronger zero-knowledge property than usually considered for -protocols with aborts, which enables a corrected analysis. A further contribution is a detailed analysis in the case of unbounded aborts, the latter inducing several additional subtleties.

This is a joint work by Julien Devevey, Pouria Fallahpour, Alain Passelègue, and Damien Stehlé, published at Crypto 2023 [14].

7.3.3 G+G: A Fiat-Shamir Lattice Signature Based on Convolved Gaussians

We describe an adaptation of Schnorr's signature to the lattice setting, which relies on Gaussian convolution rather than flooding or rejection sampling as previous approaches. It does not involve any abort, can be proved secure in the ROM and QROM using existing analyses of the Fiat-Shamir transform, and enjoys smaller signature sizes (both asymptotically and for concrete security levels).

This is a joint work by Julien Devevey, Alain Passelègue, and Damien Stehlé, published at Asiacrypt 2023 [18].

7.3.4 Efficient Updatable Public-Key Encryption from Lattices

Updatable public key encryption has recently been introduced as a solution to achieve forward-security in the context of secure group messaging without hurting efficiency, but so far, no efficient lattice-based instantiation of this primitive is known.

In this work, we construct the first LWE-based UPKE scheme with polynomial modulus-to-noise rate, which is CPA-secure in the standard model. At the core of our security analysis is a generalized reduction from the standard LWE problem to (a stronger version of) the Extended LWE problem. We further extend

our construction to achieve stronger security notions by proposing two generic transforms. Our first transform allows to obtain CCA security in the random oracle model and adapts the Fujisaki-Okamoto transform to the UPKE setting. Our second transform allows to achieve security against malicious updates by adding a NIZK argument in the update mechanism. In the process, we also introduce the notion of Updatable Key Encapsulation Mechanism (UKEM), as the updatable variant of KEMs. Overall, we obtain a CCA-secure UKEM in the random oracle model whose ciphertext sizes are of the same order of magnitude as that of CRYSTALS-Kyber.

This is a joint work by Calvin Abou Haidar, Alain Passelègue, and Damien Stehlé, published at Asiacrypt 2023 [19].

7.3.5 Ideal-SVP is Hard for Small-Norm Uniform Prime Ideals

The presumed hardness of the Shortest Vector Problem for ideal lattices (Ideal-SVP) has been a fruitful assumption to understand other assumptions on algebraic lattices and as a security foundation of cryptosystems. Gentry [CRYPTO'10] proved that Ideal-SVP enjoys a worst-case to average-case reduction, where the average-case distribution is the uniform distribution over the set of inverses of prime ideals of small algebraic norm (below $d^{O(d)}$ for cyclotomic fields, here d refers to the field degree). De Boer et al. [CRYPTO'20] obtained another random self-reducibility result for an average-case distribution involving integral ideals of norm 2^{d^2} .

In this work, we show that Ideal-SVP for the uniform distribution over inverses of small-norm prime ideals reduces to Ideal-SVP for the uniform distribution over small-norm prime ideals. Combined with Gentry's reduction, this leads to a worst-case to average-case reduction for the uniform distribution over the set of *small-norm prime ideals*. Using the reduction from Pellet-Mary and Stehlé [ASIACRYPT'21], this notably leads to the first distribution over NTRU instances with a polynomial modulus whose hardness is supported by a worst-case lattice problem.

This is a joint work by Joël Felderhoff, Alice Pellet-Mary, Damien Stehlé, and Benjamin Wesolowski published at TCC 2023 [15].

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 [3].

7.4.2 Differential-Difference Properties of Hypergeometric Series

Six families of generalized hypergeometric series in a variable x and an arbitrary number of parameters are considered. Each of them is indexed by an integer n. Linear recurrence relations in n relate these functions and their product by the variable x. We give explicit factorizations of these equations as products of first order recurrence operators. Related recurrences are also derived for the derivative with respect to x. These formulas generalize well-known properties of the classical orthogonal polynomials [6].

7.4.3 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 [9].

7.4.4 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 [17].

7.4.5 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 [27].

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 [9] 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 $d = O(n^{0.47})$ [10].

7.4.7 Exact computations with quasiseparable matrices

Quasiseparable matrices are a class of rank-structured matrices widely used in numerical linear algebra and of growing interest in computer algebra, with applications in e.g. the linearization of polynomial matrices. Various representation formats exist for these matrices that have rarely been compared. We show how the most central formats SSS and HSS can be adapted to symbolic computation, where the exact rank replaces threshold based numerical ranks. We clarify their links and compare them with the `Bruhat` format. To this end, we state their space and time cost estimates based on fast matrix multiplication, and compare them, with their leading constants. The comparison is supported by software experiments. We make further progresses for the `Bruhat` format, for which we give a generation algorithm, following a Crout elimination scheme, which specializes into fast algorithms for the construction from a sparse matrix or from the sum of `Bruhat` representations [20, 25].

7.4.8 Elimination ideal and bivariate resultant over finite fields

A new algorithm is presented for computing the largest degree invariant factor of the Sylvester matrix (with respect either to x or y) associated to two polynomials a and b in $\mathbb{F}_q[x,y]$ which have no non-trivial common divisors. The algorithm is randomized of the Monte Carlo type and requires $(de\log q)^{1+o(1)}$ bit operations, where d and e respectively bound the input degrees in x and in y. It follows that the same complexity estimate is valid for computing: a generator of the elimination ideal $\langle a,b\rangle \cap \mathbb{F}_q[x]$ (or $\mathbb{F}_q[y]$), as long as the polynomial system $a = b = 0$ has not roots at infinity; the resultant of a and b when they are sufficiently generic, especially so that the Sylvester matrix has a unique non-trivial invariant factor. Our approach is to use the reduction of the problem to a problem of minimal polynomial in the quotient algebra $\mathbb{F}_q[x,y]/\langle a,b\rangle$. By proposing a new method based on structured polynomial matrix division

for computing with the elements in the quotient, we manage to improve the best known complexity bounds [21].

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

Bosch (Stuttgart) ordered from us some support for the design and implementation of accurate functions in binary32 floating-point arithmetic (inverse trigonometric functions, hyperbolic functions and their inverses, exponential, logarithm, ...).

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

9 Partnerships and cooperations

9.1 International initiatives

9.1.1 Associate Teams in the framework of an Inria International Lab or in the framework of an Inria International Program

Associated team *Symbolic*, Canada-France, 2022-2024, University of Waterloo and Inria.

Participants: Claude-Pierre Jeannerod, Bruno Salvy, Gilles Villard.

Coordinators: Éric Schost (PI Waterloo), Gilles Villard (PI AriC). The Symbolic Computation Group at Waterloo and AriC expand established collaborations, to design and implement algorithms for linear and non-linear symbolic algebra. Four main directions are especially investigated: dense matrices, structured linear algebra, polynomial arithmetic, and analytic combinatorics.

9.2 International research visitors

9.2.1 Visits of international scientists

Inria International Chair

Participant: Warwick Tucker.

From Monash University, Australia. Title: Attracteur de Hénon; intégrales abéliennes liées aux 16e problème de Hilbert

Summary: The goal of the proposed research program is to unify the techniques of modern scientific computing with the rigors of mathematics and develop a functional foundation for solving mathematical problems with the aid of computers. Our aim is to advance the field of computer-aided proofs in analysis; we strongly believe that this is the only way to tackle a large class of very hard mathematical problems.

9.3 National initiatives

9.3.1 France 2030 ANR Project - PEPR Cybersecurity - SecureCompute

Participant: Alain Passelègue.

SecureCompute is a France 2030 ANR 6-year project (started in July 2022) focused on the study of cryptographic mechanisms allowing to ensure the security of data, during their transfer, at rest, but also during processing, despite uncontrolled environments such as the Internet for exchanges and the Cloud for hosting and processing. Security, in this context, not only means confidentiality but also integrity, a.k.a. the correct execution of operations. See the web page of the project. It is headed by ENS-PSL (Inria CASCADE team-project), and besides AriC, also involves CEA, IRIF (Université Paris Cité), and LIRMM (Université de Montpellier).

The project ended prematurely on August 31, 2023, following the departure of Alain Passelègue.

9.3.2 France 2030 ANR Project - PEPR Quantique - PostQuantum-TLS

Participant: Damien Stehlé.

PostQuantum-TLS is a France 2030 ANR 5-year project (started in 2022) focused on post-quantum cryptography. The famous "padlock" appearing in browsers when one visits websites whose address is preceded by "https" relies on cryptographic primitives that would not withstand a quantum computer. This integrated project aims to develop post-quantum primitives in a prototype of "post-quantum lock" that will be implemented in an open source browser. The evolution of cryptographic standards has already started, the choice of new primitives will be made quickly, and the transition will be made in the next few years. The objective is to play a driving role in this evolution and to make sure that the French actors of post-quantum cryptography, already strongly involved, are able to influence the cryptographic standards of the decades to come.

Benjamin Wesolowski (UMPA) replaced Damien Stehlé as the leader in Lyon for this project.

9.3.3 ANR RAGE Project

Participant: Alain Passelègue.

RAGE is a four-year project (started in January 2021) focused on the randomness generation for advanced cryptography. See the web page of the project. It is headed by Alain Passelègue and also involves Pierre Karpmann (UGA) and Thomas Prest (PQShield). The main goals of the project are: (i) construct and analyze security of low-complexity pseudorandom functions that are well-suited for MPC-based and FHE-based applications, (ii) construct advanced forms of pseudorandom functions, such as (private) constrained PRFs.

The project ended prematurely on August 31, 2023, following the departure of Alain Passelègue.

9.3.4 ANR CHARM Project

Participants: Damien Stehlé, Guillaume Hanrot, Joël Felderhoff.

CHARM is a three-year project (started in October 2021) focused on the cryptographic hardness of module lattices. See the web page of the project. It is co-headed by Shi Bai (FAU, USA) and Damien Stehlé, with two other sites: the U. of Bordeaux team led by Benjamin Wesolowski (with Bill Allombert, Karim Belabas, Aurel Page and Alice Pellet-Mary) and the Cornell team led by Noah Stephens-Davidowitz. The main goal of the project is to provide a clearer understanding of the intractability of module lattice problems via improved reductions and improved algorithms. It will be approached by investigating the

following directions: (i) showing evidence that there is a hardness gap between rank 1 and rank 2 module problems, (ii) determining whether the NTRU problem can be considered as a rank 1.5 module problem, (iii) designing algorithms dedicated to module lattices, along with implementation and experiments.

Following the departures of Guillaume Hanrot and Damien Stehlé, Benjamin Wesolowski (UMPA) took the lead on this project.

9.3.5 France 2030 ANR Project - HQI

Participant: Damien Stehlé.

The Hybrid HPC Quantum Initiative is a France 2030 ANR 5-year project (started in 2022) focused on quantum computing. We are involved in the Cryptanalysis work package. The application of quantum algorithms for cryptanalysis is known since the early stages of quantum computing when Shor presented a polynomial-time quantum algorithm for factoring, a problem which is widely believed to be hard for classical computers and whose hardness is one of the main cryptographic assumptions currently used. Therefore, with the development of (full-scalable) quantum computers, the security of many cryptographic protocols of practical importance would be broken. Therefore, it is necessary to find other computational assumptions that can lead to cryptographic schemes that are secure against quantum adversaries. While we have candidate assumptions, their security against quantum attacks is still under scrutiny. In this work package, we will study new quantum algorithms for cryptanalysis and their implementation in the hybrid platform of the national platform. The goal is to explore the potential weaknesses of old and new cryptographic assumptions, potentially finding new attacks on the proposed schemes.

The project ended prematurely on March 31, 2023, following the departure of Damien Stehlé, but Benjamin Wesolowski (UMPA) is still involved.

9.3.6 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.

9.3.7 ANR/Astrid AMIRAL Project

Participants: Alain Passelègue, Damien Stehlé.

AMIRAL is a four-year project (starting in January 2022) that aims to improve lattice-based signatures and to develop more advanced related cryptographic primitives. See the web page of the project. It is headed by Adeline Roux-Langlois from Irisa (Rennes) and locally by Alain Passelègue. The main goals of the project are: (i) optimize the NIST lattice-based signatures, namely CRYSTALS-DILITHIUM and FALCON, (ii) develop advanced signatures, such as threshold signatures, blind signatures, or aggregated signatures, and (iii) generalize the techniques developed along the project to other related primitives, such as identity-based and attribute-based encryption.

The project ended prematurely on August 31, 2023, following the departure of Alain Passelègue.

10 Dissemination

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

General chair, scientific chair

Alain Passelègue and Damien Stehlé (as well as Benjamin Wesolowski from ENS Lyon - UMPA) co-organized Eurocrypt 2023 in Lyon in April 2023.

Member of the organizing committees

Bruno Salvy and Gilles Villard have co-organized two trimesters in 2023 on Recent Trends in Computer Algebra in Lyon and Paris.

10.1.2 Scientific events: selection

Member of the conference program committees

Jean-Michel Muller and Nathalie Revol served in the program committee of the Arith 2023 conference.

Alain Passelègue served in the program committee of PKC 2023 and Crypto 2023, and of the national Journées Codes et Cryptographie (C2).

10.1.3 Journal

Member of the 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).

Damien Stehlé is an editor of the *Journal of Cryptology* and of *Designs, Codes and Cryptography*.

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

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.

10.1.5 Research administration

Nicolas Brisebarre is co-head of GT ARITH (GDR IM).

Nathalie Revol is a member of the Inria Evaluation Committee and of the Inria Commission Administrative Paritaire.

Alain Passelègue is a member of the board of GT C2, as well as a member of the program committee of the national Séminaire C2.

10.2 Teaching - Juries

10.2.1 Teaching

Master: Nicolas Brisebarre, Computer Algebra, 30h, Univ. Polynésie Française

Master: Nicolas Brisebarre, "Approximation Theory and Proof Assistants: Certified Computations", 12h, M2, ENS de Lyon

Master: Claude-Pierre Jeannerod, Computer Algebra, 30h in 2023, M2, ISFA, France

Master: Nicolas Louvet, Compilers, 15h, M1, UCB Lyon 1, France

Master: Nicolas Louvet, Introduction to Operating Systems, 30h, M2, UCB Lyon 1, France

Master: Vincent Lefèvre, Computer Arithmetic, 10.5h in 2023, M2, ISFA, France

Master: Jean-Michel Muller, Floating-Point Arithmetic and beyond, 7h in 2021, M2, ENS de Lyon, France

Master: Alain Passelègue, Cryptography and Security, 24h, M1, ENS de Lyon, France

Master: Alain Passelègue, Interactive and Non-Interactive Proofs in Complexity and Cryptography, 20h, M2, ENS de Lyon, France

Licence: Alain Passelègue, in charge of 1st year student (L3) research internships, 12h, L3, ENS de Lyon, France

Postgrad: Nathalie Revol, "Scientific Dissemination and Outreach Activities", 36h in 2023 (3 groups, 12h/group), 4th year students, ENS de Lyon, France

Master: Bruno Salvy, Computer Algebra, 24h, M1, ENS de Lyon, France

Master: Bruno Salvy, Modern Algorithms in Symbolic Summation and Integration, 10h, M2, ENS de Lyon, France

Master: Damien Stehlé, Post-quantum cryptography, 12h, M2, ENS de Lyon, France

Master: Gilles Villard, Modern Algorithms in Symbolic Summation and Integration, 10h, M2, ENS de Lyon, France

10.2.2 Juries

Nathalie Revol was a member of the recruiting committee for an associate professor position at Sorbonne University.

Nathalie Revol was an examiner in the PhD committees of Nuwan Herath Mudiyanselage (U. Lorraine), Daria Pchelina (U. Sorbonne Paris Nord) and Maria Luiza Costa Vianna (École Polytechnique).

10.3 Popularization

10.3.1 Internal or external Inria responsibilities

Nathalie Revol is the scientific leader of the Interstices magazine (above 750,000 pages visited per year), where she also regularly writes reading recommendations.

Regarding parity issues: Nathalie Revol is a member of the parity committee of the LIP laboratory; in particular she co-organized "women-only lunches". She is a member of the parity committee of Inria: this year, her work focused on the adoption of a chart about the inclusion of LGBTQI+ people, and on making the working environment more inclusive. As every year, she co-organized in November a day "Journée Filles & Maths-Info" at ENS Lyon for female high-school pupils (around 90 pupils). She was in charge of the animation of workshops about debunking stereotypes, in Lyon and St-Étienne. She co-organized the visit of the LIP laboratory for 3 groups of 15 high-school female pupils around the 8th of March during the "Sciences: un métier de femmes" day.

10.3.2 Articles and contents

Nathalie Revol wrote an article about women in mathematics and computer science [33], as an introduction to the special issue no 86 of MathemaTICE, a Web magazine for mathematics teachers. She took part to two roundtables on March 8, one at the "Global Industry and AI" forum and one at Préfecture du Rhône, about women in computer science. She introduced the structure and content of the "Journée Filles & Maths-Info" in 180 seconds during the Inria "séminaire médiation" in Sophia-Antipolis, April 2023. She took part to the creation of the topics that will be explored by high-schools pupils during a computer science camp, Fall 2024, about "green networks" in relation with the Facto ANR.

10.3.3 Education

Nathalie Revol teaches how to popularize science towards a large audience, to 4th year students at ENS de Lyon.

10.3.4 Interventions

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 Declics action, once as "captain" and once as member (lycée Juliette Récamier, 70 pupils). She was present during Mondial des Métiers to provide information about scientific careers, to high-school pupils and their parents (around 65 persons).

Alain Passelègue spend half a day in a middle school in Lagnieu to talk about modern cryptography and its usage in the world, as well as about the work as a researcher. This was part of a project around Alan Turing led by English, Maths, and History teachers from the school.

11 Scientific production

11.1 Publications of the year

International journals

[1] L. Benet, L. Ferranti and N. Revol. ‘A framework to test interval arithmetic libraries and their IEEE 1788-2015 compliance’. In: *Concurrency and Computation: Practice and Experience* (31st Aug. 2023), e7856. DOI: 10.1002/cpe.7856. URL: https://hal.science/hal-04183957.

[2] S. Boldo, C.-P. Jeannerod, G. Melquiond and J.-M. Muller. ‘Floating-point arithmetic’. In: *Acta Numerica* 32 (May 2023), pp. 203–290. DOI: 10.1017/S0962492922000101. URL: https://hal.science/hal-04095151.

[3] A. Bostan, T. Rivoal and B. Salvy. ‘Minimization of differential equations and algebraic values of E-functions’. In: *Mathematics of Computation* (2023). URL: https://hal.science/hal-03771150.

[4] F. Bréhard, N. Brisebarre, M. Joldeş and W. Tucker. ‘Efficient and Validated Numerical Evaluation of Abelian Integrals’. In: *ACM Transactions on Mathematical Software* (2023). URL: https://hal.science/hal-03561096.

[5] 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* (2023). DOI: 10.1109/TETC.2023.3294986. URL: https://hal.science/hal-04044716.

[6] N. Brisebarre and B. Salvy. ‘Differential-Difference Properties of Hypergeometric Series’. In: *Proceedings of the American Mathematical Society* 151.6 (2023), pp. 2603–2617. DOI: 10.1090/proc/16316. URL: https://inria.hal.science/hal-03712632.

[7] A. Gonon, N. Brisebarre, R. Gribonval and E. Riccietti. 'Approximation speed of quantized vs. unquantized ReLU neural networks and beyond'. In: *IEEE Transactions on Information Theory* 69.6 (1st June 2023), pp. 3960–3977. DOI: 10.1109/TIT.2023.3240360. URL: https://hal.science/hal-03672166.

[8] V. Lefèvre, N. Louvet, J.-M. Muller, J. Picot and L. Rideau. 'Accurate calculation of Euclidean Norms using Double-word arithmetic'. In: *ACM Transactions on Mathematical Software* 49.1 (21st Mar. 2023), pp. 1–34. DOI: 10.1145/3568672. URL: https://hal.science/hal-03482567.

[9] V. Neiger, B. Salvy, É. Schost and G. Villard. 'Faster Modular Composition'. In: *Journal of the ACM (JACM)* (2023). URL: https://hal.science/hal-03380258.

[10] C. Pernet, H. Signargout and G. Villard. 'High-order lifting for polynomial Sylvester matrices'. In: *Journal of Complexity* 80 (2023). DOI: 10.1016/j.jco.2023.101803. URL: https://hal.science/hal-03740320.

[11] N. Revol. 'Affine Iterations and Wrapping Effect: Various Approaches'. In: *Acta Cybernetica* 26.1 (2nd June 2023), pp. 129–147. DOI: 10.14232/actacyb.295251. URL: https://inria.hal.science/hal-03505854.

International peer-reviewed conferences

[12] N. Brisebarre and S.-I. Filip. 'Towards Machine-Efficient Rational L ∞ -Approximations of Mathematical Functions'. In: *Proceedings of the 30th IEEE International Symposium on Computer Arithmetic ARITH 2023, Sep 2023, Portland, Oregon, USA*. 30th IEEE International Symposium on Computer Arithmetic ARITH 2023. Portland, United States, 4th Sept. 2023. URL: https://hal.science/hal-04093020.

[13] N. Brisebarre, J.-M. Muller and J. Picot. 'Testing The Sharpness of Known Error Bounds on The Fast Fourier Transform'. In: 30th IEEE International Symposium on Computer Arithmetic ARITH 2023. Portland, Oregon, USA, France, 4th Sept. 2023. URL: https://inria.hal.science/hal-04092770.

[14] J. Devevey, P. Fallahpour, A. Passelègue and D. Stehlé. 'A Detailed Analysis of Fiat-Shamir with Aborts'. In: Crypto 2023. Vol. 14085. Lecture Notes in Computer Science. Santa Barbara, United States: Springer Nature Switzerland, 9th Aug. 2023, pp. 327–357. DOI: 10.1007/978-3-031-38554-4_11. URL: https://hal.science/hal-04334942.

[15] J. Felderhoff, A. Pellet-Mary, D. Stehlé and B. Wesolowski. 'Ideal-SVP is Hard for Small-Norm Uniform Prime Ideals'. In: *Lecture Notes in Computer Science*. Theory of Cryptography, TCC 2023. Vol. 14372. Lecture Notes in Computer Science. Taipei (Taiwan), Taiwan: Springer Nature Switzerland, 27th Nov. 2023, pp. 63–92. DOI: 10.1007/978-3-031-48624-1_3. URL: https://hal.science/hal-04326750.

[16] T. Hubrecht, C.-P. Jeannerod and P. Zimmermann. 'Towards a correctly-rounded and fast power function in binary64 arithmetic'. In: 2023 IEEE 30th Symposium on Computer Arithmetic (ARITH 2023). Vol. 2023 IEEE 30th Symposium on Computer Arithmetic (ARITH). Portland, Oregon (USA), United States, 2023. URL: https://inria.hal.science/hal-04326201.

[17] A. Ibrahim and B. Salvy. 'Positivity certificates for linear recurrences'. In: *Proceedings SODA*. SODA. Alexandria, Virginia, United States, 2024. URL: https://inria.hal.science/hal-04271203.

[18] A. Passelègue, J. Devevey and D. Stehlé. 'G+G: A Fiat-Shamir Lattice Signature Based on Convolved Gaussians'. In: Asiacrypt 2023. Guangzhou (Canton), China, 2023. URL: https://hal.science/hal-04334958.

[19] A. Passelègue, D. Stehlé and C. Abou Haidar. 'Efficient Updatable Public-Key Encryption from Lattices'. In: Asiacrypt 2023. Guangzhou (Canton), China, 2023. URL: https://hal.science/hal-04334950.

[20] C. Pernet, H. Signargout and G. Villard. 'Exact computations with quasiseparable matrices'. In: ISSAC'23: the 2023 International Symposium on Symbolic and Algebraic Computation. Tromso, Norway: ACM, 17th July 2023, pp. 480–489. DOI: 10.1145/2930889.2930915. URL: https://cnrs.hal.science/hal-03978799.

[21] G. Villard. 'Elimination ideal and bivariate resultant over finite fields'. In: *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation*. ISSAC 2023: International Symposium on Symbolic and Algebraic Computation 2023. Tromsø Norway, Norway: ACM; ACM, 24th July 2023, pp. 526–534. DOI: 10.1145/3597066.3597100. URL: https://hal.science/hal-03999414.

National peer-reviewed Conferences

[22] G. Couteau, P. Meyer, A. Passelègue and M. Riahinia. 'Constrained Pseudorandom Functions from Homomorphic Secret Sharing'. In: *Lecture Notes in Computer Science*. 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques,EUROCRYPT 2023. Vol. 14006. Lecture Notes in Computer Science. Lyon, France: Springer Nature Switzerland, 15th Apr. 2023, pp. 194–224. DOI: 10.1007/978-3-031-30620-4_7. URL: https://hal.science/hal-04265643.

[23] A. Gonon, L. Zheng, C. Lalanne, Q.-T. Le, G. Lauga and C. Pouliquen. 'Can sparsity improve the privacy of neural networks?' In: GRETSI 2023 - XXIXème Colloque Francophone de Traitement du Signal et des Images. Grenoble, France, 18th Apr. 2023. URL: https://hal.science/hal-04062317.

Doctoral dissertations and habilitation theses

[24] J. Devevey. 'Lattice-based Signatures in the Fiat-Shamir Paradigm'. Ecole Normale Supérieure de Lyon, 18th Sept. 2023. URL: https://hal.science/tel-04320790.

[25] H. Signargout. 'Exact computations with quasiseparable matrices and polynomial matrices with a displacement structure'. École Normale Supérieure de Lyon, 5th Oct. 2023. URL: https://hal.science/tel-04326015.

Reports & preprints

[26] N. Brisebarre and G. Hanrot. *Integer points close to a transcendental curve and correctly-rounded evaluation of a function*. 2023. URL: https://hal.science/hal-03240179.

[27] H. Brochet and B. Salvy. *Reduction-Based Creative Telescoping for Definite Summation of D-Finite Functions*. 14th July 2023. URL: https://hal.science/hal-04295759.

[28] A. Gonon, N. Brisebarre, E. Riccietti and R. Gribonval. *A path-norm toolkit for modern networks: consequences, promises and challenges*. Sept. 2023. URL: https://hal.science/hal-04225201.

[29] C. Pernet, H. Signargout and G. Villard. *Leading constants of rank deficient Gaussian elimination*. 6th Feb. 2023. URL: https://cnrs.hal.science/hal-03976168.

[30] N. Revol. *About the "accurate mode" of the IEEE 1788-2015 standard for interval arithmetic*. Apr. 2023. URL: https://inria.hal.science/hal-04160357.

11.2 Other

Scientific popularization

[31] S. Boldo, N. Brisebarre and J.-M. Muller. 'Le dilemme du fabricant de tables'. In: *La Recherche* 572 (Jan. 2023). URL: https://inria.hal.science/hal-03932037.

[32] J.-M. Muller. 'Arithmétique des Ordinateurs'. In: Colloque Raisonner en arithmétique, est-ce incongru ? Talence (33), France, 2023. URL: https://hal.science/hal-04207082.

[33] N. Revol. 'Computer science and mathematics: far from parity'. In: *MathémaTICE* 86 (Sept. 2023). URL: https://inria.hal.science/hal-04160309.