RESEARCH CENTRE

Inria Lyon Center

IN PARTNERSHIP WITH:

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

2022

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, Researcher, HDR]
- Claude-Pierre Jeannerod [INRIA, Researcher]
- Vincent Lefèvre [INRIA, Researcher]
- Benoît Libert [CNRS, Senior Researcher, until Nov 2022, HDR]
- Jean-Michel Muller [CNRS, Senior Researcher, HDR]
- Alain Passelègue [INRIA, Researcher]
- Nathalie Revol [INRIA, Researcher]
- Warwick Tucker [Monash University, Australia, Advanced Research Position, from Oct 2022]
- Gilles Villard [CNRS, Senior Researcher, HDR]

Faculty Members

- Guillaume Hanrot [ENS de LYON, Professor, HDR]
- Nicolas Louvet [UNIV LYON I, Associate Professor]
- Damien Stehlé [ENS de LYON, Professor, HDR]

Post-Doctoral Fellows

- Dmitrii Koshelev [ENS de LYON, from Oct 2022]
- Fabrice Mouhartem [ENS de LYON, until Jun 2022]

PhD Students

- Calvin Abou Haidar [INRIA]
- Orel Cosseron [ZAMA and INRIA]
- Julien Devevey [ENS de LYON]
- Pouria Fallahpour [ENS de LYON]
- Joel Felderhoff [INRIA, from Feb 2022]
- Antoine Gonon [ENS de LYON]
- Arthur Herledan Le Merdy [ENS de LYON, from Oct 2022]
- Alaa Ibrahim [INRIA, from Nov 2022]
- Mahshid Riahinia [ENS de LYON]
- Hippolyte Signargout [ENS de LYON]

Technical Staff

- Joris Picot [ENS de LYON, Engineer]

Interns and Apprentices

- Hadrien Brochet [INRIA, from Mar 2022 until May 2022]
- Alaa Ibrahim [INRIA, from Mar 2022 until Aug 2022]

Administrative Assistants

- Chiraz Benamor [ENS de LYON]
- Octavie Paris [ENS de LYON]

Visiting Scientist

- Hyeongmin Choe [SEOUL NATIONAL UNIV, from Aug 2022 until Nov 2022]

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 pratical 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

The Dilithium signature scheme and Kyber key exchange mechanism, co-authored by Damien Stehlé, have been selected by NIST for the standardization of post-quantum cryptography. Kyber is the only selected key exchange mechanism. Dilithium was chosen with two other signature schemes, Falcon and Sphincs+, and put forward as the primary choice.

6 New software and platforms

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.

News of the Year: In November 2022, a minor version (4.1.1) was released, with 13 bug fixes with respect to 4.1.0 (released in 2020), various internal changes due to the switch from Subversion to Git and a complete review of the typography of the manual. In early January 2023, a major version (4.2.0) was released, which in particular implements missing functions from the new ISO C23 standard.

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 Sipe

Keywords: Floating-point, Correct Rounding

Functional Description: Sipe is a mini-library in the form of a C header file, to perform radix-2 floating-point computations in very low precisions with correct rounding, either to nearest or toward zero. The goal of such a tool is to do proofs of algorithms/properties or computations of tight error bounds in these precisions by exhaustive tests, in order to try to generalize them to higher precisions. The currently supported operations are addition, subtraction, multiplication (possibly with the error term), fused multiply-add/subtract (FMA/FMS), and miscellaneous comparisons and conversions. Sipe provides two implementations of these operations, with the same API and the same behavior: one based on integer arithmetic, and a new one based on floating-point arithmetic.

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

Publications: hal-00763954, hal-00864580

Contact: Vincent Lefèvre

Participant: Vincent Lefèvre

6.1.5 LinBox

Keyword: Exact linear algebra

Functional Description: LinBox is an open-source C++ template library for exact, high-performance linear algebra computations. It is considered as the reference library for numerous computations (such as linear system solving, rank, characteristic polynomial, Smith normal forms,...) over finite fields and integers with dense, sparse, and structured matrices.

URL: http://linalg.org/

Contact: Clément Pernet

Participants: Clément Pernet, Thierry Gautier, Hippolyte Signargout, Gilles Villard

6.1.6 HPLLL

Keywords: Euclidean Lattices, Computer algebra system (CAS)

Functional Description: Software library for linear algebra and Euclidean lattice problems

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

Contact: Gilles Villard

6.1.7 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 Certified computation 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 in [22] 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.

7.1.2 Quantized ReLU neural networks

In [23], 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.

7.2 Floating-point and Validated Numerics

7.2.1 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 [6], different approaches, that limit the overestimation of the iterates when the components of the initial vector x_0 and b are intervals, are reviewed. The widths of the iterates computed by these different methods are compared, both theoretically and experimentally: the considered methods are 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.

7.2.2 Testing interval arithmetic libraries, including their IEEE-1788 compliance

As developers of libraries implementing interval arithmetic, we faced the same difficulties when it came 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 [20], we first list the different aspects that, in our opinion, must be tested, giving indications on the choice of test cases. Then we examine how several interval arithmetic libraries actually perform tests. Next, we present two existing frameworks developed specifically to gather test cases and to incorporate easily new libraries in order to test them, namely JInterval and ITF1788. Not every important aspects of our libraries fit in these frameworks and we list extra tests that we deem important, but not easy, to perform.

7.2.3 Formalization of double-word arithmetic

This work was done with Laurence Rideau (STAMP Team, Sophia). Recently, a complete set of algorithms for manipulating double-word numbers (some classical, some new) was analyzed [28]. In [5], we formally prove all the theorems given in that paper, using the Coq proof assistant. The formal proof work led us to: i) locate mistakes in some of the original paper proofs (mistakes that, however, do not hinder the validity of the algorithms), ii) significantly improve some error bounds, and iii) generalize some results by showing that they are still valid if we slightly change the rounding mode. The consequence is that the algorithms presented in [28] can be used with high confidence, and that some of them are even more accurate than what was believed before. This illustrates what formal proof can bring to computer arithmetic: beyond mere (yet extremely useful) verification, correction and consolidation of already known results, it can help to find new properties. All our formal proofs are freely available.

7.2.4 Accurate calculation of Euclidean Norms

This work was done with Laurence Rideau (STAMP Team, Sophia). In [3], 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.

7.2.5 High-level algorithms for correctly-rounded reciprocal square roots

This work was done in collaboration with Carlos Borges (Naval Postgraduate School, Monterrey). In [11], we analyze two fast and accurate algorithms recently presented by Borges for computing $x^{-1/2}$ in binary floating-point arithmetic (assuming that efficient and correctly-rounded FMA and square root are available). The first algorithm is based on the Newton-Raphson iteration, and the second one uses an order-3 iteration. We give attainable relative-error bounds for these two algorithms, build counterexamples showing that in very rare cases they do not provide a correctly-rounded result, and characterize precisely when such failures happen in IEEE 754 binary32 and binary64 arithmetics. We then give a generic (i.e., precision-independent) algorithm that always returns a correctly-rounded result, and show how it can be simplified and made more efficient in the important cases of binary32 and binary64.

7.3 Lattices: Algorithms and Cryptology

7.3.1 One-Shot Fiat-Shamir-based NIZK Arguments of Composite Residuosity and Logarithmic-Size Ring Signatures in the Standard Model

The standard model security of the Fiat-Shamir transform has been an active research area for many years. In breakthrough results, Canetti et al. (STOC'19) and Peikert-Shiehian (Crypto'19) showed that, under

the Learning-With-Errors (LWE) assumption, it provides soundness by applying correlation-intractable (CI) hash functions to so-called trapdoor Sigma-protocols. In order to be compatible with CI hash functions based on standard LWE assumptions with polynomial approximation factors, all known such protocols have been obtained via parallel repetitions of a basic protocol with binary challenges. In [16], we consider languages related to Paillier's composite residuosity assumption (DCR) for which we give the first trapdoor Sigma-protocols providing soundness in one shot, via exponentially large challenge spaces. This improvement is analogous to the one enabled by Schnorr over the original Fiat-Shamir protocol in the random oracle model. Using the correlation-intractable hash function paradigm, we then obtain simulation-sound NIZK arguments showing that an element of the set of invertible integers modulo N^2 is a composite residue, which opens the door to space-efficient applications in the standard model. As a concrete example, we build logarithmic-size ring signatures (assuming a common reference string) with the shortest signature length among schemes based on standard assumptions in the standard model. We prove security under the DCR and LWE assumptions, while keeping the signature size comparable with that of random-oracle-based schemes.

7.3.2 Rational Modular Encoding in the DCR Setting: Non-interactive Range Proofs and Paillier-Based Naor-Yung in the Standard Model

Range proofs allow a sender to convince a verifier that committed integers belong to an interval without revealing anything else. So far, all known non-interactive range proofs in the standard model rely on groups endowed with a bilinear map. Moreover, they either require the group order to be larger than the range of any proven statement or they suffer from a wasteful rate. Recently (Eurocrypt'21), Couteau et al. introduced a new approach to efficiently prove range membership by encoding integers as a modular ratio between small integers. In [14], we show that their technique can be transposed in the standard model under the Composite Residuosity (DCR) assumption. Interestingly, with this modification, the size of ranges is not a priori restricted by the common reference string. It also gives a constant ratio between the size of ranges and proofs. Moreover, we show that their technique of encoding messages as bounded rationals provides a secure standard model instantiation of the Naor-Yung CCA2 encryption paradigm under the DCR assumption.

7.3.3 Updatable Public Key Encryption from DCR: Efficient Constructions with Stronger Security

Forward-secure encryption (FS-PKE) is a key-evolving public-key paradigm that preserves the confidentiality of past encryptions in case of key exposure. Updatable public-key encryption (UPKE) is a natural relaxation of FS-PKE, introduced by Jost et al. (Eurocrypt'19), which is motivated by applications to secure messaging. In UPKE, key updates can be triggered by any sender – via special update ciphertexts – willing to enforce the forward secrecy of its encrypted messages. So far, the only truly efficient UPKE candidates (which rely on the random oracle idealization) only provide rather weak security guarantees against passive adversaries as they are malleable. Also, they offer no protection against malicious senders willing to hinder the decryption capability of honest users. A recent work of Dodis et al. (TCC'21) described UPKE systems in the standard model that also hedge against maliciously generated update messages in the chosen-ciphertext setting (where adversaries are equipped with a decryption oracle). While important feasibility results, their constructions lag behind random-oracle candidates in terms of efficiency. In this work, we first provide a drastically more efficient UPKE realization in the standard model using Paillier's Composite Residuosity (DCR) assumption. In the random oracle model, we then extend our initial scheme so as to achieve chosen-ciphertext security, even in a model that accounts for maliciously generated update ciphertexts. Under the DCR and Strong RSA assumptions, we thus obtain the first practical UPKE systems that satisfy the strongest security notions. This work was published in the proceedings of ACM CCS 2022 [7].

7.3.4 New and Improved Constructions for Partially Equivocable Public Key Encryption

Non-committing encryption (NCE) is an advanced form of public-key encryption which guarantees the security of a Multi-Party Computation (MPC) protocol in the presence of an adaptive adversary. Brakerski et al. (TCC 2020) recently proposed an intermediate notion, termed Packed Encryption with Partial Equivocality (PEPE), which implies NCE and preserves the ciphertext rate (up to a constant factor). In this

work, we propose three new constructions of rate-1 PEPE based on standard assumptions. In particular, we obtain the first constant ciphertext-rate NCE construction from the LWE assumption with polynomial modulus, and from the Subgroup Decision assumption. We also propose an alternative DDH-based construction with guaranteed polynomial running time. This work was published in the proceedings of SCN 2022 [18].

7.3.5 Cumulatively All-Lossy-But-One Trapdoor Functions from Standard Assumptions

Chakraborty, Prabhakaran, and Wichs (PKC'20) recently introduced a new tag-based variant of lossy trapdoor functions, termed cumulatively all-lossy-but-one trapdoor functions (CALBO-TDFs). Informally, CALBO-TDFs allow defining a public tag-based function with a (computationally hidden) special tag, such that the function is lossy for all tags except when the special secret tag is used. In the latter case, the function becomes injective and efficiently invertible using a secret trapdoor. This notion has been used to obtain advanced constructions of signatures with strong guarantees against leakage and tampering, and also by Dodis, Vaikunthanathan, and Wichs (EUROCRYPT'20) to obtain constructions of randomness extractors with extractor-dependent sources. While these applications are motivated by practical considerations, the only known instantiation of CALBO-TDFs so far relies on the existence of indistinguishability obfuscation. In this paper, we propose the first two instantiations of CALBO-TDFs based on standard assumptions. Our constructions are based on the LWE assumption with a sub-exponential approximation factor and on the DCR assumption, respectively, and circumvent the use of indistinguishability obfuscation by relying on lossy modes and trapdoor mechanisms enabled by these assumptions. This work was published in the proceedings of SCN 2022 and is invited in a special issue of the Information and Computation journal [17].

7.3.6 On Rejection Sampling in Lyubashevsky's Signature Scheme

Lyubashevsky's signatures are based on the Fiat-Shamir with aborts paradigm, whose central ingredient is the use of rejection sampling to transform secret-dependent signature samples into samples from (or close to) a secret-independent target distribution. Several choices for the underlying distributions and for the rejection sampling strategy can be considered. In this work, we study Lyubashevsky's signatures through the lens of rejection sampling, and aim to minimize signature size given signing runtime requirements. Several of our results concern rejection sampling itself and could have other applications. We prove lower bounds for compactness of signatures given signing runtime requirements, and for expected runtime of perfect rejection sampling strategies. We also propose a Rényi-divergence-based analysis of Lyubashevsky's signatures which allows for larger deviations from the target distribution, and show hyperball uniforms to be a good choice of distributions: they asymptotically reach our compactness lower bounds and offer interesting features for practical deployment. Finally, we propose a different rejection sampling strategy which circumvents the expected runtime lower bound and provides a worst-case runtime guarantee. This work was published as [13], in the proceedings of Asiacrypt 2022.

7.3.7 PointProofs, Revisited

Vector commitments allow a user to commit to a vector of length n using a constant-size commitment while being able to locally open the commitment to individual vector coordinates. Importantly, the size of position-wise openings should be independent of the dimension n. Gorbunov, Reyzin, Wee, and Zhang recently proposed PointProofs (CCS 2020), a vector commitment scheme that supports non-interactive aggregation of proofs across multiple commitments, allowing to drastically reduce the cost of block propagation in blockchain smart contracts. Gorbunov *et al.* provide a security analysis combining the algebraic group model and the random oracle model, under the weak n-bilinear Diffie-Hellman Exponent assumption (n-wBDHE) assumption. In this work, we propose a novel analysis that does not rely on the algebraic group model. We prove the security in the random oracle model under the n-Diffie-Hellman Exponent (n-DHE) assumption, which is implied by the n-wBDHE assumption considered by Gorbunov *et al.* We further note that we do not modify their scheme (and thus preserve its efficiency) nor introduce any additional assumption. Instead, we prove the security of the scheme as it is via a strictly improved analysis. This work was published in the proceedings of Asiacrypt 2022 [19].

7.3.8 On Module Unique-SVP and NTRU

The NTRU problem can be viewed as an instance of finding a short non-zero vector in a lattice, under the promise that it contains an exceptionally short vector. Further, the lattice under scope has the structure of a rank-2 module over the ring of integers of a number field. Let us refer to this problem as the module unique Shortest Vector Problem,or mod-uSVP for short. We exhibit two reductions that together provide evidence the NTRU problem is not just a particular case of mod-uSVP, but representative of it from a computational perspective.

First, we reduce worst-case mod-uSVP to worst-case NTRU. For this, we rely on an oracle for id-SVP, the problem of finding short non-zero vectors in ideal lattices. Using the worst-case id-SVP to worst-case NTRU reduction from Pellet-Mary and Stehlé [ASIACRYPT'21],this shows that worst-case NTRU is equivalent to worst-case mod-uSVP.

Second, we give a random self-reduction for mod-uSVP. We put forward a distribution D over mod-uSVP instances such that solving mod-uSVP with a non-negligible probability for samples from D allows to solve mod-uSVP in the worst-case. With the first result, this gives a reduction from worst-case mod-uSVP to an average-case version of NTRU where the NTRU instance distribution is inherited from D. This worst-case to average-case reduction requires an oracle for id-SVP.

This work appeared in the proceedings of the Asiacrypt'22 conference [15].

7.3.9 Practical, Round-optimal Lattice-based Blind Signatures

Blind signatures are a fundamental cryptographic primitive with numerous practical applications. While there exist many practical blind signatures from number-theoretic assumptions, the situation is far less satisfactory from post-quantum assumptions. In this work, we provide the first overall practical, lattice-based blind signature, supporting an unbounded number of signature queries and additionally enjoying optimal round complexity. We provide a detailed estimate of parameters achieved – we obtain a signature of size slightly above 45KB, for a core-SVP hardness of 109 bits. The run-times of the signer, user and verifier are also very small.

Our scheme relies on the Gentry, Peikert and Vaikuntanathan signature [STOC'08] and non-interactive zero-knowledge proofs for linear relations with small unknowns, which are significantly more efficient than their general purpose counterparts. Its security stems from a new and arguably natural assumption which we introduce, called the one-more-ISIS assumption. This assumption can be seen as a lattice analogue of the one-more-RSA assumption by Bellare et al [JoC'03]. To gain confidence in our assumption, we provide a detailed analysis of diverse attack strategies.

This work appeared in the proceedings of the CCS'22 conference [8].

7.3.10 Round-optimal Lattice-based Threshold Signatures, Revisited

Threshold signature schemes enable distribution of the signature issuing capability to multiple users, to mitigate the threat of signing key compromise. Though a classic primitive, these signatures have witnessed a surge of interest in recent times due to relevance to modern applications like blockchains and cryptocurrencies. In this work, we study round-optimal threshold signatures in the post-quantum regime and improve the only known lattice-based construction by Boneh et al [CRYPTO'18] in terms of asymptotic efficiency, instantiation efficiency, and security (the new scheme achieves a relaxed version of adaptive security).

This work appeared in the proceedings of the ICALP'22 conference [9].

7.3.11 Towards Globally Optimized Hybrid Homomorphic Encryption - Featuring the Elisabeth Stream Cipher

Hybrid Homomorphic Encryption (HHE) reduces the amount of computation client-side and bandwidth usage in a Fully Homomorphic Encryption (FHE) framework. HHE requires the usage of specific sym- metric schemes that can be evaluated homomorphically efficiently. In this paper, we introduce the paradigm of Group Filter Permutator (GFP) as a generalization of the Improved Filter Permutator paradigm introduced by M 'eaux et al. From this paradigm, we specify Elisabeth , a family of stream cipher and give an instance: Elisabeth-4 . After proving the security of this scheme, we provide a Rust

implementation of it and ensure its performance is comparable to state-of-the-art HHE. The true strength of Elisabeth lies in the available opera- tions server-side: while the best HHE applications were limited to a few multiplications server-side, we used data sent through Elisabeth-4 to homomorphically evaluate a neural network inference. Finally, we discuss the improvement and loss between the HHE and the FHE framework and give ideas to build more efficient schemes from the Elisabeth family

This work appeared in the proceedings of the Asiacrypt'22 conference [12].

7.4 Algebraic Computing and High-performance Kernels

7.4.1 Absolute root separation

The absolute separation of a polynomial is the minimum nonzero difference between the absolute values of its roots. In the case of polynomials with integer coefficients, it can be bounded from below in terms of the degree and the height (the maximum absolute value of the coefficients) of the polynomial. We improve the known bounds for this problem and related ones. Then we report on extensive experiments in low degrees, suggesting that the current bounds are still very pessimistic. [2]

7.4.2 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. [21]

7.4.3 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. [1]

7.4.4 Resultant of bivariate polynomials

We present a new algorithm for computing the resultant of two "sufficiently generic" bivariate polynomials over an arbitrary field $\mathbb{K}$. For such p and q in $\mathbb{K}[x,y]$ 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 Neiger et al. 2021 for the related problems of modular composition and characteristic polynomial in a univariate quotient algebra. This further 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 $d = O(n^{0.47})$.

The resultant is the determinant of the associated univariate polynomial Sylvester matrix of degree d, the problem is therefore intimately related to that of computing determinants of structured polynomial matrices. We first identify new advanced aspects of structure specific to the polynomial Sylvester matrix. Thanks to this, our contribution is to compute the determinant by successfully mixing the block baby steps/giant steps approach of Kaltofen and Villard 2005, until then restricted to the case $d = 1$ for characteristic polynomials, and the high-order lifting strategy of Storjohann 2003 usually reserved for dense polynomial matrices. [24]

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

Bosch (Germany) ordered from us some support for the design and implementation of the tanh function in fixed-point and floating-point arithmetics (choice of formats and parameters, possibility of various compromises speed/accuracy/range depending on application needs, etc.)

Participants: Claude-Pierre Jeannerod, 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

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

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

Duration: 2022-2024.

Coordinators: Éric Schost (PI Waterloo), Gilles Villard (PI AriC).

Partners: University of Waterloo (Ontario, Canada) and AriC project-team (Laboratoire LIP).

Summary: The Symbolic Computation Group at Waterloo and the AriC project team expand already established collaborations, in order to design and implement algorithms for linear and non-linear symbolic algebra.

9.2 International research visitors

9.2.1 Visits of international scientists

Inria International Chair

Participants: 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.

Other international visits to the team

Hyeongmin Choe

Status PhD student

Institution of origin: Seoul National University

Country: Korea

Dates: Sept. 5th to Oct. 31st

9.3 European initiatives

9.3.1 H2020 projects

H2020 Project PROMETHEUS

Participants: Benoît Libert, Damien Stehlé, Amit Deo, Fabrice Mouhartem, Octavie Paris.

PROMETHEUS is a project over 54 months that ended in June 2022. The goal is to develop a toolbox of privacy-preserving cryptographic algorithms and protocols (like group signatures, anonymous credentials, or digital cash systems) that resist quantum adversaries. Solutions are mainly considered in the context of Euclidean lattices and analyzed from a theoretical point of view (i.e., from a provable security aspect) and a practical angle (which covers the security of cryptographic implementations and side-channel leakages). Orange is the scientific leader and Benoît Libert is the administrative responsible on behalf of ENS de Lyon.

9.4 National initiatives

9.4.1 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).

9.4.2 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.

9.4.3 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.

9.4.4 ANR CHARM Project

Participant: 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.

9.4.5 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.

9.4.6 ANR NuSCAP Project

Participant: 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.

9.4.7 ANR/Astrid AMIRAL Project

Participant: 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.

10 Dissemination

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

Member of the organizing committees

- Nathalie Revol served in the organizing committee of the minisymposium on "Calcul numérique certifié" at Canum 2022.

10.1.2 Scientific events: selection

Member of conference program committees

- Jean-Michel Muller served in the program committee of Arith 2022.
- Alain Passelègue served in the program committee of Asiacrypt 2022.
- Nathalie Revol served in the program committee of Arith 2022, and of the minisymposium on Interval Methods at PPAM 2022.
- Damien Stehlé served in the program committees of Asiacrypt 2022 and PQCrypto 2022.

10.1.3 Journal

Member of editorial boards

- Jean-Michel Muller is Associate Editor in Chief of IEEE Transactions on Emerging Topics in Computing.
- Nathalie Revol is an associate editor of IEEE Transactions on Computers.
- Bruno Salvy is an editor of the “Journal of Symbolic Computation”, of “Annals of Combinatorics” and of the collection “Text and Monographs in Symbolic Computation” (Springer).
- Damien Stehlé is an editor of the “Designs, Codes and Cryptography” and of the “Journal of Cryptology”.

10.1.4 Invited talks

- Jean-Michel Muller gave an invited talk at the SIAM PP22 Minisymposium on understanding and exploiting mixed-precision accelerators for high-performance computing (held virtual because of the Covid Pandemic), Feb. 24-25, 2022.

- Nathalie Revol gave an invited talk at SWIM 2022, Hanover, Germany.

- Damien Stehlé gave an invited talk at Asiacrypt 2022, Taipei, Taiwan. He was also invited to give a virtual talk as part of the Qualcomm academic lectures. He gave a long talk at the ICMS "Workshop on Foundations and Applications of Lattice-based Cryptography" which took place in July in Edinburgh, UK. Finally, he gave a 8-hour lecture on lattice-based cryptography at the IACR-VIASM summer school on cryptography, which took place in August in Hanoi, Vietnam.

- Claude-Pierre Jeannerod gave an invited talk at the minisymposium "Calcul numérique certifié" of Congrès d'Analyse Numérique (CANUM), Évian-les-Bains, June 2022.

10.1.5 Leadership within the scientific community

- Jean-Michel Muller is a member of the steering committee of the conference Arith.

- Alain Passelègue is a member of the board of directors of GT-C2 of GDR-IM. He is also a member of the scientific committee of the GT-C2 seminar.

- Nathalie Revol is a member of the steering committee of the conference Arith; she is a member of the board of GDR Calcul; she is a member of the IEEE-MSC committee.

- Bruno Salvy is chair of the steering committee of the conference AofA.

- As General Chair of Eurocrypt 2023, Damien Stehlé is automatically member of the board of the International Association for Cryptologic Research (IACR).

10.1.6 Scientific expertise

- Nicolas Brisebarre is a member of the scientific council of "Journées Nationales de Calcul Formel".

- Jean-Michel Muller is a member of the Scientific Council of CERFACS.

- Jean-Michel Muller chaired the evaluation committee of LIS laboratory (Marseille, December 2022), and was a member of the evaluation committee of Icube Laboratory (Strasbourg, October 2022).

- Nathalie Revol was an expert for the "Horizon Europe" programme of the European commission.

- Bruno Salvy is a member of the scientific councils of the CIRM, Luminy and of the GDR Informatique Mathématique of the CNRS.

- Claude-Pierre Jeannerod is a member of "Comité des Moyens Incitatifs" of the Lyon Inria research center.

10.1.7 Research administration

- Jean-Michel Muller is co-chair of the GDR Informatique Mathématique of CNRS.

- Jean-Michel Muller is a member of CAP (Commission Administrative Paritaire) *Directeurs de recherche* of CNRS.

10.2 Teaching - Supervision - Juries

10.2.1 Teaching

Master: Claude-Pierre Jeannerod, Floating-Point Arithmetic and beyond, 2h in 2022, M2, ENS de Lyon, France

Master: Claude-Pierre Jeannerod, Computer Algebra, 30h in 2022, 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 2022, 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", 10h in 2022 (twice), 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 Supervision

- Calvin Abou-Haidar (PhD student), supervised by Alain Passelègue and Damien Stehlé.
- Orel Cosseron (PhD student), supervised by Duong Hieu Phan and Damien Stehlé.
- Julien Devevey (PhD student), supervised by Damien Stehlé.
- Pouria Fallahpour (PhD student), supervised by Damien Stehlé.
- Joël Felderhoff (PhD student), supervised by Guillaume Hanrot and Damien Stehlé.
- Antoine Gonon (PhD student), supervised by Nicolas Brisebarre, Rémi Gribonval and Elisa Riccietti.
- Alaa Ibrahim (PhD student), supervised by Alin Bostan, Mohab Safey el Din and Bruno Salvy.
- Dimitri Koshelev (PostDoc), supervised by Damien Stehlé.
- Mahshid Riahinia (PhD student), supervised by Alain Passelègue and Damien Stehlé.
- Hippolyte Signargout (PhD student), supervised by Clément Pernet (UGA) and Gilles Villard.

10.2.3 Juries

- Jean-Michel Muller was a member of the recruiting committee for a full professor position in Grenoble Alpes University in June 2022.
- Jean-Michel Muller was a member of the Habilitation Committee of Pablo de Oliveira Castro (Paris-Saclay University, Oct. 2022).
- Nathalie Revol was a member of the jury for CAPES NSI (written and oral examinations for high-school teachers in computer science). She was a member of "Comité de suivi de thèse" of Wassim Seifeddine (LS2N, U. Nantes).
- Damien Stehlé was a member of the recruiting committee for a full professor position at ENSIMAG.
- Damien Stehlé was an examiner in the PhD juries of Koen de Boer (U. Leiden, Netherlands) and Agnese Gini (U. Luxembourg, Luxembourg). He was a reviewer of the PhD of Alessandro Budroni (U. Bergen, Norway).

10.3 Popularization

10.3.1 Internal or external Inria responsibilities

- Nathalie Revol is the scientific editor of the website Interstices for the dissemination of computer science to a large audience, with 30 publications and close to half a million visits in 2022. In particular a video on the SIR model in epidemiology has been elaborated.
- Nathalie Revol organized the visit of the LIP laboratory for 3 groups of 15 high-schools girls each, for Women's Day on March 8. With Natacha Portier, she organized a "Filles and maths-info" day in November in Lyon, for over 80 high-school girls.
- Nathalie Revol is a member of the Inria committee on Gender Equality and Equal Opportunities, working in 2021-2022 on recommendations for a better inclusion of LGBTI+ collaborators. She co-chaired the parity committee of the LIP laboratory with Bora Uçar.
- Nathalie Revol was a member of the jury of the "Octet video" competition organized by SIF.
- Nathalie Revol was a member of the committee designing the future exhibition at MMI (Maison des Mathématiques et de l'Informatique) of Lyon.
- Nathalie Revol was the patroness of the "WiFilles" action towards high-school girls, organized by Pierre-Bénite and Saint-Genis-Laval city councils.

10.3.2 Articles and contents

- Paolo Montuschi (Politecnico di Torino), Florent de Dinechin (Emeraude team) and Jean-Michel Muller wrote a short paper for the COMPUTER magazine explaining the current trends in computer arithmetic [4].
- Damien Stehlé was interviewed for an article in "La Recherche" that appeared on January 4, on the unfounded Intellectual Property claims by CNRS on the Kyber submission to the NIST post-quantum standardization project. He was interviewed for an article in "Sciences et Avenir" that appeared on March 28, on post-quantum cryptography. Following the selection by NIST of the Kyber key exchange mechanism and Dilithium signature scheme, he was interviewed for Le Monde (July 7) and La Recherche (July 13). He was also interviewed by the Maeil (the main business newspaper in South Korea) for an article on post-quantum cryptography that appeared on August 4, and in Vietnamnet (one of the main newspapers in Vietnam) for an artice that appeared on August 24.

10.3.3 Interventions

- Joël Felderhoff made several interventions in the framework of "Math en Jeans" activities. This consisted in presenting computer science and mathematical research to middle high school students and was organized with the collège Jean Perrin and the collège La Tourette, in Lyon. Joël Felderhoff proposed activities about error correcting codes, compression and cryptography.
- Joël Felderhoff and Nathalie Revol went to collège Giono, Saint-Genis-Laval, during 3 half-days, for unplugged activities on robotics, informagics, and cryptography with 30 pupils.
- Jean-Michel Muller gave a keynote LIMOS talk in Clermont-Ferrand (Sept. 2022).
- Alain Passelègue talked about modern cryptography in a middle school in Lagnieux for one morning in the context of an annual project of the school about Alan Turing.
- Alain Passelègue hosted participants of the Alkindy competition for one afternoon at ENS Lyon about research in computer science. Joël Felderhoff and Nathalie Revol also gave talks for the participants.
- Nathalie Revol gave talks at a "Filles et Maths-Info" days in Lyon and St-Étienne, each time for 80 high-school girls, and during "Girls Can Code" summer camp for 25 high-school girls, as an incentive to choose scientific careers.
- Nathalie Revol went to lycée La Martinière Montplaisir for "Chiche!" talks: 8 sessions of 2 hours each, around 120 pupils in total.
- Nathalie Revol helped run the Inria booth about the dissemination of computer science towards a large, familial audience, during the "Femmes en Sciences" conference at Cité des Sciences.
- Nathalie Revol gave a talk during the MixIt event about the content and goals of the "Filles & maths-info" days; she took part to a round table about the dissemination of computer science during the SIF annual congress.
- Damien Stehlé gave a talk during the job fair days of ISFA, Lyon.
- Damien Stehlé gave a talk for the opening of the CODEGATE hacking competition in Seoul.

11 Scientific production

11.1 Publications of the year

International journals

[1] N. Brisebarre and B. Salvy. 'Differential-Difference Properties of Hypergeometric Series'. In: *Proceedings of the American Mathematical Society* (2022). URL: https://hal.inria.fr/hal-03712632.

[2] Y. Bugeaud, A. Dujella, W. Fang, T. Pejković and B. Salvy. 'Absolute root separation'. In: *Experimental Mathematics* 31.3 (2022), pp. 805–812. DOI: 10.1080/10586458.2019.1699480. URL: https://hal.archives-ouvertes.fr/hal-02185594.

[3] 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* (25th Oct. 2022). URL: https://hal.science/hal-03482567.

[4] P. Montuschi, J.-M. Muller and F. de Dinechin. 'Computer Arithmetic: Continuing a Long and Steady Emergence'. In: *Computer* 55.10 (Oct. 2022), pp. 4–6. DOI: 10.1109/MC.2022.3193206. URL: https://hal.archives-ouvertes.fr/hal-03806577.

[5] J.-M. Muller and L. Rideau. 'Formalization of double-word arithmetic, and comments on "Tight and rigorous error bounds for basic building blocks of double-word arithmetic"'. In: *ACM Transactions on Mathematical Software* 48.1 (Mar. 2022), pp. 1–24. DOI: 10.1145/3484514. URL: https://hal.science/hal-02972245.

[6] N. Revol. 'Affine Iterations and Wrapping Effect: Various Approaches'. In: *Acta Cybernetica* (2022). URL: https://hal.inria.fr/hal-03505854.

International peer-reviewed conferences

[7] C. Abou Haidar, B. Libert and A. Passelègue. 'Updatable Public Key Encryption from DCR: Efficient Constructions With Stronger Security'. In: ACM Conference on Computer and Communications Security (ACM-CCS) 2022. Los Angeles, United States, 7th Nov. 2022. URL: https://hal.inria.fr/hal-03738749.

[8] S. Agrawal, E. Kirshanova, D. Stehlé and A. Yadav. 'Practical, Round-Optimal Lattice-Based Blind Signatures'. In: CCS '22: 2022 ACM SIGSAC Conference on Computer and Communications Security. Los Angeles CA USA, France: ACM, 2022, pp. 39–53. DOI: 10.1145/3548606.3560650. URL: https://hal.inria.fr/hal-03904051.

[9] S. Agrawal, D. Stehlé and A. Yadav. 'Round-optimal lattice-based threshold signatures, revisited'. In: ICALP 2022. Paris, France, 2022. URL: https://hal.inria.fr/hal-03905543.

[10] T. Arrabal, M. Stojanova, I. Guérin Lassous and J. Picot. 'Analyse de la qualité des liens Wi-Fi à partir de données expérimentales'. In: CORES 2022 – 7ème Rencontres Francophones sur la Conception de Protocoles, l'Évaluation de Performance et l'Expérimentation des Réseaux de Communication. Saint-Rémy-Lès-Chevreuse, France, 30th May 2022, pp. 1–4. URL: https://hal.archives-ouvertes.fr/hal-03660891.

[11] C. F. Borges, C.-P. Jeannerod and J.-M. Muller. 'High-level algorithms for correctly-rounded reciprocal square roots'. In: 29th IEEE Symposium on Computer Arithmetic (ARITH 2022). Proceedings of the 29th International Symposium on Computer Arithmetic. Lyon (virtual meeting due to the COVID pandemic), France, 12th Sept. 2022. URL: https://hal.inria.fr/hal-03728088.

[12] O. Cosseron, C. Hoffmann, P. Méaux and F.-X. Standaert. 'Towards Globally Optimized Hybrid Homomorphic Encryption - Featuring the Elisabeth Stream Cipher'. In: ASIACRYPT 2022. Taipei, Taiwan, 2022. URL: https://hal.inria.fr/hal-03905546.

[13] J. Devevey, O. Fawzi, A. Passelègue and D. Stehlé. 'On Rejection Sampling in Lyubashevsky's Signature Scheme'. In: ASIACRYPT 2022 - 28th Annual International Conference on the Theory and Application of Cryptology and Information Security. Taipei, Taiwan, 5th Dec. 2022. URL: https://hal.inria.fr/hal-03911595.

[14] J. Devevey, B. Libert and T. Peters. 'Rational Modular Encoding in the DCR Setting: Non-Interactive Range Proofs and Paillier-Based Naor-Yung in the Standard Model'. In: Public-Key Cryptography (PKC 2022) - 25th IACR International Conference on Practice and Theory of Public-Key Cryptography. Yokohama (devenu virtuel pour cause de COVID), Japan, 8th Mar. 2022. URL: https://hal.inria.fr/hal-03807457.

[15] J. Felderhoff, A. Pellet-Mary and D. Stehlé. 'On Module Unique-SVP and NTRU'. In: Asiacrypt 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security. Taipei, Taiwan, 5th Dec. 2022. URL: https://hal.archives-ouvertes.fr/hal-03789544.

[16] B. Libert, K. Nguyen, T. Peters and M. Yung. 'One-Shot Fiat-Shamir-based NIZK Arguments of Composite Residuosity and Logarithmic-Size Ring Signatures in the Standard Model'. In: Eurocrypt 2022. Vol. 13276. Lecture Notes in Computer Science. Trondheim, Norway: Springer International Publishing, 25th May 2022, pp. 488–519. DOI: 10.1007/978-3-031-07085-3_17. URL: https://hal.inria.fr/hal-03726185.

[17] B. Libert, K. Nguyen and A. Passelègue. 'Cumulatively All-Lossy-But-One Trapdoor Functions from Standard Assumptions'. In: SCN 2022 - Proceedings of the 13th Conference on Security in Communication Networks. Amalfi, Italy, 12th Sept. 2022. URL: https://hal.inria.fr/hal-03820072.

[18] B. Libert, A. Passelègue and M. Riahinia. 'New and Improved Constructions for Partially Equivocable Public Key Encryption'. In: SCN 2022 - 13th Conference on security and cryptography for networks. Amalfi, Italy, 12th Sept. 2022, pp. 1–31. URL: https://hal.inria.fr/hal-03830141.

[19] B. Libert, A. Passelègue and M. Riahinia. 'PointProofs, Revisited'. In: *Asiacrypt 2022*. Asiacrypt 2022 - International Conference on the Theory and Application of Cryptology and Information Security. Taipei, Taiwan, 5th Dec. 2022. URL: https://hal.archives-ouvertes.fr/hal-03903981.

[20] N. Revol, L. Benet, L. Ferranti and S. Zhilin. 'Testing interval arithmetic libraries, including their IEEE-1788 compliance'. In: PPAM 2022. LNCS. Gdansk, Poland, 2022. URL: https://hal.inria.fr/hal-03674743.

Reports & preprints

[21] A. Bostan, T. Rivoal and B. Salvy. *Minimization of differential equations and algebraic values of E-functions*. 7th Sept. 2022. URL: https://hal.archives-ouvertes.fr/hal-03771150.

[22] F. Bréhard, N. Brisebarre, M. Joldeş and W. Tucker. *Efficient and Validated Numerical Evaluation of Abelian Integrals*. 7th Feb. 2022. URL: https://hal.archives-ouvertes.fr/hal-03561096.

[23] A. Gonon, N. Brisebarre, R. Gribonval and E. Riccietti. *Approximation speed of quantized vs. unquantized ReLU neural networks and beyond*. 19th May 2022. URL: https://hal.archives-ouvertes.fr/hal-03672166.

[24] C. Pernet, H. Signargout and G. Villard. *High-order lifting for polynomial Sylvester matrices*. 7th Oct. 2022. URL: https://hal.archives-ouvertes.fr/hal-03740320.

11.2 Other

Scientific popularization

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

Softwares

[26] [SW] T. L. Group, *LinBox* version 1.7.0, 26th Sept. 2022. LIC: GNU Lesser General Public License v2.1 or later. HAL: ⟨hal-03788347⟩, URL: https://hal.archives-ouvertes.fr/hal-03788347, VCS: https://github.com/linbox-team/linbox, SWHID: ⟨swh:1:dir:ab3150274e077cc4c4d18ab7bc074fab0a5c12d3;origin=https://hal.archives-ouvertes.fr/hal-03788347;visit=swh:1:snp:99e4a5b29527e7089567751cd8b75113ecd12c0b;anchor=swh:1:rel:35391e40ce3a7b02180e2dc159c095a89ed26a91;path=/⟩.

[27] [SW] G. Hanrot, P. Zimmermann, V. Lefèvre, P. Pélissier and P. Théveny, *GNU MPFR* version 4.2.0, 6th Jan. 2023. LIC: GNU General Public License. HAL: ⟨hal-03940504⟩, URL: https://hal.inria.fr/hal-03940504, VCS: https://gitlab.inria.fr/mpfr/mpfr, SWHID: ⟨swh:1:rel:b5e308c5dd459a81d8523e1dcb84c19dbc47b51b;origin=https://gitlab.inria.fr/mpfr/mpfr;visit=swh:1:snp:15595615280f9f91d107c1f4e9fa915fda0076dc⟩.

11.3 Cited publications

[28] M. Joldeş, J.-M. Muller and V. Popescu. 'Tight and rigourous error bounds for basic building blocks of double-word arithmetic'. In: *ACM Transactions on Mathematical Software* 44.2 (2017). DOI: 10.1145/3121432.