RESEARCH CENTRE

Grenoble - Rhône-Alpes

IN PARTNERSHIP WITH:

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

2021 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

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, HDR]
- Jean-Michel Muller [CNRS, Senior Researcher, HDR]
- Alain Passelègue [Inria, Researcher]
- Nathalie Revol [Inria, Researcher]
- Gilles Villard [CNRS, Senior Researcher, HDR]

Faculty Members

- Guillaume Hanrot [École Normale Supérieure de Lyon, Professor, HDR]
- Nicolas Louvet [Univ Claude Bernard, Associate Professor]
- Damien Stehlé [École Normale Supérieure de Lyon, Professor, HDR]

Post-Doctoral Fellows

- Rikki Amit Inder Deo [École Normale Supérieure de Lyon, until Jun 2021]
- Alonso Gonzalez [École Normale Supérieure de Lyon]
- Fabrice Mouhartem [École Normale Supérieure de Lyon, from Aug 2021]

PhD Students

- Calvin Abou Haidar [Inria, from Jan 2021]
- Orel Cosseron [Zama Sas, CIFRE]
- Julien Devevey [École Normale Supérieure de Lyon]
- Pouria Fallahpour [École Normale Supérieure de Lyon, from Sep 2021]
- Antoine Gonon [École Normale Supérieure de Lyon, From Sep. 2021]
- Adel Hamdi [Orange Labs, CIFRE, Jan 2021]
- Huyen Nguyen [École Normale Supérieure de Lyon, until Nov 2021]
- Mahshid Riahinia [École Normale Supérieure de Lyon, from Sep 2021]
- Hippolyte Signargout [École Normale Supérieure de Lyon, from Sept. 2020]

Technical Staff

- Joel Felderhoff [École Normale Supérieure de Lyon, Engineer, from Sep 2021]
- Joris Picot [École Normale Supérieure de Lyon, Engineer]

Interns and Apprentices

- Hadrien Brochet [École Normale Supérieure de Lyon, from Feb 2021 until Jun 2021]
- Pouria Fallahpour [École Normale Supérieure de Lyon, from Feb 2021 until Aug 2021]
- Antoine Gonon [École Normale Supérieure de Lyon, From Feb. 2021 to Jul. 2021]
- Emile Martinez [École Normale Supérieure de Lyon, from May 2021 until Jul 2021]
- Ngoc Ky Nguyen [École Normale Supérieure de Lyon, from Mar 2021 until Aug 2021]
- Mahshid Riahinia [École Normale Supérieure de Lyon, from Feb 2021 until Aug 2021]

Administrative Assistants

- Chiraz Benamor [École Normale Supérieure de Lyon]
- Octavie Paris [École Normale Supérieure de Lyon]

External Collaborator

- Fabien Laguillaumie [Univ de Montpellier, until Aug 2021, HDR]

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 $\rightarrow$ numeric), as well actions accelerating exact solutions (symbolic $\leftarrow$ 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

Best paper award at ASIACRYPT 2021. For the article 'On the hardness of the NTRU problem', by Alice Pellet–Mary and Damien Stehlé [13]. More in Section 7.3.5.

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 80 mathematical functions, in addition to utility functions (assignments, conversions...). Special data (Not a Number, infinities, signed zeros) are handled like in the IEEE 754 standard. 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 Lefevre

Participants: Guillaume Hanrot, Paul Zimmermann, Philippe Théveny, Vincent Lefevre

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 Lefevre

Participant: Vincent Lefevre

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

7 New results

7.1 Efficient approximation methods

7.1.1 New results on the Table Maker's Dilemma

Despite several significant advances over the last 30 years, guaranteeing the correctly rounded evaluation of elementary functions, such as cos, exp, $\sqrt[3]{\cdot}$ for instance, is still a difficult issue. This can be formulated as a Diophantine approximation problem, called the Table Maker's Dilemma, which consists in determining points with integer coordinates that are close to a curve. In [16], we propose two algorithmic approaches

to tackle this problem, closely related to a celebrated work by Bombieri and Pila and to the so-called Coppersmith's method. We establish the underlying theoretical foundations, prove the algorithms, study their complexity and present practical experiments; we also compare our approach with previously existing ones. In particular, our results show that the development of a correctly rounded mathematical library for the binary128 format is now possible at a much smaller cost than with previously existing approaches.

7.2 Floating-point and Validated Numerics

7.2.1 Emulating round-to-nearest-ties-to-zero "augmented" floating-point operations using round-to-nearest-ties-to-even arithmetic

The 2019 version of the IEEE 754 Standard for Floating-Point Arithmetic recommends that new "augmented" operations should be provided for the binary formats. These operations use a new "rounding direction": round to nearest ties-to-zero. In collaboration with S. Boldo (Toccata) and C. Lauter (U. Alaska), we show how they can be implemented using the currently available operations, using round-to-nearest ties-to-even with a partial formal proof of correctness [1].

7.2.2 Formalization of double-word arithmetic, and comments on "Tight and rigorous error bounds for basic building blocks of double-word arithmetic"

Recently, a complete set of algorithms for manipulating double-word numbers (some classical, some new) was analyzed[1]. In collaboration with L. Rideau (STAMP), we have formally proven 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 someresults by showing that they are still valid if we slightly change the rounding mode. The consequence is that the algorithms presented in Joldes et al.'s paper 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. [6]

7.2.3 a * (x * x) or (a * x) * x ?

Expressions such as ax^2, axy, or ax^3, where a is a constant, are not unfrequent in computing. There are several ways of parenthesizing them (and therefore, choosing the order of evaluation). Depending on the value of a, is there a more accurate evaluation order? We discuss this point (with a small digression on spurious underflows and overflows). [12]

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 [21], 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.

[1] M. Joldes, J.-M. Muller, and V. Popescu, Tight and rigourous error bounds for basic buiding blocks of double-word arithmetic, ACM Transactions on Mathematical Software, Vol. 44 No 2, October 2017.

7.2.5 Further remarks on Kahan summation with decreasing ordering

In [17], we consider Kahan's compensated summation of n floating-point numbers ordered as $|x_1| \geq \cdots \geq |x_n|$ and show that in IEEE 754 arithmetic the smallest dimension for which a large relative error can occur is $n = 4$. This answers a question raised by Higham and Priest in the early 1990s.

7.3 Lattices: Algorithms and Cryptology

7.3.1 Non-interactive CCA2-Secure Threshold Cryptosystems: Achieving Adaptive Security in the Standard Model Without Pairings

In [8], we considered threshold encryption schemes, where the decryption servers distributively hold the private key shares, and a threshold of these servers should collaborate to decrypt the message (while the system remains secure when less than the threshold is corrupted). We investigated the notion of chosen-ciphertext secure threshold systems which has been historically hard to achieve. We further require the systems to be, both, adaptively secure (i.e., secure against a strong adversary making corruption decisions dynamically during the protocol), and on-interactive (i.e., where decryption servers do not interact amongst themselves but rather efficiently contribute, each, a single message). To date, only pairing-based implementations were known to achieve security in the standard security model without relaxation (i.e., without assuming the random oracle idealization) under the above stringent requirements. We investigate how to achieve the above using other assumptions (in order to understand what other algebraic building blocks and mathematical assumptions are needed to extend the domain of encryption methods achieving the above). Specifically, we show realizations under the Decision Composite Residuosity (DCR) and Learning-With-Errors (LWE) assumption.

7.3.2 Bifurcated Signatures: Folding the Accountability vs. Anonymity Dilemma into a Single Private Signing Scheme

In anonymous credentials and group signature schemes, an orthogonality exists between users' anonymity and their accountability. Usually, the tracing authority can identify the author of any signature. In [11], we suggest an alternative approach where the tracing authority's capability to trace a signature back to its source depends on the signed message. More precisely, the traceability of a signature is determined by a predicate evaluated on the message and the user's identity/credential. At the same time, the schemes provide what we call "branch- hiding;" namely, the resulting predicate value hides from outsiders if a given signature is traceable or not. Specifically, we precisely define and give the first construction and security proof of a "Bifurcated Anonymous Signature" (BiAS): A scheme which supports either absolute anonymity or anonymity with accountability, based on a specific contextual predicate, while being branch-hiding. This novel signing scheme has numerous applications not easily implementable or not considered before, especially because: (i) the conditional traceability does not rely on a trusted authority as it is (non-interactively) encapsulated into signatures; and (ii) signers know the predicate value and can make a conscious choice at each signing time. Technically, we realize BiAS from homomorphic commitments for a general family of predicates that can be represented by bounded-depth circuits. Our construction is generic and can be instantiated in the standard model from lattices and, more efficiently, from bilinear maps. In particular, the signature length is independent of the circuit size when we use commitments with suitable efficiency properties

7.3.3 SO-CCA secure PKE from pairing based all-but-many lossy trapdoor functions

In a selective-opening chosen ciphertext (SO-CCA) attack on a public-key encryption scheme, an adversary has access to a decryption oracle, and after getting a number of ciphertexts, can then adaptively corrupt a subset of them, obtaining the plaintexts and corresponding encryption randomness. SO-CCA security requires the privacy of the remaining plaintexts being well protected. There are two flavors of SO-CCA definition: the weaker indistinguishability-based (IND) and the stronger simulation-based (SIM) ones. In [3], we study SO-CCA secure PKE constructions from all-but-many lossy trapdoor functions (ABM-LTFs) in pairing-friendly prime order groups. Concretely,

- We construct two ABM-LTFs with sublinear-size tags (in the input length), which lead to IND-SO-CCA secure PKEs with ciphertexts comprised of a sublinear number of group elements. In addition, our second ABM-LTF enjoys tight security, so as the resulting PKE.

- By equipping a lattice trapdoor for opening randomness, we show our ABM-LTFs are SIM-SO-CCA compatible.

7.3.4 Adaptively secure distributed PRFs from LWE

In distributed pseudorandom functions (DPRFs), a PRF secret key SK is secret shared among N servers so that each server can locally compute a partial evaluation of the PRF on some input X. A combiner that collects t partial evaluations can then reconstruct the evaluation $F(SK, X)$ of the PRF under the initial secret key. So far, all non-interactive constructions in the standard model are based on lattice assumptions. One caveat is that they are only known to be secure in the static corruption setting, where the adversary chooses the servers to corrupt at the very beginning of the game, before any evaluation query. In [4], we construct the first fully non-interactive adaptively secure DPRF in the standard model. Our construction is proved secure under the LWE assumption against adversaries that may adaptively decide which servers they want to corrupt. We also extend our construction in order to achieve robustness against malicious adversaries.

7.3.5 On the hardness of the NTRU problem

The 25 year-old NTRU problem is an important computational assumption in public-key cryptography. However, from a reduction perspective, its relative hardness compared to other problems on Euclidean lattices is not well-understood. Its decision version reduces to the search Ring-LWE problem, but this only provides a hardness upper bound. In [13], we provide two answers to the long-standing open problem of providing reduction-based evidence of the hardness of the NTRU problem. First, we reduce the worst-case approximate Shortest Vector Problem over ideal lattices to an average-case search variant of the NTRU problem. Second, we reduce another average-case search variant of the NTRU problem to the decision NTRU problem.

7.3.6 On the Integer Polynomial Learning with Errors Problem

Several recent proposals of efficient public-key encryption are based on variants of the polynomial learning with errors problem (PLWE$_f$) in which the underlying polynomial ring $Z_q[x]/f$ is replaced with the (related) modular integer ring $Z_{f(q)}$; the corresponding problem is known as Integer Polynomial Learning with Errors (I-PLWE$_f$). Cryptosystems based on I-PLWE$_f$ and its variants can exploit optimised big-integer arithmetic to achieve good practical performance, as exhibited by the ThreeBears cryptosystem. Unfortunately, the average-case hardness of I-PLWE$_f$ and its relation to more established lattice problems have to date remained unclear.

In [9], we describe the first polynomial-time average-case reductions for the search variant of I-PLWE$_f$, proving its computational equivalence with the search variant of its counterpart problem PLWE$_f$. Our reductions apply to a large class of defining polynomials f. To obtain our results, we employ a careful adaptation of Rényi divergence analysis techniques to bound the impact of the integer ring arithmetic carries on the error distributions. As an application, we present a deterministic public-key cryptosystem over integer rings. Our cryptosystem, which resembles ThreeBears, enjoys one-way (OW-CPA) security provably based on the search variant of I-PLWE$_f$.

7.3.7 An Anonymous Trace-and-Revoke Broadcast Encryption Scheme

Broadcast Encryption is a fundamental cryptographic primitive, that gives the ability to send a secure message to any chosen target set among registered users. In this work, we investigate broadcast encryption with anonymous revocation, in which ciphertexts do not reveal any information on which users have been revoked. We provide a scheme whose ciphertext size grows linearly with the number of revoked users. Moreover, our system also achieves traceability in the black-box confirmation model.

In [7], our contribution is threefold. First, we develop a generic transformation of linear functional encryption toward trace-and-revoke systems. It is inspired from the transformation by Agrawal et al. (CCS'17) with the novelty of achieving anonymity. Our second contribution is to instantiate the underlying linear functional encryptions from standard assumptions. We propose a DDH-based (Decision Diffie-Hellman) construction which does no longer require discrete logarithm evaluation during the decryption and thus significantly improves the performance compared to the DDH-based construction of Agrawal et al.. In the LWE-based setting, we tried to instantiate our construction by relying on the scheme from Wang et al. (PKC'19) but finally found an attack to this scheme. Our third contribution is to extend the 1-bit encryption from the generic transformation to n-bit encryption. By introducing matrix multiplication functional encryption, which essentially performs a fixed number of parallel calls on functional encryptions with the same randomness, we can prove the security of the final scheme with a tight reduction that does not depend on n, in contrast to employing the hybrid argument.

7.3.8 Non-applicability of the Gaborit and Aguilar-Melchor patent to Kyber and Saber

In the context of the NIST post-quantum cryptography project, there have been claims that the Gaborit and Aguilar-Melchor patent could apply to the Kyber and Saber encryption schemes. In [19], we argue that these claims are in contradiction with the potential validity of the patent.

This short note was complemented by a post on the post-quantum standardisation mailing list, which provided recommendations regarding how to proceed towards post-quantum standardisation in light of the scientifically baseless patent claims from CNRS on the Kyber and Saber submissions.

7.3.9 Fully-succinct Publicly Verifiable Delegation from Constant-Size Assumptions

In [10], we construct a publicly verifiable, non-interactive delegation scheme for any polynomial-size arithmetic circuit with proof-size and verification complexity comparable to those of pairing-based zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKS). Concretely, the proof consists of a constant number of group elements and verification requires $O(1)$ pairings and n group exponentiations, where n is the size of the input. While known SNARK-based constructions rely on non-falsifiable assumptions, our construction can be proven sound under any constant-size Matrix Diffie-Hellman assumption. However, the size of the reference string as well as the prover's complexity are quadratic in the size of the circuit. This result demonstrates that we can construct delegation from very simple and well-understood assumptions. We consider this work a first step towards achieving practical delegation from standard, falsifiable assumptions. Our main technical contributions are first, the introduction and construction of what we call "no-signaling, somewhere statistically binding" commitment schemes. Second, we use these commitments to construct more efficient "quasi-arguments" with no-signaling extraction, introduced by Paneth and Rothblum (TCC'17). These arguments allow extracting parts of the witness of a statement and checking it against some local constraints without revealing which part is checked. We construct pairing-based quasi arguments for linear and quadratic constraints and combine them with the low-depth delegation result of González et. al. (Asiacrypt'19) to construct the final delegation scheme.

7.4 Algebraic Computing and High-performance Kernels

7.4.1 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. [20]

7.4.2 Toeplitz, Hankel, and Toeplitz+Hankel matrices

New algorithms are presented for computing annihilating polynomials of Toeplitz, Hankel, and more generally Toeplitz+Hankel-like matrices over a field. Our approach follows works on Coppersmith's block Wiedemann method with structured projections, which have been recently successfully applied for computing the bivariate resultant and for modular composition. In particular, if the displacement rank is considered constant, then we compute the characteristic polynomial of a generic matrix that belongs to one of the classes above in $n^{2-1/\omega+o(1)}$ arithmetic operations, where ω is the exponent of matrix multiplication. Previous algorithms required $O(n^2)$ operations. [14]

7.4.3 Effective Coefficient Asymptotics of Multivariate Rational Functions via Semi-Numerical Algorithms for Polynomial Systems

The coefficient sequences of multivariate rational functions appear in many areas of combinatorics. Their diagonal coefficient sequences enjoy nice arithmetic and asymptotic properties, and the field of analytic combinatorics in several variables (ACSV) makes it possible to compute asymptotic expansions. We consider these methods from the point of view of effectivity. In particular, given a rational function, ACSV requires one to determine a (generically) finite collection of points that are called critical and minimal. Criticality is an algebraic condition, meaning it is well treated by classical methods in computer algebra, while minimality is a semi-algebraic condition describing points on the boundary of the domain of convergence of a multivariate power series. We show how to obtain dominant asymptotics for the diagonal coefficient sequence of multivariate rational functions under some genericity assumptions using symbolic-numeric techniques. To our knowledge, this is the first completely automatic treatment and complexity analysis for the asymptotic enumeration of rational functions in an arbitrary number of variables. [5]

7.4.4 Explicit degree bounds for right factors of linear differential operators

If a linear differential operator with rational function coefficients is reducible, its factors may have coefficients with numerators and denominators of very high degree. We give a completely explicit bound for the degrees of the (monic) right factors in terms of the degree and the order of the original operator, as well as the largest modulus of the local exponents at all its singularities, for which bounds are known in terms of the degree, the order and the height of the original operator. [2]

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 trigonometric functions in fixed-point and floating-point arithmetics (choice of formats and parameters, possibility of various compromises speed/accuracy/range depending on application needs, etc.)

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

8.2 Bilateral grants with industry

- Orel Cosseron is doing his PhD with Zama SAS and is supervised by Damien Stehlé. He is working on fully homomorphic encryption.

9 Partnerships and cooperations

9.1 International research visitors

9.1.1 Visits of international scientists

Inria International Chair

IIC TUCKER Warwick

Name of the chair: Warwick Tucker

Institution of origin: Monash University

Country: Australia

Dates: From Mon Jan 01 2018 to Sat Dec 31 2022

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.

9.2 European initiatives

9.2.1 FP7 & H2020 projects

H2020 Project PROMETHEUS

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

PROMETHEUS is a project over 54 months ending 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.

9.3 National initiatives

9.3.1 ANR ALAMBIC Project

Participant: Benoît Libert, Fabien Laguillaumie, Alonso Gonzalez.

ALAMBIC is a project (started in October 2016 and ending in April 2022) focused on the applications of cryptographic primitives with homomorphic or malleability properties. The project received a 6-month extension due to the COVID crisis and now ends in April 2021. The web page of the project is https://crypto.di.ens.fr/projects:alambic:description. It is headed by Damien Vergnaud (ENS Paris and CASCADE team) and, besides AriC, also involves teams from the XLIM laboratory (Université de Limoges) and the CASCADE team (ENS Paris). The main goals of the project are: (i) Leveraging the applications of malleable cryptographic primitives in the design of advanced cryptographic protocols which require

computations on encrypted data; (ii) Enabling the secure delegation of expensive computations to remote servers in the cloud by using malleable cryptographic primitives; (iii) Designing more powerful zero-knowledge proof systems based on malleable cryptography.

9.3.2 RISQ Project

Participant: Rikki Amit Inder Deo, Fabien Laguillaumie, Benoît Libert, Damien Stehlé.

RISQ (Regroupement de l'Industrie française pour la Sécurité Post – Quantique) is a BPI-DGE four-year project (started in January 2017) focused on the transfer of post-quantum cryptography from academia to industrial poducts. The web page of the project is http://risq.fr. It is headed by Secure-IC and, besides AriC, also involves teams from ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), Airbus, C& S (Communication et Systèmes), CEA (CEA-List), CryptoExperts, Gemalto, Orange, Thales Communications & Security, Paris Center for Quantum Computing, the EMSEC team of IRISA, and the Cascade and Polsys INRIA teams. The outcome of this project will include an exhaustive encryption and transaction signature product line, as well as an adaptation of the TLS protocol. Hardware and software cryptographic solutions meeting these constraints in terms of security and embedded integration will also be included. Furthermore, documents guiding industrials on the integration of these post-quantum technologies into complex systems (defense, cloud, identity and payment markets) will be produced, as well as reports on the activities of standardization committees.

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. The web page of the project is https://perso.ens-lyon.fr/alain.passelegue/projects.html. 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.

9.3.4 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. The web page of the project is https://github.com/CHARM-project/charm-project.github.io. 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.

9.3.5 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. The web page of the project is https://nuscap.gitlabpages.inria.fr/. 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.

9.3.6 ANR/Astrid AMIRAL Project

Participant: Benoît Libert, , 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. The web page of the project is https://perso.ens-lyon.fr/alain.passelegue/projects.html. 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: selection

Member of conference program committees

- Benoît Libert was a program committee member for Eurocrypt 2021, CT-RSA 2021, TCC 2021, PKC 2022
- Damien Stehlé was a program committee member for PQCrypto 2021
- Jean-Michel Muller and Nathalie Revol were program committee members for ARITH 2021

10.1.2 Journal

Member of editorial boards

- 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 "Journal of Cryptology" and of "Designs, Codes and Cryptography".
- Jean-Michel Muller is associate editor in chief of the IEEE Transactions on Emerging Topics in Computing.
- Nathalie Revol is an editor of "Reliable Computing".
- Gilles Villard is an editor of the "Journal of Symbolic Computation".

10.1.3 Invited talks

Alain Passelègue gave an invited talk about contact tracing apps during the Journées Nationales du GDR Sécurité.

Damien Stehlé gave an invited talk on the cryptographic aspects of module lattices, at the PQCRYPTO 2021 conference.

Jean-Michel Muller gave an invited talk at the SIAM CSE21 Minisymposium on Reduced Precision Arithmetic and Stochastic Rounding.

Nathalie Revol gave a talk at the International Online Seminar on Interval Methods in Control Engineering.

10.1.4 Leadership within the scientific community

Claude-Pierre Jeannerod was a member of the scientific committee of JNCF (Journées Nationales de Calcul Formel).

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

Damien Stehlé is a member of the steering committee of the PQCRYPTO conference series.

Jean-Michel Muller and Nathalie Revol are members of the steering committee of the ARITH conference series.

Nathalie Revol is a member of the scientific committee of the SCAN conference series.

10.1.5 Scientific expertise

Bruno Salvy is a member of the scientific councils of the CIRM, Luminy and of the GDR Informatique Mathématique of the CNRS. This year, he was in the hiring committee for young researchers of Inria Lyon and in one for a “Maître de conférences” at University Nancy.

Damien Stehlé was in the hiring committees for a “Maître de conférences” position at Sorbonne University and a professor position at ENS Rennes.

Jean-Michel Muller chaired the evaluation committee of LABRI (Laboratoire Bordelais de Recherche en Informatique). He is a member of the Scientific Council of CERFACS (Toulouse).

Nathalie Revol was in the hiring committee for a “Maître de conférences” position at Sorbonne University. She was an expert for the European Commission.

Claude-Pierre Jeannerod was a member of the recruitment committee for postdocs and sabbaticals at Inria Grenoble–Rhône-Alpes. He has been a member of the *Comité des Moyens Incitatifs* for the Lyon Inria research center since October 2021.

Guillaume Hanrot was in the hiring committee for a "Professor" position at Sorbonne University and for two Professor positions (mathematics and economics) at ENS de Lyon. He was also a member of the general hiring committee for positions in computer science at Ecole polytechnique.

Gilles Villard was member of the *Section 6 du Comité national de la recherche scientifique*, 2016-2021.

Vincent Lefèvre participates in the revision of the ISO C standard via the C Floating Point Study Group.

10.1.6 Research administration

Alain Passelègue is a member of the directive board of the GT C2.

Jean-Michel Muller is co-head of GDR IM (Groupement de Recherches Informatique Mathématique).

Jean-Michel Muller is a member of the Commission Administrative Paritaire 1 of CNRS.

Guillaume Hanrot has been head of the Laboratoire d’excellence MILyon since Sept. 1st, 2021.

10.2 Teaching - Supervision - Juries

10.2.1 Teaching

Master: Alain Passelègue, Advanced Topics in Cryptography, 32h, M2, ENS de Lyon, France

Master: Alain Passelègue, Interactive and Non-Interactive Proofs in Complexity and Cryptography, 16h, M2, ENS de Lyon, France

Master: Damien Stehlé, Cryptography, 24h, M1, ENS de Lyon, France

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

Bachelor: Bruno Salvy, Design and Analysis of Algorithms, 20h, École polytechnique, France

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

Postgrad: Nathalie Revol, "Scientific Dissemination and Outreach Activities", 10h in 2021 (twice), 4th year students, ENS de Lyon, France

Master: Claude-Pierre Jeannerod, Floating-Point Arithmetic and beyond, 7h in 2021, M2, ENS de Lyon, France

Master: Claude-Pierre Jeannerod, Computer Algebra, 30h in 2021, 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, 12h in 2021, M2, ISFA, France

10.2.2 Supervision

- Orel Cosseron (PhD student), supervised by Marc Joye, Pascal Paillier and Damien Stehlé
- Julien Devevey (PhD student), supervised by Damien Stehlé and Benoît Libert
- Pouria Fallahpour (PhD student), supervised by Alain Passelègue and Damien Stehlé
- Joël Felderhoff (PhD student), supervised by Damien Stehlé
- Antoine Gonon (PhD student), supervised by Nicolas Brisebarre, Rémi Gribonval and Elisa Riccietti
- Calvin Haidar (PhD student), supervised by Benoît Libert, Alain Passelègue and Damien Stehlé
- Huyen Nguyen (PhD student), supervised by Elena Kirshanova and Damien Stehlé
- Mahshid Riahinia (PhD student), supervised by Benoît Libert and Alain Passelègue
- Hippolyte Signargout (PhD student), supervised by Clément Pernet (LJK, UGA) and Gilles Villard

10.2.3 Juries

- C.-P. Jeannerod was a reviewer ("external examiner") for the PhD thesis of Stavros Birmpilis (University of Waterloo, Canada), September 2021.
- B. Salvy was in the HdR committee of Victor Magron.
- B. Libert was a reviewer for the PhD thesis of Chloé Hébant (ENS Paris), May 2021
- D. Stehlé was a reviewer for the PhD theses of Yixin Shen (U. de Paris) and Eamonn Postlethwaite (Royal Holloway, UK), and a member of the PhD committees of Jan-Pieter D'Anvers (KU Leuven, Belgium) and Carl Bootland (KU Leuven, Belgium)
- J.-M. Muller was a reviewer for the PhD committee of N. Demeure (U. Paris Saclay) and a member of the PhD committee of D. Gallois-Wong (U. Paris Saclay). He was in the HdR committee of W. Steiner (U. de Paris).
- N. Revol was in the PhD committee of Tiago Trevisan Jost (U. Grenoble). She was a member of the jury for CAPES NSI (written and oral examinations for high-school teachers in computer science).
- G. Hanrot was a member of the group in charge of designing the structure of the competitive exam "agrégation d'informatique", and a member of the group in charge of designing the program of this competitive exam.

10.3 Popularization

10.3.1 Internal or external Inria responsibilities

Alain Passelègue was a member of the Inria working group GT Recrutement-Accueil on developping new processes for hiring and welcoming new Inria employees.

Nathalie Revol is a member of the Inria committee on Gender Equality and Equal Opportunities, working in 2021 on recommendations for a better inclusion of LGBTI+ collaborators.

10.3.2 Articles and contents

Damien Stehlé was interviewed for Le Monde, in the context of the baseless patent claims from CNRS on Kyber and Saber ('Quand un brevet perturbe l'innovation post-quantique', 16 November 2021).

Jean-Michel Muller wrote a chapter [15] for a popular science book "De la mesure en toutes choses" published by CNRS editions.

10.3.3 Education

Nicolas Brisebarre was a scientific consultant for « Les maths et moi », a one-man show by Bruno Martins. He also took part to Q & A sessions with the audience after some shows.

Nathalie Revol is the scientific editor of the website Interstices for the dissemination of computer science to a large audience, with 25 publications and more than half a million visits in 2021.

10.3.4 Interventions

Alain Passelègue was a member of the panel discussion on contact tracing during the Journées Nationales du GDR Sécurité.

Damien Stehlé gave an invited talk on post-quantum cryptography at the webinar of the Chey Institute for Advanced Studies.

Damien Stehlé was invited to the Parliamentary Office for the Evaluation of Scientific and Technological Choices (OPECST) for a public hearing on quantum technologies (8 October 2021).

Nathalie Revol gave talks at a "Filles et Maths-Info" day in St-Étienne for 80 high-school girls and at lycée Descartes in St-Genis-Laval for 250 high-school pupils, as an incentive to choose scientific careers, especially for girls.

11 Scientific production

11.1 Publications of the year

International journals

[1] S. Boldo, C. Q. Lauter and J.-M. Muller. 'Emulating round-to-nearest ties-to-zero "augmented" floating-point operations using round-to-nearest ties-to-even arithmetic'. In: *IEEE Transactions on Computers* 70.7 (July 2021), pp. 1046–1058. DOI: 10.1109/TC.2020.3002702. URL: https://hal.archives-ouvertes.fr/hal-02137968.

[2] A. Bostan, T. Rivoal and B. Salvy. 'Explicit degree bounds for right factors of linear differential operators'. In: *Bulletin of the London Mathematical Society* 53.1 (1st Feb. 2021), pp. 53–62. DOI: 10.1112/blms.12396. URL: https://hal.archives-ouvertes.fr/hal-02154679.

[3] D. Jia and B. Libert. 'SO-CCA secure PKE from pairing based all-but-many lossy trapdoor functions'. In: *Designs, Codes and Cryptography* 89.5 (May 2021), pp. 895–923. DOI: 10.1007/s10623-021-00849-9. URL: https://hal.inria.fr/hal-03380672.

[4] B. Libert, D. Stehlé and R. Titiu. 'Adaptively Secure Distributed PRFs from LWE'. In: *Journal of Cryptology* 34.3 (July 2021), pp. 1–46. DOI: 10.1007/s00145-021-09393-0. URL: https://hal.inria.fr/hal-03381388.

[5] S. Melczer and B. Salvy. 'Effective Coefficient Asymptotics of Multivariate Rational Functions via Semi-Numerical Algorithms for Polynomial Systems'. In: *Journal of Symbolic Computation* 103 (2021), pp. 234–279. DOI: 10.1016/j.jsc.2020.01.001. URL: https://hal.archives-ouvertes.fr/hal-02185586.

[6] 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* (2021). URL: https://hal.archives-ouvertes.fr/hal-02972245.

International peer-reviewed conferences

[7] O. Blazy, S. Mukherjee, H. Nguyen, D. Hieu Phan and D. Stehlé. 'An Anonymous Trace-and-Revoke Broadcast Encryption Scheme'. In: ACISP 2021 - Australasian Conference on Information Security and Privacy. Vol. 13083. Lecture Notes in Computer Science. Perth, Australia: Springer International Publishing, 4th Nov. 2021, pp. 214–233. DOI: 10.1007/978-3-030-90567-5_11. URL: https://hal.archives-ouvertes.fr/hal-03475739.

[8] J. Devevey, B. Libert, K. Nguyen, T. Peters and M. Yung. 'Non-Interactive CCA2-Secure Threshold Cryptosystems: Achieving Adaptive Security in the Standard Model Without Pairings'. In: PKC 2021 - 24th edition of the International Conference on Practice and Theory of Public-Key Cryptography. Vol. 12710. LNCS. Edinburgh (devenu virtuel pour cause de COVID), United Kingdom: Springer, 10th May 2021, pp. 1–66. URL: https://hal.inria.fr/hal-03381386.

[9] J. Devevey, A. Sakzad, D. Stehlé and R. Steinfeld. 'On the Integer Polynomial Learning with Errors Problem'. In: PKC 2021 - 24th edition of the International Conference on Practice and Theory of Public-Key Cryptography. Vol. 12710. Lecture Notes in Computer Science. Edinburgh, United Kingdom: Springer International Publishing, 1st May 2021, pp. 184–214. DOI: 10.1007/978-3-030-75245-3_8. URL: https://hal.archives-ouvertes.fr/hal-03475737.

[10] A. González and A. Zacharakis. 'Fully-succinct Publicly Verifiable Delegation from Constant-Size Assumptions'. In: 19th International Conference, TCC 2021. Theory of Cryptography. Raleigh, United States, 4th Nov. 2021, pp. 1–79. URL: https://hal.archives-ouvertes.fr/hal-03419735.

[11] B. Libert, K. Nguyen, T. Peters and M. Yung. 'Bifurcated Signatures: Folding the Accountability vs. Anonymity Dilemma into a Single Private Signing Scheme'. In: Eurocrypt 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 12698. Zagreb (partiellement virtuel), Croatia: Springer, 3rd May 2021, pp. 1–48. URL: https://hal.inria.fr/hal-03380687.

[12] J.-M. Muller. '$a\cdot(x\cdot x)$ or $(a\cdot x)\cdot x$?' In: 28th IEEE Symposium on Computer Arithmetic (ARITH 2021). Proceedings of the 28th IEEE Symposium on Computer Arithmetic (ARITH 2021). Torino (virtual meeting due to the COVID Pandemic), Italy: IEEE, 2021. URL: https://hal.archives-ouvertes.fr/hal-03129747.

[13] A. Pellet-Mary and D. Stehlé. 'On the hardness of the NTRU problem'. In: Asiacrypt 2021 - 27th Annual International Conference on the Theory and Applications of Cryptology and Information Security. Advances in Cryptology – ASIACRYPT 2021. Lecture Notes in Computer Science, vol 13090. Singapore, Singapore, 1st Dec. 2021. DOI: 10.1007/978-3-030-92062-3_1. URL: https://hal.archives-ouvertes.fr/hal-03348022.

[14] C. Pernet, H. Signargout, P. Karpman and G. Villard. 'Computing the Characteristic Polynomial of Generic Toeplitz-like and Hankel-like Matrices'. In: *ISSAC'21*. ISSAC'21: International Symposium on Symbolic and Algebraic Computation. Saint Petersburg, Russia: ACM Press, July 2021, pp. 249–256. DOI: 10.1145/3452143.3465542. URL: https://hal.archives-ouvertes.fr/hal-03189115.

Scientific book chapters

[15] J.-M. Muller. 'Arithmétique et Précision des Calculs sur Ordinateur'. In: *De la mesure en toutes choses, CNRS Editions*. 14th Oct. 2021. URL: https://hal.archives-ouvertes.fr/hal-03461132.

Reports & preprints

[16] N. Brisebarre and G. Hanrot. *Integer points close to a transcendental curve and correctly-rounded evaluation of a function*. 11th Nov. 2021. URL: https://hal.archives-ouvertes.fr/hal-03240179.

[17] C.-P. Jeannerod. *Further remarks on Kahan summation with decreasing ordering*. 11th Dec. 2021. URL: https://hal.inria.fr/hal-03475741.

[18] V. Lefèvre, N. Louvet, J.-M. Muller, J. Picot and L. Rideau. *Accurate calculation of Euclidean Norms using Double-word arithmetic*. 16th Dec. 2021. URL: https://hal.archives-ouvertes.fr/hal-03482567.

[19] V. Lyubashevsky and D. Stehlé. *Non-applicability of the Gaborit&Aguilar-Melchor patent to Kyber and Saber*. ENS de Lyon; IBM Zürich, 9th Oct. 2021, pp. 1–8. URL: https://hal.archives-ouvertes.fr/hal-03372244.

[20] V. Neiger, B. Salvy, É. Schost and G. Villard. *Faster Modular Composition*. 15th Oct. 2021. URL: https://hal.archives-ouvertes.fr/hal-03380258.

[21] N. Revol. *Affine Iterations and Wrapping Effect: Various Approaches*. 31st Dec. 2021. URL: https://hal.inria.fr/hal-03505854.