RESEARCH CENTRE

Grenoble - Rhône-Alpes

IN PARTNERSHIP WITH:

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

2020 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 Team: 2012 January 01, updated into 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]
- Fabien Laguillaumie [Univ Claude Bernard, Professor, until Aug 2020, HDR]
- Nicolas Louvet [Univ Claude Bernard, Associate Professor]
- Damien Stehlé [École Normale Supérieure de Lyon, Professor, HDR]

Post-Doctoral Fellows

- Qian Chen [Université de Trondheim - Norvège, until Oct 2020]
- Rikki Amit Inder Deo [Inria - ENS, (March-June 2020), ENSL since July 2020]
- Alonso Gonzalez [École Normale Supérieure de Lyon]
- Dingding Jia [CNRS, until Oct 2020]
- Changmin Lee [Univ de Lyon, until Sep 2020]
- Herve Tale Kalachi [Inria, until Aug 2020]

PhD Students

- Orel Cosseron [Zama Sas, CIFRE, from Oct 2020]
- Julien Devevey [École Normale Supérieure de Lyon, from Sep 2020]
- Adel Hamdi [Orange Labs, CIFRE]
- Huyen Nguyen [École Normale Supérieure de Lyon]
- Miruna Rosca [BitDefender Bucarest - Roumanie, until Oct 2020]
- Hippolyte Signargout [École Normale Supérieure de Lyon, from Oct 2020]
- Radu Titiu [BitDefender Bucarest - Roumanie, until Oct 2020]
- Ida Tucker [École Normale Supérieure de Lyon, until Sep 2020]

Technical Staff

- Rikki Amit Inder Deo [Inria, Engineer, until Feb 2020]
- Joris Picot [École Normale Supérieure de Lyon, Engineer]

Interns and Apprentices

- Calvin Abou Haidar [École Normale Supérieure de Lyon, until Jun 2020]
- Bilel Bensaid [École Normale Supérieure de Lyon, from Jun 2020 until Aug 2020]
- Quentin Corradi [École Normale Supérieure de Lyon, from Apr 2020 until Jul 2020]
- Miguel Cueto Noval [ENS Lyon, Intern, From May 2020 until June 2020]
- Mathis Deronzier [École Normale Supérieure de Lyon, from Jun 2020 until Aug 2020]
- Julien Devevey [École Normale Supérieure de Lyon, until Jun 2020]
- Justine Sauvage [École Normale Supérieure de Lyon, from Apr 2020 until Jul 2020]
- Mohamed Sidi Ali Cherif [École Normale Supérieure de Lyon, from Apr 2020 until Jul 2020]
- Hermenegilde Valentin [École Normale Supérieure de Lyon, until Jun 2020]

Administrative Assistants

- Nelly Amsellem [École Normale Supérieure de Lyon, until Mar 2020]
- Chiraz Benamor [École Normale Supérieure de Lyon, from Mar 2020]
- Virginie Bouyer [École Normale Supérieure de Lyon, until Mar 2020]
- Octavie Paris [Ecole Normale Supérieure de Lyon, June 2019 - Present, European H2020 project manager]
- Octavie Paris [École Normale Supérieure de Lyon]

External Collaborator

- Fabien Laguillaumie [Univ de Montpellier, from Sep 2020, 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 → 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

Ida Tucker is one of 35 winners of the 2020 L'Oréal-UNESCO France Rising Talent Award for Women in Science.

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 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/

Contacts: Clément Pernet, Thierry Gautier, Gilles Villard

Participants: Clément Pernet, Thierry Gautier

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 Computation of Tight Enclosures for Laplacian Eigenvalues

Recently, there has been interest in high precision approximations of the first eigenvalue of the Laplace–Beltrami operator on spherical triangles for combinatorial purposes. We compute improved and certified enclosures to these eigenvalues. This is achieved by applying the method of particular solutions in high precision, the enclosure being obtained by a combination of interval arithmetic and Taylor models. The index of the eigenvalue is certified by exploiting the monotonicity of the eigenvalue with respect to the domain. The classically troublesome case of singular corners is handled by combining expansions at all corners and an expansion from an interior point. In particular, this allows us to compute 100 digits of the fundamental eigenvalue for the three-dimensional Kreweras model that has been the object of previous efforts. [6]

7.2 Floating-point and Validated Numerics

7.2.1 Error Analysis of some Operations Involved in the Cooley-Tukey Fast Fourier Transform

In [4], we obtain error bounds for the classical Cooley-Tukey FFT algorithm in floating-point arithmetic, for the 2-norm as well as for the infinity norm. For that purpose we also give some results on the relative error of the complex multiplication by a root of unity, and on the largest value that can take the real or imaginary part of one term of the FFT of a vector x, assuming that all terms of x have real and imaginary parts less than some value b.

7.2.2 Influence of the Condition Number on Interval Computations: Illustration on Some Examples

The condition number is a quantity that is well-known in “classical” numerical analysis, that is, where numerical computations are performed using floating-point numbers. This quantity appears much less frequently in interval numerical analysis, that is, where the computations are performed on intervals. The goal of [29] is twofold. On the one hand, it is stressed that the notion of condition number already appears in the literature on interval analysis, even if it does not bear that name. On the other hand, three small examples are used to illustrate experimentally the impact of the condition number on interval computations.

7.2.3 The Relative Accuracy of (x+y)*(x-y)

We consider in [7] the relative accuracy of evaluating $(x+y)(x-y)$ in IEEE floating-point arithmetic, when x, y are two floating-point numbers and rounding is to nearest. This expression can be used, for example, as an efficient cancellation-free alternative to x^2-y^2 and (at least in the absence of underflow and overflow) is well known to have low relative error, namely, at most about $3u$ with u denoting the unit roundoff. In this paper we propose to complement this traditional analysis with a finer-grained one, aimed at improving and assessing the quality of that bound. Specifically, we show that if the tie-breaking rule is to away then the bound $3u$ is asymptotically optimal (as the precision tends to ∞). In contrast, if the tie-breaking rule is to even, we show that asymptotically optimal bounds are now $2.25u$ for base two and $2u$ for larger bases, such as base ten. In each case, asymptotic optimality is obtained by the

explicit construction of a certificate, that is, some floating-point input (x, y) parametrized by u and such that the error of the associated result is equivalent to the error bound as u tends to zero. We conclude with comments on how $(x+y)(x-y)$ compares with x^2 in the presence of floating-point arithmetic, in particular showing cases where the computed value of $(x+y)(x-y)$ exceeds that of x^2.

7.2.4 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 [2], 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. This is a collaboration with S. Boldo (Inria Saclay) and C. Lauter (University of Alaska).

7.2.5 Elementary Functions and Approximate Computing

In [12], we review some of the classical methods used for quickly obtaining low-precision approximations to the elementary functions. Then, for each of the three main classes of elementary function algorithms (shift-and-add algorithms, polynomial or rational approximations, table-based methods) and for the additional, specific to approximate computing, "bit-manipulation" techniques, we examine what can be done for obtaining very fast estimates of a function, at the cost of a (controlled) loss in terms of accuracy.

7.2.6 Algorithms for Manipulating Quaternions in Floating-point Arithmetic

Quaternions form a set of four global but not unique parameters, which can represent three-dimensional rotations in a non-singular way. They are frequently used in computer graphics, drone and aerospace vehicle control. Floating-point quaternion operations (addition, multiplication, reciprocal, norm) are often implemented "by the book". Although all usual implementations are algebraically equivalent, their numerical behavior can be quite different. For instance, the arithmetic operations on quaternions as well as conversion algorithms to/from rotation matrices are subject to spurious under/overflow (an intermediate calculation underflows or overflows, making the computed final result irrelevant, although the exact result is in the domain of the representable numbers). We analyze and then propose workarounds and better accuracy alternatives for such algorithms [24].

7.2.7 Alternative Split Functions and Dekker's Product

We introduce algorithms for splitting a positive binary floating-point number into two numbers of around half the system precision, using arithmetic operations all rounded either toward $-\infty$ or toward $+\infty$. We use these algorithms to compute "exact" products (i.e., to express the product of two floating-point numbers as the unevaluated sum of two floating-point numbers, the rounded product and an error term). This is similar to the classical Dekker product, adapted here to directed roundings [23].

7.2.8 Formalization of Double-word Arithmetic

Recently, a complete set of algorithms for manipulating double-word numbers (some classical, some new) was analyzed by Joldes, Popescu and Muller. 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 some results 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 [34].

7.2.9 Hardware Implementation of Division Algorithms

We show the details of an implementation of Ercegovac and Muller's variable radix division algorithm. This implementation takes advantage of the easier prescaling offered by low-radix division and recodes it as necessary for higher radix iterations throughout the design. This, along with proper use of redundant digit sets, allows us to significantly alter performance characteristics relative to exclusively high-radix division implementations. Comparisons to existing architectures are shown, as well as common implementation optimizations for future iterations. Results are given in cmos32soi 32nm MTCMOS technology using ARMbased standard-cells and commercial EDA toolsets. This work was done in cooperation with M. Ercegovac (U.C. Los Angeles) and J. Stine (Oklahoma State Univ.) [28].

7.3 Lattices: Algorithms and Cryptology

7.3.1 On the Smoothing Parameter and Last Minimum of Random Orthogonal Lattices

Let $X \in \mathbb{Z}^{n\times m}$, with each entry independently and identically distributed from an integer Gaussian distribution. We conside the orthogonal lattice $\Lambda^{\perp}(X)$, i.e., the set of vectors $v \in \mathbb{Z}^m$ such that $Xv = 0$. We prove probabilistic upper bounds on the smoothing parameter and the $(m-n)$-th minimum of $\Lambda^{\perp}(X)$. These bounds improve and the techniques build upon prior works of Agrawal, Gentry, Halevi and Sahai [Asiacrypt'13], and of Aggarwal and Regev [Chicago J. Theoret. Comput. Sci.'16]. [9]

7.3.2 ModFalcon: Compact Signatures Based On Module-NTRU Lattices

Lattices lead to promising practical post-quantum digital signatures, combining asymptotic efficiency with strong theoretical security guarantees. However, tuning their parameters for practical instantiations is a delicate task. On the one hand, NIST round-2 candidates based on Lyubashevsky's design (such as dilithium and qtesla) allow several tradeoffs between security and efficiency, but at the expense of a large bandwidth consumption. On the other hand, the hash-and-sign falcon signature is much more compact and is still very efficient, but it allows only two security levels, with large compactness and security gaps between them. We introduce a new family of signature schemes based on the falcon design, which relies on module lattices. Our concrete instantiation enjoys the compactness and efficiency of falcon, and allows an intermediate security level. It leads to the most compact lattice-based signature achieving a quantum security above 128 bits.[19]

7.3.3 Faster Enumeration-Based Lattice Reduction

We give a lattice reduction algorithm that achieves root Hermite factor $k^{1/(2k)}$ in time $k^{k/8+o(k)}$ and polynomial memory. This improves on the previously best known enumeration-based algorithms which achieve the same quality, but in time $k^{k/(2e)+o(k)}$. A cost of $k^{k/8+o(k)}$ was previously mentioned as potentially achievable (Hanrot-Stehlé'10) or as a heuristic lower bound (Nguyen'10) for enumeration algorithms. We prove the complexity and quality of our algorithm under a heuristic assumption and provide empirical evidence from simulation and implementation experiments attesting to its performance for practical and cryptographic parameter sizes. The techniques used to achieve these results also suggest potential avenues for achieving costs below $k^{k/8+o(k)}$ for the same root Hermite factor, based on the geometry of SDBKZ-reduced bases.[14]

7.3.4 MPSign: a Signature from Small-Secret Middle-Product Learning with Errors

We describe a digital signature scheme MPSign, whose security relies on the conjectured hardness of the Polynomial Learning With Errors problem (PLWE) for at least one defining polynomial within an exponential-size family (as a function of the security parameter). The proposed signature scheme follows the Fiat-Shamir framework and can be viewed as the Learning With Errors counterpart of the signature scheme described by Lyubashevsky at Asiacrypt 2016, whose security relies on the conjectured hardness of the Polynomial Short Integer Solution (PSIS) problem for at least one defining polynomial within an exponential-size family. As opposed to the latter, MPSign enjoys a security proof from PLWE that is tight in the quantum-access random oracle model.

The main ingredient is a reduction from PLWE for an arbitrary defining polynomial among exponentially many, to a variant of the Middle-Product Learning with Errors problem (MPLWE) that allows for secrets that are small compared to the working modulus. We present concrete parameters for MPSign using such small secrets, and show that they lead to significant savings in signature length over Lyubashevsky's Asiacrypt 2016 scheme (which uses larger secrets) at typical security levels. As an additional small contribution, and in contrast to MPSign (or MPLWE), we present an efficient key-recovery attack against Lyubashevsky's scheme (or the inhomogeneous PSIS problem), when it is used with sufficiently small secrets, showing the necessity of a lower bound on secret size for the security of that scheme.[16]

7.3.5 Towards Practical GGM-Based PRF from (Module-)Learning with-Rounding

We investigate the efficiency of a (module-)LWR -based PRF built using the GGM design. Our construction enjoys the security proof of the GGM construction and the (module-)LWR hardness assumption which is believed to be post-quantum secure. We propose GGM-based PRFs from PRGs with larger ratio of output to input. This reduces the number of PRG invocations which improves the PRF performance and reduces the security loss in the GGM security reduction. Our construction bridges the gap between practical and provably secure PRFs. We demonstrate the efficiency of our construction by providing parameters achieving at least 128-bit post-quantum security and optimized implementations utilizing AVX2 vector instructions. Our PRF requires, on average, only 39.4 cycles per output byte.

7.3.6 Measure-Rewind-Measure: Tighter Quantum Random Oracle Model Proofs for One-Way to Hiding and CCA Security

We introduce a new technique called 'Measure-Rewind-Measure' (MRM) to achieve tighter security proofs in the quantum random oracle model (QROM). We first apply our MRM technique to derive a new security proof for a variant of the 'double-sided' quantum One-Way to Hiding Lemma (O2H) of Bindel et al. [TCC 2019] which, for the first time, avoids the square-root advantage loss in the security proof. In particular, it bypasses a previous 'impossibility result' of Jiang, Zhang and Ma [IACR eprint 2019]. We then apply our new O2H Lemma to give a new tighter security proof for the Fujisaki-Okamoto transform for constructing a strong (IND-CCA) Key Encapsulation Mechanism (KEM) from a weak (IND-CPA) public-key encryption scheme satisfying a mild injectivity assumption. [25]

7.3.7 New Constructions of Statistical NIZKs: Dual-Mode DV-NIZKs and More

Non-interactive zero-knowledge proofs (NIZKs) are important primitives in cryptography. A major challenge since the early works on NIZKs has been to construct NIZKs with a statistical zero-knowledge guarantee against unbounded verifiers. In the common reference string (CRS) model, such "statistical NIZK arguments" are currently known from k-Lin in a pairing-group and from LWE. In the (reusable) designated-verifier model (DV-NIZK), where a trusted setup algorithm generates a reusable verification key for checking proofs, we also have a construction from DCR. If we relax our requirements to computational zero-knowledge, we additionally have NIZKs from factoring and CDH in a pairing group in the CRS model, and from nearly all assumptions that imply public-key encryption (e.g., CDH, LPN, LWE) in the designated-verifier model. Thus, there still remains a gap in our understanding of statistical NIZKs in both the CRS and the designated-verifier models. In [27], we develop new techniques for constructing statistical NIZK arguments. First, we construct statistical DV-NIZK arguments from the k-Lin assumption in pairing-free groups, the QR assumption, and the DCR assumption. These are the first constructions in pairing-free groups and from QR that satisfy statistical zero-knowledge. All of our constructions are secure even if the verification key is chosen maliciously (i.e., they are "malicious-designated-verifier" NIZKs), and moreover, they satisfy a "dual-mode" property where the CRS can be sampled from two computationally indistinguishable distributions: one distribution yields statistical DV-NIZK arguments while the other yields computational DV-NIZK proofs. We then show how to adapt our k-Lin construction in a pairing group to obtain new publicly-verifiable statistical NIZK arguments from pairings with a qualitatively weaker assumption than existing constructions of pairing-based statistical NIZKs. Our constructions follow the classic paradigm of Feige, Lapidot, and Shamir (FLS). While the FLS framework has traditionally been used to construct computational (DV)-NIZK proofs, we newly show that the same framework can be leveraged to construct dual-mode (DV)-NIZKs.

7.3.8 Adaptive Simulation Security for Inner Product Functional Encryption

Inner product functional encryption (IPFE) is a popular primitive which enables inner product computations on encrypted data. In IPFE, the ciphertext is associated with a vector x, the secret key is associated with a vector y and decryption reveals the inner product x, y. Previously, it was known how to achieve adaptive indistinguishability (IND) based security for IPFE from the DDH, DCR and LWE assumptions. However, in the stronger simulation (SIM) based security game, it was only known how to support a restricted adversary that makes all its key requests either before or after seeing the challenge ciphertext, but not both. In more detail, Wee (TCC 2017) showed that the DDH-based scheme of Agrawal et al. (Crypto 2016) achieves semi-adaptive simulation-based security, where the adversary must make all its key requests after seeing the challenge ciphertext. On the other hand, O'Neill showed that all IND-secure IPFE schemes (which may be based on DDH, DCR and LWE) satisfy SIM based security in the restricted model where the adversary makes all its key requests before seeing the challenge ciphertext. In [13], we resolve the question of SIM-based security for IPFE by showing that variants of the IPFE constructions by Agrawal et al., based on DDH, Paillier and LWE, satisfy the strongest possible adaptive SIM-based security where the adversary can make an unbounded number of key requests both before and after seeing the (single) challenge ciphertext. This establishes optimal security of the IPFE schemes, under all hardness assumptions on which it can (presently) be based.

7.3.9 Simulation-Sound Arguments for LWE and Applications to KDM-CCA2 Security

The Naor-Yung paradigm is a well-known technique that constructs IND-CCA2-secure encryption schemes by means of non-interactive zero-knowledge proofs satisfying a notion of simulation-soundness. Until recently, it was an open problem to instantiate it under the sole Learning-With-Errors (LWE) assumption without relying on random oracles. While the recent results of Canetti et al. (STOC'19) and Peikert-Shiehian (Crypto'19) provide a solution to this problem by applying the Fiat-Shamir transform in the standard model, the resulting constructions are extremely inefficient as they proceed via a reduction to an NP-complete problem. In [26], we give a direct, non-generic method for instantiating Naor-Yung under the LWE assumption outside the random oracle model. Specifically, we give a direct construction of an unbounded simulation-sound NIZK argument system which, for carefully chosen parameters, makes it possible to express the equality of plaintexts encrypted under different keys in Regev's cryptosystem. We also give a variant of our argument that provides tight security. As an application, we obtain an LWE-based public-key encryption scheme for which we can prove (tight) key-dependent message security under chosen-ciphertext attacks in the standard model.

7.3.10 Lattice-based e-cash, Revisited

Electronic cash (e-cash) was introduced 40 years ago as the digital analogue of traditional cash. It allows users to withdraw electronic coins that can be spent anonymously with merchants. As advocated by Camenisch et al. (Eurocrypt 2005), it should be possible to store the withdrawn coins compactly (i.e., with logarithmic cost in the total number of coins), which has led to the notion of compact e-cash. Many solutions were proposed for this problem but the security proofs of most of them were invalidated by a very recent paper by Bourse et al. (Asiacrypt 2019). The same paper describes a generic way of fixing existing constructions/proofs but concrete instantiations of this patch are currently unknown in some settings. In particular, compact e-cash is no longer known to exist under quantum-safe assumptions. In [20], we resolve this problem by proposing the first secure compact e-cash system based on lattices following the result from Bourse et al. Contrarily to the latter work, our construction is not only generic, but we describe two concrete instantiations. We depart from previous frameworks of e-cash systems by leveraging lossy trapdoor functions to construct our coins. The indistinguishability of lossy and injective keys allows us to avoid the very strong requirements on the involved pseudo-random functions that were necessary to instantiate the generic patch proposed by Bourse et al.

7.3.11 Signatures of Knowledge and NIZK Proofs for Boolean Circuits

In [15], we construct unbounded simulation-sound proofs for Boolean circuit satisfiability under standard assumptions with proofs comprised of $O(n+d)$ group elements, where d is the depth and n is the input

size of the circuit. Our technical contribution is to add unbounded simulation soundness to a recent NIZK of González and Ràfols (ASIACRYPT'19) with very small overhead. We give two different constructions: the first one is more efficient but not tight, and the second one is tight. The new scheme can be used to construct Signatures of Knowledge based on standard assumptions that also can be composed universally with other cryptographic protocols/primitives. As an independent contribution, we also detail a simple formula to encode Boolean circuits as Quadratic Arithmetic Programs.

7.3.12 Bandwidth-efficient Threshold EC-DSA

Threshold Signatures allow n parties to share the power of issuing digital signatures so that any coalition of size at least (t+1) can sign, whereas groups of t or less players cannot. Over the last few years many schemes addressed the question of realizing efficient threshold variants for the specific case of EC-DSA signatures. In [18] we present new solutions to the problem that aim at reducing the overall bandwidth consumption. Our main contribution is a new variant of the Gennaro and Goldfeder protocol from ACM CCS 2018 that avoids all the required range proofs, while retaining provable security against malicious adver- saries in the dishonest majority setting. Our experiments show that – for all levels of security – our signing protocol reduces the bandwidth consumption of best previously known secure protocols for factors varying between 4.4 and 9, while key generation is consistently two times less expensive. Furthermore compared to these same protocols, our signature generation is faster for 192-bits of security and beyond.

7.3.13 Blind Functional Encryption

Functional encryption (FE) gives the power to retain control of sensitive information and is particularly suitable in several practical real-world use cases. Using this primitive, anyone having a specific functional decryption key (derived from some master secret key) could only obtain the evaluation of an authorized function f over a message m, given its encryption. For many scenarios, the data owner is always different from the functionality owner, such that a classical implementation of functional encryption naturally implies an interactive key generation protocol between an entity owning the function f and another one managing the master secret key. We focus on this particular phase and consider the case where the function needs to be secret. In [17], we introduce the new notion of blind functional encryption in which, during an interactive key generation protocol, the master secret key owner does not learn anything about the function f. Our new notion can be seen as a generalisation of the existing concepts of blind IBE/ABE. After a deep study of this new property and its relation with other security notions, we show how to obtain a generic blind FE from any non-blind FE, using homomorphic encryption and zero-knowledge proofs of knowledge. We finally illustrate such construction by giving an efficient instantiation in the case of the inner product functionality.

7.3.14 Alternative Constructions of Asymmetric Primitives from Obfuscation: Hierarchical IBE, Predicate Encryption, and More

We revisit constructions of asymmetric primitives from obfuscation and give simpler alternatives. We consider public-key encryption, (hierarchical) identity-based encryption ((H)IBE), and predicate encryption. Obfuscation has already been shown to imply PKE by Sahai and Waters (STOC'14) and full-fledged functional encryption by Garg et al. (FOCS'13). We simplify all these constructions and reduce the necessary assumptions on the class of circuits that the obfuscator needs to support. Our PKE scheme relies on just a PRG and does not need any puncturing. Our IBE and bounded HIBE schemes convert natural key-delegation mechanisms from (recursive) applications of puncturable PRFs to IBE and HIBE schemes. Our most technical contribution is an unbounded HIBE, which uses (public-coin) differing-inputs obfuscation for circuits and whose proof relies on a recent pebbling-based hybrid argument by Fuchsbauer et al. (ASIACRYPT'14). All our constructions are anonymous, support arbitrary inputs, and have compact keys and ciphertexts. [21]

7.3.15 From Cryptomania to Obfustopia through Secret-Key Functional Encryption

Functional encryption lies at the frontiers of current research in cryptography; some variants have been shown sufficiently powerful to yield indistinguishability obfuscation (IO) while other variants have been constructed from standard assumptions such as LWE. Indeed, most variants have been classified as belonging to either the former or the latter category. However, one mystery that has remained is the case of secret-key functional encryption with an unbounded number of keys and ciphertexts. On the one hand, this primitive is not known to imply anything outside of minicrypt, the land of secret-key crypto, but on the other hand, we do no know how to construct it without the heavy hammers in obfustopia. In this work, we show that (subexponentially secure) secret-key functional encryption is powerful enough to construct indistinguishability obfuscation if we additionally assume the existence of (subexponentially secure) plain public-key encryption. In other words, secret-key functional encryption provides a bridge from cryptomania to obfustopia. On the technical side, our result relies on two main components. As our first contribution, we show how to use secret key functional encryption to get "exponentially-efficient indistinguishability obfuscation" (XIO), a notion recently introduced by Lin et al. (PKC '16) as a relaxation of IO. Lin et al. show how to use XIO and the LWE assumption to build IO. As our second contribution, we improve on this result by replacing its reliance on the LWE assumption with any plain public-key encryption scheme. Lastly, we ask whether secret-key functional encryption can be used to construct public-key encryption itself and therefore take us all the way from minicrypt to obfustopia. A result of Asharov and Segev (FOCS '15) shows that this is not the case under black-box constructions, even for exponentially secure functional encryption. We show, through a non-black box construction, that subexponentially securekey functional encryption indeed leads to public-key encryption. The resulting public-key encryption scheme, however, is at most quasi-polynomially secure, which is insufficient to take us to obfustopia. [1]

7.3.16 Privately Outsourcing Exponentiation to a Single Server: Cryptanalysis and Optimal Constructions

In [5], we address the problem of speeding up group computations in cryptography using a single untrusted computational resource. We analyze the security of two efficient protocols for securely outsourcing (multi-)exponentiations. We show that the schemes do not achieve the claimed security guarantees and we present practical polynomial-time attacks on the delegation protocols which allow the untrusted helper to recover part (or the whole) of the device's secret inputs. We then provide simple constructions for outsourcing group exponentiations in different settings (e.g. public/secret, fixed/variable bases and public/secret exponents). Finally, we prove that our attacks are unavoidable if one wants to use a single untrusted computational resource and to limit the computational cost of the limited device to a constant number of (generic) group operations. In particular, we show that our constructions are actually optimal in terms of operations in the underlying group.

7.3.17 Functional Encryption and Distributed Signatures Based on Projective Hash Functions, the Benefit of Class Groups

One of the current challenges in cryptographic research is the development of advanced cryptographic primitives ensuring a high level of confidence. In this thesis, we focus on their design, while proving their security under well-studied algorithmic assumptions.

This work grounds itself on the linearity of homomorphic encryption, which allows to perform linear operations on encrypted data. Precisely, it built upon the linearly homomorphic encryption scheme introduced by Castagnos and Laguillaumie at CT-RSA'15. Their scheme possesses the unusual property of having a prime order plaintext space, whose size can essentially be tailored to ones' needs. Aiming at a modular approach, technical tools are designed from their work (projective hash functions, zero-knowledge proofs of knowledge) which provide a rich framework lending itself to many applications.

This framework first makes it possible to build functional encryption schemes; this highly expressive primitive allows a fine grained access to the information contained in e.g., an encrypted database. Then, in a different vein, but from these same tools, threshold digital signatures are designed, allowing a secret key to be shared among multiple users, so that the latter must collaborate in order to produce valid signatures. Such signatures can be used, among other applications, to secure crypto-currency wallets.

Significant efficiency gains, namely in terms of bandwidth, result from the instantiation of these constructions from class groups. This work is at the forefront of the revival these mathematical objects have seen in cryptography over the last few years. [32]

7.4 Algebraic Computing and High-performance Kernels

7.4.1 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. [11]

7.4.2 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. [3]

7.4.3 Fast Computation of Approximant Bases in Canonical Form

In [8], we design fast algorithms for the computation of approximant bases in shifted Popov normal form. We first recall the algorithm known as PM-Basis, which will be our second fundamental engine after polynomial matrix multiplication: most other fast approximant basis algorithms basically aim at efficiently reducing the input instance to instances for which PM-Basis is fast. Such reductions usually involve partial linearization techniques due to Storjohann, which have the effect of balancing the degrees and dimensions in the manipulated matrices. Following these ideas, Zhou and Labahn gave two algorithms which are faster than PM-Basis for important cases including Hermite-Padé approximation, yet only for shifts whose values are concentrated around the minimum or the maximum value. The three mentioned algorithms were designed for balanced orders and compute approximant bases that are generally not normalized. Here, we show how they can be modified to return the shifted Popov basis without impact on their cost bound; besides, we extend Zhou and Labahn's algorithms to arbitrary orders. Furthermore, we give an algorithm which handles arbitrary shifts with one extra logarithmic factor in the cost bound compared to the above algorithms. To the best of our knowledge, this improves upon previously known algorithms for arbitrary shifts, including for particular cases such as Hermite-Padé approximation. This algorithm is based on a recent divide-and-conquer approach that reduces the general case to the case where information on the output degree is available. As outlined above, we solve the latter case via partial linearizations and PM-Basis.

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 square root algorithms in fixed-point and floating-point arithmetics (participants: Claude-Pierre Jeannerod and

Jean-Michel Muller).

8.2 Bilateral grants with industry

- Miruna Rosca and Radu Titiu are employees of BitDefender. Their PhD's are supervised by Damien Stehlé and Benoît Libert, respectively. Miruna Rosca works on the foundations of lattice-based cryptography, and Radu Titiu works on pseudo-random functions and functional encryption.
- Adel Hamdi is doing his PhD with Orange Labs and is supervised by Fabien Laguillaumie. He is working on advanced encryption protocols for the cloud.
- 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 initiatives

9.1.1 Participation in other international programs

IFCPAR Research grant with IIT Madras

Participant Benoît Libert, Damien Stehlé, Dingding Jia.

The project "Computing on Encrypted Data: New Paradigms in Functional Encryption" is funded by the Indo-French Centre for the Promotion of Advanced Research (IFCPAR/CEFIPRA) since January 2019 (for 3 years) and hosted by CNRS on the French side. The co-PIs are Shweta Agrawal (IIT Madras) and Benoît Libert. The global budget is 200,000€. This projects deals with a cryptographic primitive called "Functional Encryption" which aims at developing new techniques for evaluating expressive functions on encrypted data and obtaining the evaluation result in the clear. It aims at leveraging the potential of Euclidean lattices to build functional encryption schemes that evaluate expressive functions (represented by Boolean circuits or Turing machines) on encrypted data.

9.2 European initiatives

9.2.1 FP7 & H2020 Projects

PROMETHEUS H2020 Project

Participant Benoît Libert, Damien Stehlé, Amit Deo, Octavie Paris.

PROMETHEUS (Privacy-Preserving Systems from Advanced Cryptographic Mechanisms Using Lattices) is a European H2020 project (Call H2020-DS-2016-2017, Cybersecurity PPP Cryptography (DS-06-2017)) that started in January 2018 (http://www.h2020prometheus.eu/). The project was initially over 4 years but received a 6-month extension due to the COVID crisis (expected end is now June 2022). It involves 7 academic partners and 5 academic partners (Orange, IBM, Thales, TNO, Scytl). The Global budget is 5,496,968€ (amount received by ENS de Lyon: 567,340€). The goal of this consortium 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 they are 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, which is hosting the project.

9.3 National initiatives

ANR ALAMBIC Project

Participant Benoît Libert, Fabien Laguillaumie, Ida Tucker, Alonso Gonzalez.

ALAMBIC is a four-year project (started in October 2016) 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.

RISQ Project

Participant Chitchanok Chuengsatiansup, Rikki Amit Inder Deo, Hervé Tale Kalachi, 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.

10 Dissemination

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

Member of the organizing committees Bruno Salvy was an organizer of the workshop "Symbolic Analysis" of the conference "Foundations of Computational Mathematics" in Vancouver, that ended up being cancelled.

Damien Stehlé co-organized the workshop "Lattices: From Theory to Practice", which was part of the Simons Institute trimester "Lattices: Algorithms, Complexity, and Cryptography".

10.1.2 Scientific events: selection

Member of the conference program committees Benoît Libert was a program committee member for PKC 2020, SCN 2020, Asiacrypt 2020, Eurocrypt 2021 and CT-RSA 2021.

Nathalie Revol was a member of the program commmittee for Arith 2020 and Arith 2021.

Bruno Salvy was a member of the program committee for AofA 2020.

Damien Stehlé was a member of the PQCrypto 2020 program committee.

Jean-Michel Muller was a member of the program commmittee for Arith 2020, Arith 2021, and ASAP 2021.

10.1.3 Journal

Member of the editorial boards Nathalie Revol belongs to the editorial board of "Reliable Computing".

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 for the "Journal of Cryptology" and "Designs, Codes and Cryptography".

Jean-Michel is associate Editor in Chief of the IEEE Transactions on Emerging Topics in Computing.

10.1.4 Leadership within the scientific community

Claude-Pierre Jeannerod is a member of the scientific committee of JNCF (Journées Nationales de Calcul Formel). He is also a member of the recruitment committee for postdocs and sabbaticals at Inria Grenoble–Rhône-Alpes.

Nathalie Revol is a member of the scientific committee of the GdR Calcul.

Bruno Salvy is in the steering committee of the conference AofA. He is a member of the scientific councils of the CIRM, Luminy and of the GDR Informatique Mathématique of the CNRS. He headed a selection committee for positions of professor and assistant professor in computer science at École polytechnique and was a member of a selection committee for a professor in mathematics at Université Versailles-Saint-Quentin.

Damien Stehlé is a member of the advisory board of the Cryptography Research Centre of the Technology Innovation Institute (Abu Dhabi).

Damien Stehlé is a member of the advisary board of CryptoNext-security (France).

Damien Stehlé was a member of a selection committee for an assistant professor position in computer science at ENS Lyon.

Jean-Michel Muller is in the steering committee of the Conference Arith.

10.1.5 Scientific expertise

Nathalie Revol belonged to the scientific jury for the attribution of BQR of U. Perpignan. She has been an expert for the European H2020 program.

Jean-Michel Muller belongs to the scientific council of CERFACS.

10.1.6 Research administration

Jean-Michel Muller is co-head of GdR IM.

10.2 Teaching - Supervision - Juries

Teaching

- Master: Nicolas Brisebarre, Approximation Theory and Proof Assistants: Certified Computations, 12h, M2, ENS de Lyon, France
- Master: Claude-Pierre Jeannerod, Floating-Point Arithmetic, 6h, M2, ENS de Lyon, France
- Master: Jean-Michel Muller, Floating-Point Arithmetic, 6h, M2, ENS de Lyon, France
- Master: Guillaume Hanrot, Computer algebra, 10h, ENS de Lyon, France
- Master: Guillaume Hanrot, Cryptanalysis, 15h, ENS de Lyon, France
- Master (1&2): Fabien Laguillaumie, Cryptography, 160 h, ISFA, UCBL, France
- Master: Nicolas Louvet, Compilers, 15h, M1, UCB Lyon 1, France

- Master: Nicolas Louvet, Operating Systems, 30h, M2, UCB Lyon 1, France
- Master: Alain Passelègue, Computer Algebra, 10h, M1, ENS de Lyon, France
- Master: Alain Passelègue, Advanced Topics in Cryptography, 30h, M2, ENS de Lyon, France
- Master: Bruno Salvy, Computer Algebra, 6h, ENS de Lyon, France
- Master: Bruno Salvy, Logic and Complexity, 32h, École polytechnique, France
- Master : Gilles Villard, Computer Algebra, 8h, ENS de Lyon, France
- Master : Vincent Lefèvre, Computer arithmetic, 12h, ISFA (Institut de Science Financière et d'Assurances), Université Claude Bernard Lyon 1, France
- Bachelor: Guillaume Hanrot, Calculability and complexity, 32h, ENS de Lyon, France
- Bachelor: Nicolas Louvet, Computer Architecture, 6h, L1, UCB Lyon 1, France
- Bachelor: Nicolas Louvet, Operating Systems, 35h, L2, UCB Lyon 1, France
- Bachelor: Nicolas Louvet, Data Structures and Algorithms, 24h, L2, UCB Lyon 1, France
- Bachelor: Nicolas Louvet, Data Structures and Algorithms, 45h, L3, UCB Lyon 1, France
- Bachelor: Nicolas Louvet, Formal Languages, 21h, L3, UCB Lyon 1, France
- Bachelor: Nicolas Louvet, Classical Logic, 24h, L3, UCB Lyon 1, France
- Bachelor: Bruno Salvy, Design and Analysis of Algorithms, 20h, École polytechnique, France

Supervision

- PhD: Miruna Rosca, On Algebraic Variants of Learning With Errors, November 16, Damien Stehlé
- PhD: Radu Titiu, New Encryption Schemes and Pseudo Random Functions with Advanced Properties from Standard Assumptions, October 16, Benoît Libert
- PhD in progress: Huyen Nguyen, Cryptographic aspects of orthogonal lattices, September 2018, Damien Stehlé
- PhD in progress: Orel Cosseron, Cryptographic aspects of orthogonal lattices, October 2020 2018, Damien Stehlé (co-supervised by Pascal Paillier and Marc Joye, Zama)
- PhD in progress: Julien Devevey, Threshold cryptography, October 2020 2018, Co-supervised by Benoît Libert and Damien Stehlé
- PhD in progress: Adel Hamdi, Functional Encryption, December 2017, Fabien Laguillaumie (co-supervised by Sébastien Canard, Orange)
- PhD in progress: Ida Tucker, Advanced cryptographic primitives from homomorphic encryption, October 2017, Fabien Laguillaumie (co-direction with Guilhem Castagnos, Université de Bordeaux)

Juries

- Fabien Laguillaumie was reviewer and jury member of the PhD of Guillaume Kaim (Université de Rennes)
- Benoît Libert was a member of the PhD committee of Michele Orrù (ENS Paris) and Patrick Towa (LIP6).
- Nathalie Revol belonged to the jury for CAPES NSI. She was a member of the PhD committee of Andrea Bocco (U. Lyon).
- Bruno Salvy was a member of the PhD committee of Mickaël Maazoun (maths, ENS Lyon) and of the habilitation committee of Delphine Boucher (maths, U. Rennes).
- Damien Stehlé was a reviewer and jury member of the PhD of Mélissa Rossi (ENS Paris) and a reviewer for the PhD of Monosij Maitra (IIT Madras).
- Gilles Villard was reviewer for the PhD thesis of Robin Larrieu (Université Paris-Saclay); examiner for the habilitation of Pascal Giorgi (Université de Montpellier) and the PhD thesis of Matías Bender (Sorbonne Université).

10.3 Popularization

10.3.1 Internal or external Inria responsibilities

Nathalie Revol is the scientific editor of the Web magazine Interstices: https://interstices.info. She belongs to the prospective committee of MMI: https://mmi-lyon.fr. She was a member of the jury for the scientific video competition, organized by SIF and sponsored by Fred Courant, from "L'esprit sorcier".

Regarding parity concerns: Nathalie Revol is the co-chair of the LIP committee for parity and a member of the Inria parity committee.

10.3.2 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.

10.3.3 Interventions

Nathalie Revol gave a conference about computer arithmetic for "OpenMinds", that gathers a conference in science and a conference in humanities, intended for students at ENS Lyon.

For high-school pupils (about 70 pupils): as an incentive, especially for girls, to choose scientific careers, Nathalie Revol gave talks at Mondial des Métiers (in February 2020) and "Sciences, un métier de femmes" (in March 2020). She took part in two "Filles & Maths-Info" days, each of them gathering around 80 high-school girls of 1e S in France and Lebanon: as a speaker in May 2020 and as a co-organizer in December 2020.

Damien Stehlé was interviewed on LCI and Radio B to warn about the privacy risks of contact tracing apps. He co-signed an opinion column in L'Humanité entitled "StopCovid. Ce traitement expéditif d'une question aussi centrale pour les libertés individuelles".

11 Scientific production

11.1 Publications of the year

International journals

[1] N. Bitansky, R. Nishimaki, A. Passelègue and D. Wichs. 'From Cryptomania to Obfustopia Through Secret-Key Functional Encryption'. In: *Journal of Cryptology* 33.2 (Apr. 2020), pp. 357–405. DOI: 10.1007/s00145-019-09337-9. URL: https://hal.inria.fr/hal-03025568.

[2] 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* (2020). DOI: 10.1109/TC.2020.3002702. URL: https://hal.archives-ouvertes.fr/hal-02137968.

[3] 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.

[4] N. Brisebarre, M. Joldes, J.-M. Muller, A.-M. Naneş and J. Picot. 'Error analysis of some operations involved in the Cooley-Tukey Fast Fourier Transform'. In: *ACM Transactions on Mathematical Software* 46.2 (May 2020), pp. 1–34. DOI: 10.1145/3368619. URL: https://hal.archives-ouvertes.fr/hal-01949458.

[5] C. Chevalier, F. Laguillaumie and D. Vergnaud. 'Privately Outsourcing Exponentiation to a Single Server: Cryptanalysis and Optimal Constructions'. In: *Algorithmica* 83.1 (30th Jan. 2021), pp. 72–115. DOI: 10.1007/s00453-020-00750-2. URL: https://hal.archives-ouvertes.fr/hal-02899803.

[6] J. Dahne and B. Salvy. 'Computation of Tight Enclosures for Laplacian Eigenvalues'. In: *SIAM Journal on Scientific Computing* 42.5 (Sept. 2020), A3210–A3232. DOI: 10.1137/20M1326520. URL: https://hal.archives-ouvertes.fr/hal-03015691.

[7] C.-P. Jeannerod. 'The relative accuracy of $(x+y)*(x-y)$'. In: *Journal of Computational and Applied Mathematics* (2020), pp. 1–17. DOI: 10.1016/j.cam.2019.112613. URL: https://hal.inria.fr/hal-02100500.

[8] C.-P. Jeannerod, V. Neiger and G. Villard. 'Fast computation of approximant bases in canonical form'. In: *Journal of Symbolic Computation* 98 (2020), pp. 192–224. DOI: 10.1016/j.jsc.2019.07.011. URL: https://hal-unilim.archives-ouvertes.fr/hal-01683632.

[9] E. Kirshanova, H. Nguyen, D. Stehlé and A. Wallet. 'On the smoothing parameter and last minimum of random orthogonal lattices'. In: *Designs, Codes and Cryptography* 88.5 (May 2020), pp. 931–950. DOI: 10.1007/s10623-020-00719-w. URL: https://hal.archives-ouvertes.fr/hal-03011623.

[10] B. Libert and M. Yung. 'Adaptively Secure Non-interactive CCA-Secure Threshold Cryptosystems: Generic Framework and Constructions'. In: *Journal of Cryptology* 33 (9th June 2020), pp. 1405–1441. DOI: 10.1007/s00145-020-09350-3. URL: https://hal.inria.fr/hal-03116642.

[11] 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.

[12] J.-M. Muller. 'Elementary Functions and Approximate Computing'. In: *Proceedings of the IEEE* 108.12 (Dec. 2020), pp. 1558–2256. DOI: 10.1109/JPROC.2020.2991885. URL: https://hal.archives-ouvertes.fr/hal-02517784.

International peer-reviewed conferences

[13] S. Agrawal, B. Libert, M. Maitra and R. Titiu. 'Adaptive Simulation Security for Inner Product Functional Encryption'. In: PKC 2020 - International Conference on Public Key Cryptography. Virtual, United Kingdom, 1st June 2020, pp. 1–30. URL: https://hal.inria.fr/hal-02993611.

[14] M. Albrecht, S. Bai, P.-A. Fouque, P. Kirchner, D. Stehlé and W. Wen. 'Faster Enumeration-Based Lattice Reduction: Root Hermite Factor $k^{1/(2k)}$ Time $k^{k/8+o(k)}$'. In: *Advances in Cryptology - {CRYPTO} 2020; Advances in Cryptology - {CRYPTO} 2020*. Crypto. Santa Barbara, United States, 2020, pp. 186–212. DOI: 10.1007/978-3-030-56880-1_7. URL: https://hal.archives-ouvertes.fr/hal-03011699.

[15] K. Baghery, A. González, Z. Pindado and C. Ràfols. 'Signatures of Knowledge for Boolean Circuits under Standard Assumptions (Full version)'. In: AFRICACRYPT 2020 - 12th International Conference on Cryptology in Africa. Vol. 12174. LNCS - Lecture Notes in Computer Science. Cairo / Virtual, Egypt: Springer, 20th July 2020. DOI: 10.1007/978-3-030-51938-4_2. URL: https://hal.inria.fr/hal-03118271.

[16] S. Bai, D. Das, R. Hiromasa, M. Rosca, A. Sakzad, D. Stehlé, R. Steinfeld and Z. Zhang. 'MPSign: A Signature from Small-Secret Middle-Product Learning with Errors'. In: *IACR International Conference on Public-Key Cryptography*. PKC. Edimburgh, United Kingdom, 29th Apr. 2020, pp. 66–93. DOI: 10.1007/978-3-030-45388-6_3. URL: https://hal.archives-ouvertes.fr/hal-03011669.

[17] S. Canard, A. Hamdi and F. Laguillaumie. 'Blind Functional Encryption'. In: ICICS 2020 - International Conference on Information and Communications Security. Vol. Lecture Notes in Computer Science. Information and Communications Security - 22nd International Conference, ICICS 2020, Copenhagen, Denmark, August 24-26, 2020, Proceedings 12282. Copenhagen, Denmark: Springer, 28th Nov. 2020, pp. 183–201. DOI: 10.1007/978-3-030-61078-4_11. URL: https://hal.archives-ouvertes.fr/hal-03039850.

[18] G. Castagnos, D. Catalano, F. Laguillaumie, F. Savasta and I. Tucker. 'Bandwidth-Efficient Threshold EC-DSA'. In: PKC 2020 - 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography. Public-Key Cryptography – PKC 2020. Edinburgh / Virtual, United Kingdom: Springer International Publishing, 29th Apr. 2020, pp. 266–296. DOI: 10.1007/978-3-030-45388-6_10. URL: https://hal.archives-ouvertes.fr/hal-02944825.

[19] C. Chuengsatiansup, T. Prest, D. Stehlé, A. Wallet and K. Xagawa. 'ModFalcon: Compact Signatures Based On Module-NTRU Lattices'. In: ASIA-CCS. Taipei, France: ACM, 2020, pp. 853–866. DOI: 10.1145/3320269.3384758. URL: https://hal.archives-ouvertes.fr/hal-03011646.

[20] A. Deo, B. Libert, K. Nguyen and O. Sanders. 'Lattice-Based E-Cash, Revisited'. In: Asiacrypt 2020 - 26th Annual International Conference on the Theory and Application of Cryptology and Information Security. Corée (devenu virtuel pour cause de COVID), South Korea, 7th Dec. 2020, pp. 1–47. URL: https://hal.inria.fr/hal-02993620.

[21] P. Farshim, G. Fuchsbauer and A. Passelègue. 'Alternative Constructions of Asymmetric Primitives from Obfuscation: Hierarchical IBE, Predicate Encryption, and More'. In: Indocrypt 2020. Virtual conference, India, 13th Dec. 2020. URL: https://hal.inria.fr/hal-03120656.

[22] J. Gong and H. Wee. 'Adaptively Secure ABE for DFA from k-Lin and More'. In: *EUROCRYPT 2020 - International Conference on Theory and Applications of Cryptographic Techniques*. EUROCRYPT 2020 - 9th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. LNCS. 12107. Zagreb / Virtual, Croatia: Springer, 1st May 2020, pp. 278–308. DOI: 10.1007/978-3-030-45727-3_10. URL: https://hal.inria.fr/hal-02894509.

[23] S. Graillat, V. Lefèvre and J.-M. Muller. 'Alternative Split Functions and Dekker's Product'. In: *Proceedings of ARITH-2020, IEEE 27th Symposium on Computer Arithmetic*. ARITH-2020 - IEEE 27th Symposium on Computer Arithmetic. Portland, United States: IEEE, June 2020, pp. 1–7. DOI: 10.1109/ARITH48897.2020.00015. URL: https://hal.archives-ouvertes.fr/hal-02470782.

[24] M. Joldeş and J.-M. Muller. 'Algorithms for manipulating quaternions in floating-point arithmetic'. In: *Proceedings of ARITH-2020, IEEE 27th Symposium on Computer Arithmetic*. ARITH-2020 - IEEE 27th Symposium on Computer Arithmetic. Proceedings of ARITH-2020, IEEE 27th Symposium on Computer Arithmetic. Portland, United States: IEEE, June 2020, pp. 1–8. DOI: 10.1109/ARITH48897.2020.00016. URL: https://hal.archives-ouvertes.fr/hal-02470766.

[25] V. Kuchta, A. Sakzad, D. Stehlé, R. Steinfeld and S.-F. Sun. 'Measure-Rewind-Measure: Tighter Quantum Random Oracle Model Proofs for One-Way to Hiding and CCA Security'. In: *Advances in Cryptology - {EUROCRYPT} 2020*. Eurocrypt. Zagreb, Croatia, 1st May 2020, pp. 703–728. DOI: 10.1007/978-3-030-45727-3_24. URL: https://hal.archives-ouvertes.fr/hal-03011691.

[26] B. Libert, K. Nguyen, A. Passelègue and R. Titiu. 'Simulation-Sound Arguments for LWE and Applications to KDM-CCA2 Security'. In: Asiacrypt 2020 - 26th Annual International Conference on the Theory and Application of Cryptology and Information Security. Virtual, South Korea, 7th Dec. 2020, pp. 1–67. URL: https://hal.inria.fr/hal-02993617.

[27] B. Libert, A. Passelègue, H. Wee and D. J. Wu. 'New Constructions of Statistical NIZKs: Dual-Mode DV-NIZKs and More'. In: Eurocrypt 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Zagreb / Virtual, Croatia: Springer, 10th May 2020, pp. 1–85. URL: https://hal.inria.fr/hal-02993608.

[28] J. E. Stine, M. D. Ercegovac and J.-M. Muller. 'An Architecture for Improving Variable Radix Real and Complex Division Using Recurrence Division'. In: Asilomar Conference on Signals, Systems, and Computers. Proceedings of the 2020 Asilomar Conference on Signals, Systems, and Computers. Pacific Grove, CA (virtual), United States, 2nd Nov. 2020. URL: https://hal.archives-ouvertes.fr/hal-03047208.

Scientific book chapters

[29] N. Revol. 'Influence of the Condition Number on Interval Computations: Illustration on Some Examples'. In: *Beyond Traditional Probabilistic Data Processing Techniques: Interval, Fuzzy etc. Methods and Their Applications*. Vol. 835. Studies in Computational Intelligence. Springer, 2020, pp. 359–373. DOI: 10.1007/978-3-030-31041-7_20. URL: https://hal.inria.fr/hal-01588713.

Doctoral dissertations and habilitation theses

[30] G.-M. Rosca. 'On algebraic variants of Learning With Errors'. Université de Lyon, 17th Nov. 2020. URL: https://tel.archives-ouvertes.fr/tel-03085029.

[31] R. Titiu. 'New Encryption Schemes and Pseudo-Random Functions with Advanced Properties from Standard Assumptions'. Université de Lyon, 16th Oct. 2020. URL: https://tel.archives-ouvertes.fr/tel-03116774.

[32] I. Tucker. 'Functional encryption and distributed signatures based on projective hash functions, the benefit of class groups'. Université de Lyon, 19th Oct. 2020. URL: https://tel.archives-ouvertes.fr/tel-03021689.

Reports & preprints

[33] T. Genet, T. Jensen and J. Sauvage. *Termination of Ethereum's Smart Contracts*. Univ Rennes, Inria, CNRS, IRISA, 27th Apr. 2020. URL: https://hal.inria.fr/hal-02555738.

[34] 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"*. 20th Oct. 2020. URL: https://hal.archives-ouvertes.fr/hal-02972245.

[35] C. Pernet, H. Signargout, P. Karpman and G. Villard. *Computing the Characteristic Polynomial of Generic Toeplitz-like and Hankel-like Matrices*. 2nd Apr. 2021. URL: https://hal.archives-ouvertes.fr/hal-03189115.