IN PARTNERSHIP WITH:
CNRS

Ecole normale supérieure de Lyon

Université Claude Bernard (Lyon 1)

Activity Report 2018

Project-Team ARIC

Arithmetic and Computing

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

RESEARCH CENTER
Grenoble - Rhône-Alpes

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Project-Team ARIC

Creation of the Team: 2012 January 01, updated into Project-Team: 2013 January 01

Keywords:

Computer Science and Digital Science:

A1.1. - Architectures
A2.4. - Formal method for verification, reliability, certification
A4. - Security and privacy
A7. - Theory of computation
A8. - Mathematics of computing

Other Research Topics and Application Domains:

B9.5. - Sciences
B9.10. - Privacy

1. Team, 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, from Oct 2018]
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, HDR]
Nicolas Louvet [Univ. Claude Bernard, Associate Professor]
Damien Stehlé [École Normale Supérieure de Lyon, Professor, HDR]

Post-Doctoral Fellows

Chitchanok Chuengsatiansup [Inria]
Junqing Gong [École Normale Supérieure de Lyon]
Alonso Gonzalez [École Normale Supérieure de Lyon]
Gottfried Herold [École Normale Supérieure de Lyon]
Elena Kirshanova [École Normale Supérieure de Lyon]
Changmin Lee [Univ. de Lyon, from Oct 2018]
Anastasiia Volkova Lozanova [Inria]
Alexandre Wallet [École Normale Supérieure de Lyon]

PhD Students

Florent Bréhard [École Normale Supérieure de Lyon]
Adel Hamdi [Orange Labs]
Fabrice Mouhartem [École Normale Supérieure de Lyon]
Huyen Nguyen [École Normale Supérieure de Lyon, intern, then PhD student from Sep 2018]
Alice Pellet–Mary [École Normale Supérieure de Lyon]

Chen Qian [École Normale Supérieure de Rennes]
Miruna Rosca [Bitdefender Romania, École Normale Supérieure de Lyon]
Radu Titiu [Bitdefender Romania, École Normale Supérieure de Lyon]
Ida Tucker [École Normale Supérieure de Lyon]
Weiqiang Wen [École Normale Supérieure de Lyon, until Aug 2018]

Technical staff

Laurent Grémy [École Normale Supérieure de Lyon]
Joris Picot [École Normale Supérieure de Lyon]

Interns

Joel Dahne [École Normale Supérieure de Lyon, June–July 2018]
Nicolas Fabiano [École Normale Supérieure Paris, June–August 2018]
Ana Maria Nanes [Inria, July–August 2018]
Aadil Oufkir [Univ. Claude Bernard, May–July 2018]

Administrative Assistants

Nelly Amsellem [École Normale Supérieure de Lyon, from Feb 2018]
Kadiatou Bangoura [École Normale Supérieure de Lyon]
Chiraz Benamor [École Normale Supérieure de Lyon]
Evelyne Blesle [Inria, until Jan 2018]

Visiting Scientists

Shi Bai [École Normale Supérieure de Lyon, May–July 2018]
Lloyd Nicholas Trefethen [École Normale Supérieure de Lyon, until Jul 2018]
Warwick Tucker [Univ. de Lyon, until Jul 2018]

2. Overall Objectives

2.1. Overall Objectives

The overall objective of AriC (Arithmetic and Computing) is, through computer arithmetic and computational mathematics, to improve computing at large.

A major challenge in modeling and scientific computing is the simultaneous mastery of hardware capabilities, software design, and mathematical algorithms for the efficiency of the computation. Further, performance relates as much to efficiency as to reliability, requiring progress on automatic proofs, certificates and code generation. In this context, computer arithmetic and mathematical algorithms are the keystones of AriC. Our approach conciliates fundamental studies, practical performance and qualitative aspects, with a shared strategy going from high-level problem specifications and normalization actions, to computer arithmetic and the lowest-level details of implementations.

We focus on 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 cryptology aspects, focus on the practicality of existing protocols and design of more powerful lattice-based primitives.
- Generalization of a hybrid symbolic-numeric trend, and interplay between arithmetics for both improving and controlling numerical approaches (symbolic $\rightarrow$ numeric), and accelerating exact solutions (symbolic $\longleftarrow$ 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 cryptology. 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. These themes also correspond to complementary angles for addressing the general computing challenge stated at the beginning of this introduction:

- **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 cryptology** (§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 approximation methods

3.1.1. Computer algebra generation of certified approximations

We plan to focus on the generation of certified and efficient approximations for solutions of linear differential equations. These functions cover many classical mathematical functions and many more can be built by combining them. One classical target area is the numerical evaluation of elementary or special functions. This is currently performed by code specifically handcrafted for each function. The computation of approximations and the error analysis are major steps of this process that we want to automate, in order to reduce the probability of errors, to allow one to implement “rare functions”, to quickly adapt a function library to a new context: new processor, new requirements – either in terms of speed or accuracy.

In order to significantly extend the current range of functions under consideration, several methods originating from approximation theory have to be considered (divergent asymptotic expansions; Chebyshev or generalized Fourier expansions; Padé approximants; fixed point iterations for integral operators). We have done preliminary work on some of them. Our plan is to revisit them all from the points of view of effectivity, computational complexity (exploiting linear differential equations to obtain efficient algorithms), as well as in their ability to produce provable error bounds. This work is to constitute a major progress towards the automatic generation of code for moderate or arbitrary precision evaluation with good efficiency. Other useful, if not critical, applications are certified quadrature, the determination of certified trajectories of spatial objects and many more important questions in optimal control theory.

3.1.2. Digital Signal Processing

As computer arithmeticians, a wide and important target for us is the design of efficient and certified linear filters in digital signal processing (DSP). Actually, following the advent of MATLAB as the major tool for filter design, the DSP experts now systematically delegate to MATLAB all the part of the design related to numerical issues. And yet, various key MATLAB routines are neither optimized, nor certified. Therefore, there is a lot of room for enhancing numerous DSP numerical implementations and there exist several promising approaches to do so.

The main challenge that we want to address over the next period is the development and the implementation of optimal methods for rounding the coefficients involved in the design of the filter. If done in a naive way, this rounding may lead to a significant loss of performance. We will study in particular FIR and IIR filters.

3.1.3. *Table Maker's Dilemma (TMD)*

Implementing "ultimately accurate" functions (i.e., rounded to nearest) requires either the knowledge of hardest-to-round cases, or an as tight as possible lower bound on the distance between the image of a floating-point number by the function and the middle of two consecutive floating-point numbers. Obtaining such results is a challenge. Several computer manufacturers have contacted us to obtain new cases. One of our current solutions for obtaining hardest-to-round cases is based on Lefèvre's algorithm. We aim at rewriting the current implementations of this algorithm, and giving formal proofs of their correction.

We plan to use uniform polynomial approximation and diophantine techniques in order to tackle the case of the IEEE quad precision, and continue to use analytic number theory techniques (exponential sums estimates) for counting the hardest-to-round cases.

3.2. Lattices: algorithms and cryptology

Lattice-based cryptography (LBC) is an utterly promising, attractive (and competitive) research ground in cryptography, thanks to a combination of unmatched properties:

- **Improved performance.** LBC primitives have low asymptotic costs, but remain cumbersome in practice (e.g., for parameters achieving security against computations of up to 2100 bit operations). To address this limitation, a whole branch of LBC has evolved where security relies on the restriction of lattice problems to a family of more structured lattices called *ideal lattices*. Primitives based on such lattices can have quasi-optimal costs (i.e., quasi-constant amortized complexities), outperforming all contemporary primitives. This asymptotic performance sometimes translates into practice, as exemplified by NTRUEncrypt.
- **Improved security.** First, lattice problems seem to remain hard even for quantum computers. Moreover, the security of most of LBC holds under the assumption that standard lattice problems are hard in the worst case. Oppositely, contemporary cryptography assumes that specific problems are hard with high probability, for some precise input distributions. Many of these problems were artificially introduced for serving as a security foundation of new primitives.
- **Improved flexibility.** The master primitives (encryption, signature) can all be realized based on worst-case (ideal) lattice assumptions. More evolved primitives such as ID-based encryption (where the public key of a recipient can be publicly derived from its identity) and group signatures, that were the playing-ground of pairing-based cryptography (a subfield of elliptic curve cryptography), can also be realized in the LBC framework, although less efficiently and with restricted security properties. More intriguingly, lattices have enabled long-wished-for primitives. The most notable example is homomorphic encryption, enabling computations on encrypted data. It is the appropriate tool to securely outsource computations, and will help overcome the privacy concerns that are slowing down the rise of the cloud.

We work on three directions, detailed now.

3.2.1. *Lattice algorithms*

All known lattice reduction algorithms follow the same design principle: perform a sequence of small elementary steps transforming a current basis of the input lattice, where these steps are driven by the Gram-Schmidt orthogonalisation of the current basis.

In the short term, we will fully exploit this paradigm, and hopefully lower the cost of reduction algorithms with respect to the lattice dimension. We aim at asymptotically fast algorithms with complexity bounds closer to those of basic and normal form problems (matrix multiplication, Hermite normal form). In the same vein, we plan to investigate the parallelism potential of these algorithms.

Our long term goal is to go beyond the current design paradigm, to reach better trade-offs between run-time and shortness of the output bases. To reach this objective, we first plan to strengthen our understanding of the interplay between lattice reduction and numerical linear algebra (how far can we push the idea of working on approximations of a basis?), to assess the necessity of using the Gram-Schmidt orthogonalisation (e.g., to obtain a weakening of LLL-reduction that would work up to some stage, and save computations), and to determine whether working on generating sets can lead to more efficient algorithms than manipulating bases. We will also study algorithms for finding shortest non-zero vectors in lattices, and in particular look for quantum accelerations.

We will implement and distribute all algorithmic improvements, e.g., within the fplll library. We are interested in high performance lattice reduction computations (see application domains below), in particular in connection with/continuation of the HPAC ANR project (algebraic computing and high performance consortium).

3.2.2. Lattice-based cryptography

Our long term goal is to demonstrate the superiority of lattice-based cryptography over contemporary public-key cryptographic approaches. For this, we will 1- Strengthen its security foundations, 2- Drastically improve the performance of its primitives, and 3- Show that lattices allow to devise advanced and elaborate primitives.

The practical security foundations will be strengthened by the improved understanding of the limits of lattice reduction algorithms (see above). On the theoretical side, we plan to attack two major open problems: Are ideal lattices (lattices corresponding to ideals in rings of integers of number fields) computationally as hard to handle as arbitrary lattices? What is the quantum hardness of lattice problems?

Lattice-based primitives involve two types of operations: sampling from discrete Gaussian distributions (with lattice supports), and arithmetic in polynomial rings such as $(\mathbb{Z}/q\mathbb{Z})[x]/(x^n+1)$ with n a power of 2. When such polynomials are used (which is the case in all primitives that have the potential to be practical), then the underlying algorithmic problem that is assumed hard involves ideal lattices. This is why it is crucial to precisely understand the hardness of lattice problems for this family. We will work on improving both types of operations, both in software and in hardware, concentrating on values of q and n providing security. As these problems are very arithmetic in nature, this will naturally be a source of collaboration with the other themes of the AriC team.

Our main objective in terms of cryptographic functionality will be to determine the extent to which lattices can help securing cloud services. For example, is there a way for users to delegate computations on their outsourced dataset while minimizing what the server eventually learns about their data? Can servers compute on encrypted data in an efficiently verifiable manner? Can users retrieve their files and query remote databases anonymously provided they hold appropriate credentials? Lattice-based cryptography is the only approach so far that has allowed to make progress into those directions. We will investigate the practicality of the current constructions, the extension of their properties, and the design of more powerful primitives, such as functional encryption (allowing the recipient to learn only a function of the plaintext message). To achieve these goals, we will in particular focus on cryptographic multilinear maps.

This research axis of AriC is gaining strength thanks to the recruitment of Benoit Libert. We will be particularly interested in the practical and operational impacts, and for this reason we envision a collaboration with an industrial partner.

3.2.3. Application domains

- Diophantine equations. Lattice reduction algorithms can be used to solve diophantine equations, and in particular to find simultaneous rational approximations to real numbers. We plan to investigate the interplay between this algorithmic task, the task of finding integer relations between real numbers, and lattice reduction. A related question is to devise LLL-reduction algorithms that exploit specific shapes of input bases.
- Communications. We will continue our collaboration with Cong Ling (Imperial College) on the use of lattices in communications. We plan to work on the wiretap channel over a fading channel (modeling cell phone communications in a fast moving environment). The current approaches rely

on ideal lattices, and we hope to be able to find new approaches thanks to our expertise on them due to their use in lattice-based cryptography. We will also tackle the problem of sampling vectors from Gaussian distributions with lattice support, for a very small standard deviation parameter. This would significantly improve current schemes for communication schemes based on lattices, as well as several cryptographic primitives.

- Cryptanalysis of variants of RSA. Lattices have been used extensively to break variants of the RSA encryption scheme, via Coppersmith's method to find small roots of polynomials. We plan to work with Nadia Heninger (U. of Pennsylvania) on improving these attacks, to make them more practical. This is an excellent test case for testing the practicality of LLL-type algorithm. Nadia Heninger has a strong experience in large scale cryptanalysis based on Coppersmith's method (http://smartfacts.cr.yp.to/)

3.3. Algebraic computing and high performance kernels

The main theme here is the study of fundamental operations ("kernels") on a hierarchy of symbolic or numeric data types spanning integers, floating-point numbers, polynomials, power series, as well as matrices of all these. Fundamental operations include basic arithmetic (e.g., how to multiply or how to invert) common to all such data, as well as more specific ones (change of representation/conversions, GCDs, determinants, etc.). For such operations, which are ubiquitous and at the very core of computing (be it numerical, symbolic, or hybrid numeric-symbolic), our goal is to ensure both high performance and reliability.

3.3.1. Algorithms

On the symbolic side, we will focus on the design and complexity analysis of algorithms for matrices over various domains (fields, polynomials, integers) and possibly with specific properties (structure). So far, our algorithmic improvements for polynomial matrices and structured matrices have been obtained in a rather independent way. Both types are well known to have much in common, but this is sometimes not reflected by the complexities obtained, especially for applications in cryptology and coding theory. Our goal in this area is thus to explore these connections further, to provide a more unified treatment, and eventually bridge these complexity gaps, A first step towards this goal will be the design of enhanced algorithms for various generalizations of Hermite-Padé approximation; in the context of list decoding, this should in particular make it possible to match or even improve over the structured-matrix approach, which is so far the fastest known.

On the other hand we will focus on the design of algorithms for certified computing. We will study the use of various representations, such as mid-rad for classical interval arithmetic, or affine arithmetic. We will explore the impact of precision tuning in intermediate computations, possibly dynamically, on the accuracy of the results (e.g. for iterative refinement and Newton iterations). We will continue to revisit and improve the classical error bounds of numerical linear algebra in the light of the subtleties of IEEE floating-point arithmetic.

Our goals in linear algebra and lattice basis reduction that have been detailed above in Section 3.2 will be achieved in the light of a hybrid symbolic-numeric approach.

3.3.2. Computer arithmetic

We aim at providing tight error bounds for basic "buiding blocks" of numerical computing. Examples are complex arithmetic (in the continuity of what we have already done), Fourier transforms.

We will also work on the interplay between floating-point and integer arithmetics. Currently, small numerical kernels like an exponential or a 2×2 determinant are typically written using exclusively one of these two kinds of arithmetic. However, modern processors now have hardware support for both floating-point and integer arithmetics, often with vector (SIMD) extensions, and an important question is how to make the best use of all such capabilities to optimize for both accuracy and efficiency.

A third direction will be to work on algorithms for performing correctly-rounded arithmetic operations in medium precision as efficiently and reliably as possible. Indeed, many numerical problems require higher precision than the conventional floating-point (single, double) formats. One solution is to use multiple precision libraries, such as GNU MPFR, which allow the manipulation of very high precision numbers, but their generality (they are able to handle numbers with millions of digits) is a quite heavy alternative when high performance is needed. Our objective here is thus to design a multiple precision arithmetic library that would allow to tackle problems where a precision of a few hundred bits is sufficient, but which have strong performance requirements. Applications include the process of long-term iteration of chaotic dynamical systems ranging from the classical Henon map to calculations of planetary orbits. The designed algorithms will be formally proved.

Finally, our work on the IEEE 1788 standard leads naturally to the development of associated reference libraries for interval arithmetic. A first direction will be to implement IEEE 1788 interval arithmetic within MPFI, our library for interval arithmetic using the arbitrary precision floating-point arithmetic provided by MPFR: indeed, MPFI has been originally developed with definitions and handling of exceptions which are not compliant with IEEE 1788. Another one will be to provide efficient support for multiple-precision intervals, in mid-rad representation and by developing MPFR-based code-generation tools aimed at handling families of functions.

3.3.3. High-performance algorithms and software

The algorithmic developments for medium precision floating-point arithmetic discussed above will lead to high performance implementations on GPUs. As a follow-up of the HPAC project (which ended in December 2015) we shall pursue the design and implementation of high performance linear algebra primitives and 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. Highlights of the Year

5.1.1. Awards

Damien Stehlé was nominated IUF junior member.

5.1.2. Book

Publication of the second edition of the “Handbook of Floating-Point Arithmetic” [43].

BEST PAPER AWARD:

[42]
G. VILLARD. *On Computing the Resultant of Generic Bivariate Polynomials*, in "ISSAC 2018, 43rd International Symposium on Symbolic and Algebraic Computation, New York, USA, July 16-19, 2018", New York, United States, July 2018, https://hal.archives-ouvertes.fr/hal-01921369

6. New Software and Platforms

6.1. 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.

- Author: Damien Stehlé
- Contact: Damien Stehlé
- URL: https://github.com/fplll/fplll

6.2. Gfun

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.

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

6.3. 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.

- Participants: Guillaume Hanrot, Paul Zimmermann, Philippe Théveny and Vincent Lefèvre
- Contact: Vincent Lefèvre
- Publications: Correctly Rounded Arbitrary-Precision Floating-Point Summation - Optimized Binary64 and Binary128 Arithmetic with GNU MPFR - Évaluation rapide de fonctions hypergéométriques - Arbitrary Precision Error Analysis for computing $\zeta(s)$ with the Cohen-Olivier algorithm: Complete description of the real case and preliminary report on the general case - MPFR: A Multiple-Precision Binary Floating-Point Library with Correct Rounding. - The Generic Multiple-Precision Floating-Point Addition With Exact Rounding (as in the MPFR Library)
- URL: https://www.mpfr.org/

6.4. 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.

- Participant: Vincent Lefèvre
- Contact: Vincent Lefèvre
- Publications: SIPE: Small Integer Plus Exponent - Sipe: a Mini-Library for Very Low Precision Computations with Correct Rounding
- URL: https://www.vinc17.net/research/sipe/

6.5. 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.

- Participants: Clément Pernet and Thierry Gautier
- Contact: Clément Pernet
- URL: http://linalg.org/

6.6. HPLLL

KEYWORDS: Euclidean Lattices - Computer algebra system (CAS)
FUNCTIONAL DESCRIPTION: Software library for linear algebra and Euclidean lattice problems

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

7. New Results

7.1. Efficient approximation methods

7.1.1. A High Throughput Polynomial and Rational Function Approximations Evaluator

In [21] we present an automatic method for the evaluation of functions via polynomial or rational approximations and its hardware implementation, on FPGAs. These approximations are evaluated using Ercegovac's iterative E-method adapted for FPGA implementation. The polynomial and rational function coefficients are optimized such that they satisfy the constraints of the E-method. We present several examples of practical interest; in each case a resource-efficient approximation is proposed and comparisons are made with alternative approaches.

7.1.2. Continued fractions in power series fields

In [4], we explicitly describe a noteworthy transcendental continued fraction in the field of power series over $\mathbb{Q}$, having irrationality measure equal to 3. This continued fraction is a generating function of a particular sequence in the set $\{1, 2\}$. The origin of this sequence, whose study was initiated in a recent paper, is to be found in another continued fraction, in the field of power series over $\mathbb{F}_3$, which satisfies a simple algebraic equation of degree 4, introduced thirty years ago by D. Robbins.

7.1.3. A Lattice Basis Reduction Approach for the Design of Finite Wordlength FIR Filters

Many applications of finite impulse response (FIR) digital filters impose strict format constraints for the filter coefficients. Such requirements increase the complexity of determining optimal designs for the problem at hand. In [6], we introduce a fast and efficient method, based on the computation of good nodes for polynomial interpolation and Euclidean lattice basis reduction. Experiments show that it returns quasi-optimal finite wordlength FIR filters; compared to previous approaches it also scales remarkably well (length 125 filters are treated in < 9s). It also proves useful for accelerating the determination of optimal finite wordlength FIR filters.

7.1.4. Validated and numerically efficient Chebyshev spectral methods for linear ordinary differential equations

In [7], we develop a validated numerics method for the solution of linear ordinary differential equations (LODEs). A wide range of algorithms (i.e., Runge-Kutta, collocation, spectral methods) exist for numerically computing approximations of the solutions. Most of these come with proofs of asymptotic convergence, but usually, provided error bounds are non-constructive. However, in some domains like critical systems and computer-aided mathematical proofs, one needs validated effective error bounds. We focus on both the theoretical and practical complexity analysis of a so-called *a posteriori* quasi-Newton validation method, which mainly relies on a fixed-point argument of a contracting map. Specifically, given a polynomial approximation, obtained by some numerical algorithm and expressed in Chebyshev basis, our algorithm efficiently computes an accurate and rigorous error bound. For this, we study theoretical properties like compactness, convergence, invertibility of associated linear integral operators and their truncations in a suitable coefficient space of Chebyshev series. Then, we analyze the almost-banded matrix structure of these operators, which allows for very efficient numerical algorithms for both numerical solutions of LODEs and rigorous computation of the approximation error. Finally, several representative examples show the advantages of our algorithms as well as their theoretical and practical limits.

7.1.5. Validated semi-analytical transition matrices for linearized relative spacecraft dynamics via Chebyshev series appproximations

In [14], we provide an efficient generic algorithm to compute validated approximations of transition matrices of linear time-variant systems using Chebyshev expansions, and apply it to two different examples of relative motion of satellites (spacecraft rendezvous with Tschauner-Hempel equations and geostationary station keeping with J2 perturbation in the linearized Orange model).

7.1.6. A Newton-like Validation Method for Chebyshev Approximate Solutions of Linear Ordinary Differential Systems

In [22], we provide a new framework for *a posteriori* validation of vector-valued problems with componentwise tight error enclosures, and use it to design a symbolic-numeric Newton-like validation algorithm for Chebyshev approximate solutions of coupled systems of linear ordinary differential equations. More precisely, given a coupled differential system with polynomial coefficients over a compact interval (or continuous coefficients rigorously approximated by polynomials) and componentwise polynomial approximate solutions in Chebyshev basis, the algorithm outputs componentwise rigorous upper bounds for the approximation errors, with respect to the uniform norm over the interval under consideration.

A complexity analysis shows that the number of arithmetic operations needed by this algorithm (in floating-point or interval arithmetics) is proportional to the approximation degree when the differential equation is considered fixed. Finally, we illustrate the efficiency of this fully automated validation method on an example of a coupled Airy-like system.

7.1.7. Fuel-optimal impulsive fixed-time trajectories in the linearized circular restricted 3-body-problem

In [41], the problem of fixed-time fuel-optimal trajectories with high-thrust propulsion in the vicinity of a Lagrange point is tackled via the linear version of the primer vector theory. More precisely, the proximity to a Lagrange point i.e. any equilibrium point-stable or not-in the circular restricted three-body problem allows for a linearization of the dynamics. Furthermore, it is assumed that the spacecraft has ungimbaled thrusters, leading to a formulation of the cost function with the 1-norm for space coordinates, even though a generalization exists for steerable thrust and the 2-norm. In this context, the primer vector theory gives necessary and sufficient optimality conditions for admissible solutions to two-value boundary problems. Similarly to the case of rendezvous in the restricted two-body problem, the in-plane and out-of-plane trajectories being uncoupled, they can be treated independently. As a matter of fact, the out-of-plane dynamics is simple enough for the optimal control problem to be solved analytically via this indirect approach. As for the in-plane dynamics, the primer vector solution of the so-called primal problem is derived by solving a hierarchy of linear programs, as proposed recently for the aforementioned rendezvous. The optimal thrusting strategy is then numerically obtained from the necessary and sufficient conditions. Finally, in-plane and out-of-plane control laws are combined to form the complete 3-D fuel-optimal solution. Results are compared to the direct approach that consists in working on a discrete set of times in order to perform optimization in finite dimension. Examples are provided near various Lagrange points in the Sun-Earth and Earth-Moon systems, hinting at the extensive span of possible applications of this technique in station-keeping as well as mission analysis, for instance when connecting manifolds to achieve escape or capture.

7.2. Floating-point and Validated Numerics

7.2.1. Optimal bounds on relative errors of floating-point operations

Rounding error analyses of numerical algorithms are most often carried out via repeated applications of the so-called standard models of floating-point arithmetic. Given a round-to-nearest function fl and barring underflow and overflow, such models bound the relative errors $E_1(t) = |t - fl(t)|/|t|$ and $E_2(t) = |t - fl(t)|/|fl(t)|$ by the unit roundoff u. In [10] we investigate the possibility and the usefulness of refining these bounds, both in the case of an arbitrary real t and in the case where t is the exact result of an arithmetic operation on some floating-point numbers. We show that $E_1(t)$ and $E_2(t)$ are optimally bounded by $u/(1 + u)$ and u, respectively, when t is real or, under mild assumptions on the base and the precision, when $t = x \pm y$ or $t = xy$ with x, y two floating-point numbers. We prove that while this remains true for division in base $\beta > 2$, smaller, attainable bounds can be derived for both division in base $\beta = 2$ and square root. This set of optimal bounds is then applied to the rounding error analysis of various numerical algorithms: in all cases, we obtain significantly shorter proofs of the best-known error bounds for such algorithms, and/or improvements on these bounds themselves.

7.2.2. On various ways to split a floating-point number

In [32] we review several ways to split a floating-point number, that is, to decompose it into the exact sum of two floating-point numbers of smaller precision. All the methods considered here involve only a few IEEE floating-point operations, with rounding to nearest and including possibly the fused multiply-add (FMA). Applications range from the implementation of integer functions such as `round` and `floor` to the computation of suitable scaling factors aimed, for example, at avoiding spurious underflows and overflows when implementing functions such as the hypotenuse.

7.2.3. Algorithms for triple-word arithmetic

Triple-word arithmetic consists in representing high-precision numbers as the unevaluated sum of three floating-point numbers. In [45], we introduce and analyze various algorithms for manipulating triple-word numbers. Our new algorithms are faster than what one would obtain by just using the usual floating-point expansion algorithms in the special case of expansions of length 3, for a comparable accuracy.

7.2.4. Error analysis of some operations involved in the Fast Fourier Transform

In [44], we are interested in obtaining error bounds for the classical 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.

7.3. Lattices: algorithms and cryptology

7.3.1. Reduction of orthogonal lattice bases

As a typical application, the LLL lattice basis reduction algorithm is applied to bases of the orthogonal lattice of a given integer matrix, via reducing lattice bases of a special type. With such bases in input, we have proposed in [26] a new technique for bounding from above the number of iterations required by the LLL algorithm. The main technical ingredient is a variant of the classical LLL potential, which could prove useful to understand the behavior of LLL for other families of input bases.

7.3.2. Lattice-Based Zero-Knowledge Arguments for Integer Relations

The paper [36] provides lattice-based protocols allowing to prove relations among committed integers. While the most general zero-knowledge proof techniques can handle arithmetic circuits in the lattice setting, adapting them to prove statements over the integers is non-trivial, at least if we want to handle exponentially large integers while working with a polynomial-size modulus q. For a polynomial L, the paper provides zero-knowledge arguments allowing a prover to convince a verifier that committed L-bit bitstrings x, y and z are the binary representations of integers X, Y and Z satisfying $Z = X + Y$ over $\mathbb{Z}$. The complexity of the new arguments is only linear in L. Using them, the paper constructs arguments allowing to prove inequalities $X < Z$ among committed integers, as well as arguments showing that a committed X belongs to a public interval $[\alpha, \beta]$, where α and β can be arbitrarily large. The new range arguments have logarithmic cost (i.e., linear in L) in the maximal range magnitude. Using these tools, the paper obtains zero-knowledge arguments showing that a committed element X does not belong to a public set S using $O(n \cdot \log |S|)$ bits of communication, where n is the security parameter. The paper finally gives a protocol allowing to argue that committed L-bit integers X, Y and Z satisfy multiplicative relations $Z = XY$ over the integers, with communication cost subquadratic in L. To this end, the paper uses its new protocol for integer addition to prove the correct recursive execution of Karatsuba's multiplication algorithm. The security of the new protocols relies on standard lattice assumptions with polynomial modulus and polynomial approximation factor.

7.3.3. Logarithmic-Size Ring Signatures With Tight Security from the DDH Assumption

Ring signatures make it possible for a signer to anonymously and, yet, convincingly leak a secret by signing a message while concealing his identity within a flexibly chosen ring of users. Unlike group signatures, they do not involve any setup phase or tracing authority. Despite a lot of research efforts in more than 15 years, most of their realizations require linear-size signatures in the cardinality of the ring. In the random oracle model, two recent constructions decreased the signature length to be only logarithmic in the number N of ring members. On the downside, their suffer from rather loose reductions incurred by the use of the Forking Lemma. This paper considers the problem of proving them tightly secure without affecting their space efficiency. Surprisingly, existing techniques for proving tight security in ordinary signature schemes do not trivially extend to the ring signature setting. The paper [37] overcomes these difficulties by combining the Groth-Kohlweiss Σ-protocol (Eurocrypt'15) with dual-mode encryption schemes. The main result is a fully tight construction based on the Decision Diffie-Hellman assumption in the random oracle model. By full tightness, we mean that the reduction's advantage is as large as the adversary's, up to a constant factor.

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. The paper [38] constructs the first fully non-interactive adaptively secure DPRF in the standard model. The construction is proved secure under the LWE assumption against adversaries that may adaptively decide which servers they want to corrupt. The new construction is also extended in order to achieve robustness against malicious adversaries.

7.3.5. Unbounded ABE via Bilinear Entropy Expansion, Revisited

This paper [24] presents simpler and improved constructions of unbounded attribute-based encryption (ABE) schemes with constant-size public parameters under static assumptions in bilinear groups. Concretely, we obtain: a simple and adaptively secure unbounded ABE scheme in composite-order groups, improving upon a previous construction of Lewko and Waters (Eurocrypt'11) which only achieves selective security; an improved adaptively secure unbounded ABE scheme based on the k-linear assumption in prime-order groups with shorter ciphertexts and secret keys than those of Okamoto and Takashima (Asiacrypt'12); the first adaptively secure unbounded ABE scheme for arithmetic branching programs under static assumptions. At the core of all of these constructions is a "bilinear entropy expansion" lemma that allows us to generate any polynomial amount of entropy starting from constant-size public parameters; the entropy can then be used to transform existing adaptively secure "bounded" ABE schemes into unbounded ones.

7.3.6. Improved Anonymous Broadcast Encryptions: Tight Security and Shorter Ciphertext

This paper [35] investigates anonymous broadcast encryptions (ANOBE) in which a ciphertext hides not only the message but also the target recipients associated with it. Following Libert et al.'s generic construction [PKC, 2012], we propose two concrete ANOBE schemes with tight reduction and better space efficiency.

- The IND-CCA security and anonymity of our two ANOBE schemes can be tightly reduced to standard k-Linear assumption (and the existence of other primitives). For a broadcast system with n users, Libert et al.'s security analysis suffers from $\mathcal{O}(n^3)$ loss while our security loss is constant.
- Our first ANOBE supports fast decryption and has a shorter ciphertext than the fast-decryption version of Libert et al.'s concrete ANOBE. Our second ANOBE is adapted from the first one. We sacrifice the fast decryption feature and achieve shorter ciphertexts than Libert et al.'s concrete ANOBE with the help of bilinear groups. Technically, we start from an instantiation of Libert et al.'s generic ANOBE [PKC, 2012], but we work out all our proofs from scratch instead of relying on their generic security result. This intuitively allows our optimizations in the concrete setting.

7.3.7. Compact IBBE and Fuzzy IBE from Simple Assumptions

This paper [29] proposes new constructions for identity-based broadcast encryption (IBBE) and fuzzy identity-based encryption (FIBE) in composite-order groups equipped with a bilinear pairing. Our starting point is the IBBE scheme of Delerablée (Asiacrypt 2007) and the FIBE scheme of Herranz et al. (PKC 2010) proven secure under parameterized assumptions called generalized decisional bilinear Diffie-Hellman (GDDHE) and augmented multi-sequence of exponents Diffie-Hellman (aMSE-DDH) respectively. The two schemes are described in the prime-order pairing group. We transform the schemes into the setting of (symmetric) composite-order groups and prove security from two static assumptions (subgroup decision). The Déjà Q framework of Chase et al. (Asiacrypt 2016) is known to cover a large class of parameterized assumptions (dubbed "Uber assumption"), that is, these assumptions, when defined in asymmetric composite-order groups, are implied by subgroup decision assumptions in the underlying composite-order groups. We argue that the GDDHE and aMSE-DDH assumptions are not covered by the Déjà Q uber assumption framework. We therefore work out direct security reductions for the two schemes based on subgroup decision assumptions. Furthermore, our proofs involve novel extensions of Déjà Q techniques of Wee (TCC 2016-A) and Chase et al. Our constructions have constant-size ciphertexts. The IBBE has constant-size keys as well and achieves a stronger security guarantee as compared to Delerablée's IBBE, thus making it the first compact IBBE known to be selectively secure without random oracles under simple assumptions. The fuzzy IBE scheme is the first to simultaneously feature constant-size ciphertexts and security under standard assumptions.

7.3.8. Improved Inner-product Encryption with Adaptive Security and Full Attribute-hiding

This paper [25] proposes two IPE schemes achieving both adaptive security and full attribute-hiding in the prime-order bilinear group, which improve upon the unique existing result satisfying both features from Okamoto and Takashima [Eurocrypt'12] in terms of efficiency.

- Our first IPE scheme is based on the standard k-Lin assumption and has shorter master public key and shorter secret keys than Okamoto and Takashima's IPE under weaker $DLIN$=2-lin assumption.
- Our second IPE scheme is adapted from the first one; the security is based on the XDLIN assumption (as Okamoto and Takashima's IPE) but now it also enjoys shorter ciphertexts.

Technically, instead of starting from composite-order IPE and applying existing transformation, we start from an IPE scheme in a very restricted setting but already in the prime-order group, and then gradually upgrade it to our full-fledged IPE scheme. This method allows us to integrate Chen et al.'s framework [Eurocrypt'15] with recent new techniques [TCC'17, Eurocrypt'18] in an optimized way.

7.3.9. Improved Security Proofs in Lattice-Based Cryptography: Using the Rényi Divergence Rather than the Statistical Distance

The Rényi divergence is a measure of closeness of two probability distributions. In this paper [5], we show that it can often be used as an alternative to the statistical distance in security proofs for lattice-based cryptography. Using the Rényi divergence is particularly suited for security proofs of primitives in which the attacker is required to solve a search problem (e.g., forging a signature). We show that it may also be used in the case of distinguishing problems (e.g., semantic security of encryption schemes), when they enjoy a public sampleability property. The techniques lead to security proofs for schemes with smaller parameters, and sometimes to simpler security proofs than the existing ones.

7.3.10. CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme

This paper [8] presents Dilithium, a lattice-based signature scheme that is part of the CRYSTALS (Cryptographic Suite for Algebraic Lattices) package that will be submitted to the NIST call for post-quantum standards. The scheme is designed to be simple to securely implement against side-channel attacks and to have comparable efficiency to the currently best lattice-based signature schemes. Our implementation results show that Dilithium is competitive with lattice schemes of the same security level and outperforms digital signature schemes based on other post-quantum assumptions.

7.3.11. On the asymptotic complexity of solving LWE

In this paper [9], we provide for the first time an asymptotic comparison of all known algorithms for the search version of the Learning with Errors (LWE) problem. This includes an analysis of several lattice-based approaches as well as the combinatorial BKW algorithm. Our analysis of the lattice-based approaches defines a general framework, in which the algorithms of Babai, Lindner–Peikert and several pruning strategies appear as special cases. We show that within this framework, all lattice algorithms achieve the same asymptotic complexity. For the BKW algorithm, we present a refined analysis for the case of only a polynomial number of samples via amplification, which allows for a fair comparison with lattice-based approaches. Somewhat surprisingly, such a small number of samples does not make the asymptotic complexity significantly inferior, but only affects the constant in the exponent. As the main result we obtain that both, lattice-based techniques and BKW with a polynomial number of samples, achieve running time $2^{O(n)}$ for n-dimensional LWE, where we make the constant hidden in the big-O notion explicit as a simple and easy to handle function of all LWE-parameters. In the lattice case this function also depends on the time to compute a BKZ lattice basis with block size $\Theta(n)$. Thus, from a theoretical perspective our analysis reveals how LWE 's complexity changes as a function of the LWE-parameters, and from a practical perspective our analysis is a useful tool to choose LWE-parameters resistant to all currently known attacks.

7.3.12. Measuring, Simulating and Exploiting the Head Concavity Phenomenon in BKZ

The Blockwise-Korkine-Zolotarev (BKZ) lattice reduction algorithm is central in cryptanalysis, in particular for lattice-based cryptography. A precise understanding of its practical behavior in terms of run-time and output quality is necessary for parameter selection in cryptographic design. As the provable worst-case bounds poorly reflect the practical behavior, cryptanalysts rely instead on the heuristic BKZ simulator of Chen and Nguyen (Asiacrypt'11). It fits better with practical experiments, but not entirely. In particular, it over-estimates the norm of the first few vectors in the output basis. Put differently, BKZ performs better than its Chen-Nguyen simulation.

In this article [15], we first report experiments providing more insight on this shorter-than-expected phenomenon. We then propose a refined BKZ simulator by taking the distribution of short vectors in random lattices into consideration. We report experiments suggesting that this refined simulator more accurately predicts the concrete behavior of BKZ. Furthermore, we design a new BKZ variant that exploits the shorter-than-expected phenomenon. For the same cost assigned to the underlying SVP-solver, the new BKZ variant produces bases of better quality. We further illustrate its potential impact by testing it on the SVP-120 instance of the Darmstadt lattice challenge.

7.3.13. CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM

Rapid advances in quantum computing, together with the announcement by the National Institute of Standards and Technology (NIST) to define new standards for digital signature, encryption, and key-establishment protocols, have created significant interest in post-quantum cryptographic schemes. This paper [17] introduces Kyber (part of CRYSTALS - Cryptographic Suite for Algebraic Lattices - a package submitted to NIST post-quantum standardization effort in November 2017), a portfolio of post-quantum cryptographic primitives built around a key-encapsulation mechanism (KEM), based on hardness assumptions over module lattices. Our KEM is most naturally seen as a successor to the NEWHOPE KEM (Usenix 2016). In particular, the key and ciphertext sizes of our new construction are about half the size, the KEM offers CCA instead of only passive security, the security is based on a more general (and flexible) lattice problem, and our optimized implementation results in essentially the same running time as the aforementioned scheme. We first introduce a CPA-secure public-key encryption scheme, apply a variant of the Fujisaki-Okamoto transform to create a CCA-secure KEM, and eventually construct, in a black-box manner, CCA-secure encryption, key exchange, and authenticated-key-exchange schemes. The security of our primitives is based on the hardness of Module-LWE in the classical and quantum random oracle models, and our concrete parameters conservatively target more than 128 bits of postquantum security.

7.3.14. Learning with Errors and Extrapolated Dihedral Cosets

The hardness of the learning with errors (LWE) problem is one of the most fruitful resources of modern cryptography. In particular, it is one of the most prominent candidates for secure post-quantum cryptography. Understanding its quantum complexity is therefore an important goal. In this paper [20], we show that under quantum polynomial time reductions, LWE is equivalent to a relaxed version of the dihedral coset problem (DCP), which we call extrapolated DCP (eDCP). The extent of extrapolation varies with the LWE noise rate. By considering different extents of extrapolation, our result generalizes Regev's famous proof that if DCP is in BQP (quantum poly-time) then so is LWE (FOCS'02). We also discuss a connection between eDCP and Childs and Van Dam's algorithm for generalized hidden shift problems (SODA'07). Our result implies that a BQP solution for LWE might not require the full power of solving DCP, but rather only a solution for its relaxed version, eDCP, which could be easier.

7.3.15. Pairing-friendly twisted Hessian curves

This paper [27] presents efficient formulas to compute Miller doubling and Miller addition utilizing degree-3 twists on curves with j-invariant 0 written in Hessian form. We give the formulas for both odd and even embedding degrees and for pairings on both $G_1 \times G_2$ and $G_2 \times G_1$. We propose the use of embedding degrees 15 and 21 for 128-bit and 192-bit security respectively in light of the NFS attacks and their variants. We give a comprehensive comparison with other curve models; our formulas give the fastest known pairing computation for embedding degrees 15, 21, and 24.

7.3.16. On the Statistical Leak of the GGH13 Multilinear Mapand some Variants

At EUROCRYPT 2013, Garg, Gentry and Halevi proposed a candidate construction (later referred as GGH13) of cryptographic multilinear map (MMap). Despite weaknesses uncovered by Hu and Jia (EUROCRYPT 2016), this candidate is still used for designing obfuscators. The naive version of the GGH13 scheme was deemed susceptible to averaging attacks, i.e., it could suffer from a statistical leak (yet no precise attack was described). A variant was therefore devised, but it remains heuristic. Recently, to obtain MMaps with low noise and modulus, two variants of this countermeasure were developed by Döttling et al. (EPRINT:2016/599). In this work [28], we propose a systematic study of this statistical leak for all these GGH13 variants. In particular, we confirm the weakness of the naive version of GGH13. We also show that, among the two variants proposed by Döttling et al., the so-called conservative method is not so effective: it leaks the same value as the unprotected method. Luckily, the leak is more noisy than in the unprotected method, making the straightforward attack unsuccessful. Additionally, we note that all the other methods also leak values correlated with secrets. As a conclusion, we propose yet another countermeasure, for which this leak is made unrelated to all secrets. On our way, we also make explicit and tighten the hidden exponents in the size of the parameters, as an effort to assess and improve the efficiency of MMaps.

7.3.17. Higher dimensional sieving for the number field sieve algorithms

Since 2016 and the introduction of the exTNFS (extended tower number field sieve) algorithm, the security of cryptosystems based on nonprime finite fields, mainly the pairing- and torus-based ones, is being reassessed. The feasibility of the relation collection, a crucial step of the NFS variants, is especially investigated. It usually involves polynomials of degree 1, i.e., a search space of dimension 2. However, exTNFS uses bivariate polynomials of at least four coefficients. If sieving in dimension 2 is well described in the literature, sieving in higher dimensions has received significantly less attention. In this work [30], we describe and analyze three different generic algorithms to sieve in any dimension for the NFS algorithms. Our implementation shows the practicability of dimension-4 sieving, but the hardness of dimension-6 sieving.

7.3.18. Speed-Ups and Time-Memory Trade-Offs for Tuple Lattice Sieving

In this work [31], we study speed-ups and time–space trade-offs for solving the shortest vector problem (SVP) on Euclidean lattices based on tuple lattice sieving. Our results extend and improve upon previous work of Bai–Laarhoven–Stehlé [ANTS'16] and Herold–Kirshanova [PKC'17], with better complexities for arbitrary tuple sizes and offering tunable time–memory tradeoffs. The trade-offs we obtain stem from the generalization and combination of two algorithmic techniques: the configuration framework introduced by Herold–Kirshanova, and the spherical locality-sensitive filters of Becker–Ducas–Gama–Laarhoven [SODA'16]. When the available memory scales quasi-linearly with the list size, we show that with triple sieving we can solve SVP in dimension n in time $2^{0.3588n+o(n)}$ and space $2^{0.1887n+o(n)}$, improving upon the previous best triple sieve time complexity of $2^{0.3717n+o(n)}$ of Herold–Kirshanova. Using more memory we obtain better asymptotic time complexities. For instance, we obtain a triple sieve requiring only $2^{0.3300n+o(n)}$ time and $2^{0.2075n+o(n)}$ memory to solve SVP in dimension n. This improves upon the best double Gauss sieve of Becker–Ducas–Gama–Laarhoven, which runs in $2^{0.3685n+o(n)}$ time when using the same amount of space.

7.3.19. Improved Quantum Information Set Decoding

In this paper [34], we present quantum information set decoding (ISD) algorithms for binary linear codes. First, we refine the analysis of the quantum walk based algorithms proposed by Kachigar and Tillich (PQCrypto'17). This refinement allows us to improve the running time of quantum decoding in the leading order term: for an n-dimensional binary linear code the complexity of May-Meurer-Thomae ISD algorithm (Asiacrypt'11) drops down from $2^{0.05904n+o(n)}$ to $2^{0.05806n+o(n)}$. Similar improvement is achieved for our quantum version of Becker-JeuxMay-Meurer (Eurocrypt'12) decoding algorithm. Second, we translate May-Ozerov Near Neighbour technique (Eurocrypt'15) to an 'updateand-query' language more common in a similarity search literature. This re-interpretation allows us to combine Near Neighbour search with the quantum walk framework and use both techniques to improve a quantum version of Dumer's ISD algorithm: the running time goes down from $2^{0.059962n+o(n)}$ to $2^{0.059450+o(n)}$.

7.3.20. Quantum Attacks against Indistinguishablility Obfuscators Proved Secure in the Weak Multilinear Map Model

We present in [39] a quantum polynomial time attack against the GMMSSZ branching program obfuscator of Garg et al. (TCC'16), when instantiated with the GGH13 multilinear map of Garg et al. (EUROCRYPT'13). This candidate obfuscator was proved secure in the weak multilinear map model introduced by Miles et al. (CRYPTO'16). Our attack uses the short principal ideal solver of Cramer et al. (EUROCRYPT'16), to recover a secret element of the GGH13 multilinear map in quantum polynomial time. We then use this secret element to mount a (classical) polynomial time mixed-input attack against the GMMSSZ obfuscator. The main result of this article can hence be seen as a classical reduction from the security of the GMMSSZ obfuscator to the short principal ideal problem (the quantum setting is then only used to solve this problem in polynomial time). As an additional contribution, we explain how the same ideas can be adapted to mount a quantum polynomial time attack against the DGGMM obfuscator of Döttling et al. (ePrint 2016), which was also proved secure in the weak multilinear map model.

7.3.21. On the Ring-LWE and Polynomial-LWE Problems

The Ring Learning With Errors problem (RLWE) comes in various forms. Vanilla RLWE is the decision dual-RLWE variant, consisting in distinguishing from uniform a distribution depending on a secret belonging to the dual $O_K^\vee$ of the ring of integers O_K of a specified number field K. In primal-RLWE, the secret instead belongs to O_K. Both decision dual-RLWE and primal-RLWE enjoy search counterparts. Also widely used is (search/decision) Polynomial Learning With Errors (PLWE), which is not defined using a ring of integers O_K of a number field K but a polynomial ring $Z[x]/f$ for a monic irreducible $f \in Z[x]$. We show that there exist reductions between all of these six problems that incur limited parameter losses. More precisely: we prove that the (decision/search) dual to primal reduction from Lyubashevsky et al. [EUROCRYPT 2010] and Peikert [SCN 2016] can be implemented with a small error rate growth for all rings (the resulting reduction is nonuniform polynomial time); we extend it to polynomial-time reductions between (decision/search) primal RLWE and PLWE that work for a family of polynomials f that is exponentially large as a function of deg(f) (the resulting reduction is also non-uniform polynomial time); and we exploit the recent technique from Peikert et al. [STOC 2017] to obtain a search to decision reduction for RLWE for arbitrary number fields. The reductions incur error rate increases that depend on intrinsic quantities related to K and f.

7.3.22. Non-Trivial Witness Encryption and Null-iO from Standard Assumptions

A *witness encryption (WE)* scheme can take any NP statement as a public-key and use it to encrypt a message. If the statement is true then it is possible to decrypt the message given a corresponding witness, but if the statement is false then the message is computationally hidden. Ideally, the encryption procedure should run in polynomial time, but it is also meaningful to define a weaker notion, which we call *non-trivially exponentially efficient* WE (XWE), where the encryption run-time is only required to be much smaller than the trivial 2^m bound for NP relations with witness size m. In [19], we show how to construct such XWE schemes for all of NP with encryption run-time $2^{m/2}$ under the sub-exponential learning with errors (LWE) assumption. For NP relations that can be verified in NC^1 (e.g., SAT) we can also construct such XWE schemes under the sub-exponential Decisional Bilinear Diffie-Hellman (DBDH) assumption. Although we find the result surprising, it follows via a very simple connection to *attribute-based encryption*.

We also show how to upgrade the above results to get non-trivially exponentially efficient *indistinguishability obfuscation for null circuits (niO)*, which guarantees that the obfuscations of any two circuits that always output 0 are indistinguishable. In particular, under the LWE assumptions we get a XniO scheme where the obfuscation time is $2^{n/2}$ for all circuits with input size n. It is known that in the case of indistinguishability obfuscation (iO) for all circuits, non-trivially efficient XiO schemes imply fully efficient iO schemes (Lin et al., PKC 2016) but it remains as a fascinating open problem whether any such connection exists for WE or niO.

Lastly, we explore a potential approach toward constructing fully efficient WE and niO schemes via multi-input ABE.

7.3.23. Function-Revealing Encryption

Multi-input functional encryption is a paradigm that allows an authorized user to compute a certain function—and nothing more—over multiple plaintexts given only their encryption. The particular case of two-input functional encryption has very exciting applications, including comparing the relative order of two plaintexts from their encrypted form (order-revealing encryption).

While being extensively studied, multi-input functional encryption is not ready for a practical deployment, mainly for two reasons. First, known constructions rely on heavy cryptographic tools such as multilinear maps. Second, their security is still very uncertain, as revealed by recent devastating attacks.

In [33], we investigate a simpler approach towards obtaining practical schemes for functions of particular interest. We introduce the notion of function-revealing encryption, a generalization of order-revealing encryption to any multi-input function as well as a relaxation of multi-input functional encryption. We then propose a simple construction of order-revealing encryption based on function-revealing encryption for simple functions, namely orthogonality testing and intersection cardinality. Our main result is an efficient order-revealing encryption scheme with limited leakage based on the standard DLin assumption.

7.3.24. Exploring Crypto Dark Matter: New Simple PRF Candidates and Their Applications

Pseudorandom functions (PRFs) are one of the fundamental building blocks in cryptography. We explore a new space of plausible PRF candidates that are obtained by mixing linear functions over different small moduli. Our candidates are motivated by the goals of maximizing simplicity and minimizing complexity measures that are relevant to cryptographic applications such as secure multiparty computation.

In [16], we present several concrete new PRF candidates that follow the above approach. Our main candidate is a *weak* PRF candidate (whose conjectured pseudorandomness only holds for uniformly random inputs) that first applies a secret mod-2 linear mapping to the input, and then a public mod-3 linear mapping to the result. This candidate can be implemented by depth-2 ACC^0 circuits. We also put forward a similar depth-3 *strong* PRF candidate. Finally, we present a different weak PRF candidate that can be viewed as a deterministic variant of “Learning Parity with Noise” (LPN) where the noise is obtained via a mod-3 inner product of the input and the key.

The advantage of our approach is twofold. On the theoretical side, the simplicity of our candidates enables us to draw natural connections between their hardness and questions in complexity theory or learning theory (e.g., learnability of depth-2 ACC^0 circuits and width-3 branching programs, interpolation and property testing for sparse polynomials, and natural proof barriers for showing super-linear circuit lower bounds). On the applied side, the "piecewise-linear" structure of our candidates lends itself nicely to applications in secure multiparty computation (MPC). Using our PRF candidates, we construct protocols for distributed PRF evaluation that achieve better round complexity and/or communication complexity (often both) compared to protocols obtained by combining standard MPC protocols with PRFs like AES, LowMC, or Rasta (the latter two are specialized MPC-friendly PRFs). Our advantage over competing approaches is maximized in the setting of MPC with an honest majority, or alternatively, MPC with preprocessing.

Finally, we introduce a new primitive we call an *encoded-input PRF*, which can be viewed as an interpolation between weak PRFs and standard (strong) PRFs. As we demonstrate, an encoded-input PRF can often be used as a drop-in replacement for a strong PRF, combining the efficiency benefits of weak PRFs and the security benefits of strong PRFs. We conclude by showing that our main weak PRF candidate can plausibly be boosted to an encoded-input PRF by leveraging error-correcting codes.

7.3.25. Related-Key Security for Pseudorandom Functions Beyond the Linear Barrier

Related-key attacks (RKAs) concern the security of cryptographic primitives in the situation where the key can be manipulated by the adversary. In the RKA setting, the adversary's power is expressed through the class of related-key deriving (RKD) functions which the adversary is restricted to using when modifying keys. Bellare and Kohno (Eurocrypt 2003) first formalised RKAs and pin-pointed the foundational problem of constructing RKA-secure pseudorandom functions (RKA-PRFs). To date there are few constructions for RKA-PRFs under standard assumptions, and it is a major open problem to construct RKA-PRFs for larger classes of RKD functions. We make significant progress on this problem. In [3], we first show how to repair the Bellare-Cash framework for constructing RKA-PRFs and extend it to handle the more challenging case of classes of RKD functions that contain claws. We apply this extension to show that a variant of the NaorReingold function already considered by Bellare and Cash is an RKA-PRF for a class of affine RKD functions under the DDH assumption, albeit with an exponential-time security reduction. We then develop a second extension of the Bellare-Cash framework, and use it to show that the same Naor-Reingold variant is actually an RKA-PRF for a class of degree d polynomial RKD functions under the stronger decisional d-Diffie-Hellman inversion assumption. As a significant technical contribution, our proof of this result avoids the exponential-time security reduction that was inherent in the work of Bellare and Cash and in our first result.

7.3.26. Practical Fully Secure Unrestricted Inner Product Functional Encryption modulo p

In [23], we provide adaptively secure functional encryption schemes for the inner product functionality which are both efficient and allow for the evaluation of unbounded inner products modulo a prime p. Our constructions rely on new natural cryptographic assumptions in a cyclic group containing a subgroup where the discrete logarithm (DL) problem is easy which extend Castagnos and Laguillaumie's assumption (RSA 2015) of a DDH group with an easy DL subgroup. Instantiating our generic construction using class groups of imaginary quadratic fields gives rise to the most efficient functional encryption for inner products modulo an arbitrary large prime p. One of our schemes outperforms the DCR variant of Agrawal et al.'s protocols in terms of size of keys and ciphertexts by factors varying between 2 and 20 for a 112-bit security.

7.4. Algebraic computing and high-performance kernels

7.4.1. Generalized Hermite Reduction, Creative Telescoping and Definite Integration of D-Finite Functions

Hermite reduction is a classical algorithmic tool in symbolic integration. It is used to decompose a given rational function as a sum of a function with simple poles and the derivative of another rational function. In [18], we extend Hermite reduction to arbitrary linear differential operators instead of the pure derivative, and develop efficient algorithms for this reduction. We then apply the generalized Hermite reduction to the computation of linear operators satisfied by single definite integrals of D-finite functions of several continuous or discrete parameters. The resulting algorithm is a generalization of reduction-based methods for creative telescoping.

7.4.2. Hermite-Padé approximant bases

In [46] we design fast algorithms for the computation of approximant bases in shifted Popov normal form. For K a commutative field, let F be a matrix in $\mathsf{K}[x]^{m \times n}$ (truncated power series) and $\overrightarrow{d}$ be a degree vector, the problem is to compute a basis $P \in \mathsf{K}[x]^{m \times m}$ of the $\mathsf{K}[x]$-module of the relations $p \in \mathsf{K}[x]^{1 \times m}$ such that $p(x) \cdot F(x) \equiv 0 \mod x^{\overrightarrow{d}}$. We obtain improved complexity bounds for handling arbitrary (possibly highly unbalanced) vectors $\overrightarrow{d}$. We also improve upon previously known algorithms for computing P in normalized shifted form for an arbitrary shift. Our approach combines a recent divide and conquer strategy which reduces the general case to the case where information on the output degree is available, and partial linearizations of the involved matrices.

7.4.3. Resultant of bivariate polynomials

We have proposed in [42] an algorithm for computing the resultant of two generic bivariate polynomials over a field K. For such p and q in $\mathsf{K}[x, y]$ both of degree d in x and n in y, the algorithm computes the resultant with respect to y using $(n^{2-1/\omega}d)^{1+o(1)}$ arithmetic operations, where ω is the exponent of matrix multiplication. Previous algorithms from the early 1970's required time $(n^2 d)^{1+o(1)}$. We have also described some extensions of the approach to the computation of generic Gröbner bases and of characteristic polynomials of generic structured matrices and in univariate quotient algebras.

7.4.4. Recursive Combinatorial Structures: Enumeration, Probabilistic Analysis and Random Generation

The probabilistic behaviour of many data-structures, like series-parallel graphs used as a running example is this tutorial [13], can be analysed very precisely, thanks to a set of high-level tools provided by Analytic Combinatorics, as described in the book by Flajolet and Sedgewick. In this framework, recursive combinatorial definitions lead to generating function equations from which efficient algorithms can be designed for enumeration, random generation and, to some extent, asymptotic analysis. With a focus on random generation, this tutorial given at STACS first covers the basics of Analytic Combinatorics and then describes the idea of Boltzmann sampling and its realisation. The tutorial addresses a broad TCS audience and no particular pre-knowledge on analytic combinatorics is expected.

7.4.5. Linear Differential Equations as a Data-Structure

A lot of information concerning solutions of linear differential equations can be computed directly from the equation. It is therefore natural to consider these equations as a data-structure, from which mathematical properties can be computed. A variety of algorithms has thus been designed in recent years that do not aim at "solving", but at computing with this representation. Many of these results are surveyed in [11].

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

Bosch (Germany) ordered from us some support for implementing complex numerical algorithms (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 is PhD with Orange Labs and is supervised by Fabien Laguillaumie. He is working on advanced encryption protocols for the cloud.

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR DYNA3S Project

Participants: Guillaume Hanrot, Gilles Villard.

Dyna3S has been a 2013-2018 ANR project headed by Valérie Berthé (IRIF, U. Paris 7). The Web page of the project is https://www.irif.fr/~dyna3s. The aim of Dyna3S was to study algorithms that compute the greatest common divisor (gcd) from the point of view of dynamical systems. A gcd algorithm is considered as a discrete dynamical system by focusing on integer input. In Lyon we have worked on the computation of the gcd of several integers, in link with integer relation algorithms based on lattice basis reduction. A main motivation of Dyna3S was also discrete geometry, a framework where the understanding of basic primitives, discrete lines and planes, relies on algorithms of the Euclidean type.

9.1.2. ANR FastRelax Project

Participants: Nicolas Brisebarre, Guillaume Hanrot, Vincent Lefèvre, Jean-Michel Muller, Bruno Salvy, Serge Torres.

FastRelax stands for "Fast and Reliable Approximation". It is a four year ANR project (started in October 2014 and extended till September 2019). The web page of the project is http://fastrelax.gforge.inria.fr/. It is headed by B. Salvy and involves AriC as well as members of the Marelle Team (Sophia), of the Mac group (LAAS, Toulouse), of the Specfun and Toccata Teams (Saclay), as well as of the Pequan group in UVSQ and a colleague in the Plume group of LIP.

The aim of this project is to develop computer-aided proofs of numerical values, with certified and reasonably tight error bounds, without sacrificing efficiency. Applications to zero-finding, numerical quadrature or global optimization can all benefit from using our results as building blocks. We expect our work to initiate a "fast and reliable" trend in the symbolic-numeric community. This will be achieved by developing interactions between our fields, designing and implementing prototype libraries and applying our results to concrete problems originating in optimal control theory.

9.1.3. ANR MetaLibm Project

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

MetaLibm is a four-year project (started in October 2013 and extended till March 2018) focused on the design and implementation of code generators for mathematical functions and filters. The web page of the project is http://www.metalibm.org/ANRMetaLibm/. It is headed by Florent de Dinechin (INSA Lyon and Socrate team) and, besides Socrate and AriC, also involves teams from LIRMM (Perpignan), LIP6 (Paris), CERN (Geneva), and Kalray (Grenoble). The main goals of the project are to automate the development of mathematical libraries (libm), to extend it beyond standard functions, and to make it unified with similar approaches developed in or useful for signal processing (filter design). Within AriC, we are especially interested in studying the properties of fixed-point arithmetic and floating-point arithmetic that can help develop such a framework.

9.1.4. ANR ALAMBIC Project

Participants: Benoît Libert, Fabien Laguillaumie, Ida Tucker.

ALAMBIC is a four-year project (started in October 2016) focused on the applications of cryptographic primitives with homomorphic or malleability properties. 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.

9.1.5. RISQ Project

Participants: Chitchanok Chuengsatiansup, 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.

9.2. European Initiatives

9.2.1. LattAC ERC grant

Participants: Shi Bai, Laurent Grémy, Gottfried Herold, Elena Kirshanova, Fabien Laguillaumie, Huyen Nguyen, Alice Pellet–Mary, Miruna Rosca, Damien Stehlé, Alexandre Wallet, Weiqiang Wen.

Damien Stehlé was awarded an ERC Starting Grant for his project *Euclidean lattices: algorithms and cryptography* (LattAC) in 2013 (1.4Meur for 5 years from January 2014). The LattAC project aims at studying all computational aspects of lattices, from algorithms for manipulating them to applications. The main objective is to enable the rise of lattice-based cryptography.

9.2.2. PROMETHEUS Project

Participants: Laurent Grémy, Fabien Laguillaumie, Benoît Libert, Damien Stehlé.

PROMETHEUS (Privacy-Preserving Systems from Advanced Cryptographic Mechanisms Using Lattices) is a 4-year European H2020 project (call H2020-DS-2016-2017, Cybersecurity PPP Cryptography, DS-06-2017) that started in January 2018. It gathers 8 academic partners (ENS de Lyon and Université de Rennes 1; CWI, Pays-Bas; IDC Herzliya, Israel; Royal Holloway University of London, United Kingdom; Universitat Politècnica de Catalunya, Spain; Ruhr-Universität Bochum, Germany; Weizmann Institute, Israel), 4 industrial partners (Orange, Thales, TNO, Scytl). The goal of this project 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 will be mainly considered in the context of Euclidean lattices and they will be 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). The project is hosted by ENS de Lyon and Benoît Libert is the administrative coordinator while Orange is the scientific leader.

9.2.3. *Other international projects*

9.2.3.1. IFCPAR grant: “Computing on Encrypted Data: New Paradigms in Functional Encryption”

Participants: Benoît Libert, Damien Stehlé.

3-year project accepted in July 2018. Expected beginning on January 1, 2019. Benoît Libert is co-PI with Shweta Agrawal (IIT Madras, India). Budget on the French side amounts to 100k€.

Functional encryption is a paradigm that enables users to perform data mining and analysis on encrypted data. Users are provided cryptographic keys corresponding to particular functionalities which enable them to learn the output of the computation without learning anything about the input. Despite recent advances, efficient realizations of functional encryption are only available for restricted function families, which are typically represented by small-depth circuits: indeed, solutions for general functionalities are either way too inefficient for pratical use or they rely on uncertain security foundations like the existence of circuit obfuscators (or both). This project will explore constructions based on well-studied hardness assumptions and which are closer to being usable in real-life applications. To this end, we will notably consider solutions supporting other models of computation than Boolean circuits – like Turing machines – which support variable-size inputs. In the context of particular functionalities, the project will aim for more efficient realizations that satisfy stronger security notions.

9.3. International Initiatives

9.3.1. *Participation in International Programs*

Vincent Lefèvre actively participated in the revision of the IEEE Standard for Floating-Point Arithmetic (IEEE 754) for 2019.

9.4. International Research Visitors

9.4.1. *Visits of International Scientists*

- Lloyd Nicholas Trefethen, from Oxford University (UK), is an expert in numerical analysis and notably the systematic use of Chebyshev approximation. He spent the academic year 2017-2018 with AriC.
- Warwick Tucker, from Uppsala University (Sweden), is an expert of certified computation for dynamical systems. He spent the academic year 2017-2018 with AriC.

9.4.2. *Internships*

Monosij Maitra, PhD student at IIT Madras (India) under the supervision of Shweta Agrawal, did a 2-month internship, in September and October 2018.

Joel Dahne did an internship with Bruno Salvy from May to July.

9.4.3. *Visits to International Teams*

- From November 15 to December 15, 2018, Benoît Libert visited the “Cryptography and Coding Research Group” of the Nanyang Technological University (Singapore).
- From July 1 to July 31, 2018, Damien Stehlé visited the cryptography group of Prof. Jung Hee Cheon, at Seoul National University (South Korea)

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. *Scientific Events Organisation*

10.1.1.1. Member of Organizing Committees

- Claude-Pierre Jeannerod and Gilles Villard organized the workshop "Structured Matrix Days" (May 14–15, ENS de Lyon, France).
- Fabien Laguillaumie and Damien Stehlé organized the National Codes and Cryptography Days (Journées C2), in Aussois, France.
- Nathalie Revol co-organized the "École Jeunes Chercheurs et Jeunes Chercheuses en Programmation" (June 25–28, ENS de Lyon, France).
- Bruno Salvy is a co-chair of AofA'2019 (Analysis of Algorithms), in Luminy, France.

10.1.2. Scientific Events Selection

10.1.2.1. Member of Conference Program Committees

Chitchanok Chuengsatiansup was in the program committee of CRYPTO 2018.

Gottfried Herold was in the program committee of INDOCRYPT 2018.

Elena Kirshanova was in the program committee of INDOCRYPT 2018.

Benoît Libert was in the program committees of ACNS 2018, SCN 2018, Asiacrypt 2018, PKC 2019.

Jean-Michel Muller was in the program committee of Arith'25 and ASAP'2018.

Alain Passelègue was in the program committee of PKC 2018.

Nathalie Revol was in the program committee of Arith'25, of SCAN 2018 and of Correctness 2018.

Bruno Salvy was in the program committee for AofA'2018, is in the program committee of FPSAC 2019, in the steering committee of AofA and in the scientific committee of OPSFA 2019.

Damien Stehlé was in the program committees of Eurocrypt 2018, SCN 2018, PQCrypto 2018 and PQCrypto 2019. He is in the steering committee of the PQCrypto conference series.

Fabien Laguillaumie was in the program committee of ACISP 2018

10.1.3. Journals

Jean-Michel Muller is associate editor of the IEEE Transactions on Computers.

Nathalie Revol is a member of the editorial board of Reliable Computing.

Damien Stehlé is a member of the editorial board of the IACR Journal of Cryptology.

Bruno Salvy and Gilles Villard are members of the editorial board of Journal of Symbolic Computation.

Bruno Salvy is a member of the editorial board of the collection *Text and Monographs in Symbolic Computation* (Springer) and has been for 10 years in the editorial board of the *Journal of Algebra* (section Computational Algebra), which he left in March.

10.1.4. Invited Talks

- Claude-Pierre Jeannerod gave an invited talk *Recent results in fine-grained rounding error analysis* at the SCAN 2018 conference (Tokyo, September 10–15, 2018).
- Jean-Michel Muller gave an invited talk *Arithmétique et précision des calculs sur ordinateurs* at the conference *Tous mesureurs, tous mesurés*, organised by the INSHS and INP Institutes of CNRS, Paris, October 18-19, 2018.
- Benoît Libert gave an invited talk *New Applications of the Lossy Mode of LWE* at the *Chinacrypt 2018* conference, organised by the Chinese Association for Cryptologic Research (CACR) in Chengdu (China) on October 27-28, 2018.
- Damien Stehlé gave an invited talk *On algebraic variants of the LWE problem* at the ICERM workshop *Computational Challenges in the Theory of Lattices*, Providence (RI), on April 23-28, 2018. He also gave an invited talk on the same topic at the *Cryptography and Algorithmic Number Theory* workshop, held in Caen on June 20-22, 2018.

- Elena Kirshanova gave an invited talk *Sieving algorithms for the Shortest Vector Problem* at the *Joint Meeting of the Korean Mathematical Society and the German Mathematical Society*, held in Seoul, Korea, on October 3-6, 2018.
- Gottfried Herold gave an invited talk *Sieving in Practice* at the *Joint Meeting of the Korean Mathematical Society and the German Mathematical Society*, held in Seoul, Korea, on October 3-6, 2018.
- Jean-Michel Muller gave an invited talk *Make computer arithmetic great again* at a panel session on the future of computer arithmetic at Arith-25, 25-27 june 2018.
- Bruno Salvy gave an invited tutorial talk at STACS'2018 on random generation of combinatorial structures.

10.1.5. Leadership within the Scientific Community

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

Jean-Michel Muller is co-director of the *Groupement de Recherche Informatique Mathématique* (GDR IM) of CNRS; he chaired the HCERES evaluation committees of IRIF (UMR 8243, march 2018) and LIX (UMR 7161, october 2018); he is a member of the Scientific Concil of CERFACS; he participated to the jury of the *Prix La Recherche* award in 2018.

Alain Passelègue is a member of the steering committee of the *Groupe de Travail Codage et Cryptographie* (GT-C2) of the GDR-IM.

Bruno Salvy was a member of the HCERES evaluation committees of IRIF.

Damien Stehlé was a member of the jury for *prix de thèse SIF*.

10.1.6. Research Administration

Gilles Villard is a member of the *Section 6* of the *Comité national de la recherche scientifique*.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master: Claude-Pierre Jeannerod, Nathalie Revol, *Algorithmique numérique et fiabilité des calculs en arithmétique flottante* (24h), M2 ISFA (Institut de Science Financière et d'Assurances), Université Claude Bernard Lyon 1.

Master: Nicolas Brisebarre, Approximation Theory and Proof Assistants: Certified Computations, 18h, M2, ENS de Lyon, France

Master: Elena Kirshanova, Cryptanalysis, 18h, M2, ENS de Lyon, France

Master: Guillaume Hanrot, Cryptanalysis, 18h, M2, ENS de Lyon, France

Master: Damien Stehlé, Hard lattice problems, 36h, M2, ENS de Lyon, France

Post-graduate: Damien Stehlé, Hard lattice problems, 45h, Seoul National University, South Korea

Master: Elena Kirshanova, Computer Algebra, 10h, M1, ENS de Lyon, France

Master: Alexandre Wallet, Computer Algebra, 10h, M1, ENS de Lyon, France

Master: Guillaume Hanrot, Computer Algebra, 10h, M1, ENS de Lyon, France

Master: Bruno Salvy, Computer Algebra, 9h, MPRI, Paris, France

Master: Bruno Salvy, Logic and Complexity, 32h, École polytechnique, France

Master: Vincent Lefèvre, Computer arithmetic, 12h, M2 ISFA (Institut de Science Financière et d'Assurances), Université Claude Bernard Lyon 1.

Bachelor: Bruno Salvy, Design and Analysis of Algorithms, 15h, École polytechnique, France

Post-graduate: Bruno Salvy, Experimental Mathematics, 3h, Atelier jeunes chercheurs, St-Flour, France

Post-graduate: Bruno Salvy, Recent algorithms in symbolic summation and integration, 4h, Journées Louis Antoine, Rennes, France

Master: Fabien Laguillaumie, Cryptography, Security, Université Claude Bernard Lyon 1, 150h

Post-graduate : Fabien Laguillaumie, 2-party Computation and Homomorphic Encryption, 1h, École Cyber in Occitanie, France

10.2.2. Supervision

PhD: Fabrice Mouhartem, Privacy-preserving cryptography from pairings and lattices, ENS de Lyon (UdL), 18/10/2018, Benoît Libert

PhD in progress: Radu Titiu, Pseudo-random functions and functional encryption from lattices, ENS de Lyon (UdL), 01/01/2017, Benoît Libert

PhD in progress: Chen Qian, Additively homomorphic encryption and its applications, ENS de Lyon (UdL), 01/09/2016, Benoît Libert

PhD: Weiqiang Wen, Contributions to the hardness foundations of lattice-based cryptography, ENS de Lyon (UdL), 01/09/2015, Damien Stehlé

PhD in progress: Miruna Rosca, Algebraic variants of the LWE problem, ENS de Lyon (UdL), 01/01/2017, Damien Stehlé

PhD in progress: Alice Pellet–Mary, obfuscation cryptanalysis, ENS de Lyon (UdL), 01/09/2016, Damien Stehlé

PhD in progress: Huyen Nguyen, mathematical foundations of lattice-based cryptography, ENS de Lyon (UdL), 01/09/2018, Damien Stehlé

PhD in progress: Florent Bréhard, Outils pour un calcul numérique certifié -Applications aux systèmes dynamiques et à la théorie du contrôle, Ens de Lyon (UdL), 01/09/2016, Nicolas Brisebarre, Mioara Joldeş (CRNS, LAAS) et Damien Pous (CNRS, LIP, Plume)

PhD in progress: Adel Hamdi, Chiffrement fonctionnel pour le traitement de données externes en aveugle, UCBL (UdL) & Orange, 07/12/2017, Sébastien Canard (Orange), Fabien Laguillaumie

PhD in progress: Ida Tucker, Conception de systèmes cryptographiques avancés reposant sur des briques homomorphes, Ens de Lyon (UdL) et Université de Bordeaux, 17/10/2017, Guilhem Castagnos (IMB, Université de Bordeaux), Fabien Laguillaumie

10.2.3. Committees

Benoît Libert: reviewer for the PhD thesis of Pierre-Alain Dupont, ENS, 29/08/2018.

Damien Stehlé: reviewer for the PhD thesis of Thomas Ricosset, ENSEEIHT, 12/11/2018; reviewer for the PhD thesis of Ilaria Chillotti, UVSQ, 17/05/2018; examiner for the PhD thesis of Rachel Player, Royal Holloway University of London, 19/03/2018; president for the PhD thesis of Guillaume Bonnoron, Ecole nationale supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire, 15/03/2018; jury member for the PhD thesis of Quentin Santos, ENS, 20/12/2018.

Bruno Salvy: member of the HdR committee of Guillaume Chapuy, IRIF, April and of Enrica Duchi, IRIF, November; reviewer for the PhD thesis of Pablo Rotondo, IRIF, September.

Fabien Laguillaumie: reviewer for the PhD thesis of Raphaël Bost, Université Rennes 1, 08/01/2018, Xavier Bultel, Université Clermont Auvergne, 17/05/2018, Vincent Zucca, Sorbonne Université, 25/06/2018, Quentin Santos, ENS, 20/12/2018

Nathalie Revol: examiner for the PhD thesis of Romain Picot, Université Paris 6, 27/03/2018

10.3. Popularization

10.3.1. Internal or external Inria responsibilities

- Nathalie Revol is a member of the editorial board of interstices; she belongs to the steering committee of MMI (Maison des Mathématiques et de l'Informatique, Lyon)
- Bruno Salvy is “référent chercheur” for the Inria Grenoble Center.

10.3.2. Articles and contents

Nathalie Revol belonged to the working group that elaborated the "7 families of computer science" playcards

10.3.3. Education

Nathalie Revol taught "Dissemination of Scientific Knowledge", 10h, to the 4th year students (between Master and PhD) of ENS de Lyon, France. She has been invited to a panel about "Flashmob" type activities, at ESOF 2018 (EuroScience Open Forum), July 9–14, 2018, Toulouse, France.

Nathalie Revol works with DANE (Délégation Académique au Numérique dans l'Éducation) of Rectorat de Lyon towards educating primary school teachers, by educating educators. She has been invited to present her past activities, using educational robots, at 3es Rencontres Nationales de la Robotique Éducative, October 2–3, Lyon, France.

10.3.4. Interventions

Laurent Grémy and Fabrice Mouhartem gave talks at *Fête de la Science* for a general audience. Nathalie Revol gave talks at *Fête de la Science* for 3 classes (9 years old, 11 years old and 13 years old).

As an incentive for high-school pupils, and especially girls, to choose scientific careers, Nathalie Revol gave talks at Lycée Ella Fitzgerald (Saint-Romain-en-Gal) and Mondial des Métiers (in February 2018). With Jérôme Germoni and Natacha Portier, she organized a day *Filles & Info* in March 2018, gathering about 100 high-school girls of 1e S. She was part of the panel discussing with the audience after the movie "Les figures de l'ombre - Hidden figures" at Comoedia cinema in Lyon in March 2018.

Damien Stehlé received at ENS de Lyon several winning teams of the Alkindi highschool competition. Alice Pellet–Mary and Fabrice Mouhartem gave talks at this event.

11. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] F. MOUHARTEM. *Privacy-preserving cryptography from pairings and lattices*, Université de Lyon, October 2018, https://tel.archives-ouvertes.fr/tel-01913872

[2] W. WEN. *Contributions to the hardness foundations of lattice-based cryptography*, Université de Lyon, November 2018, https://tel.archives-ouvertes.fr/tel-01949339

Articles in International Peer-Reviewed Journals

[3] M. ABDALLA, F. BENHAMOUDA, A. PASSELÈGUE, K. PATERSON. *Related-Key Security for Pseudorandom Functions Beyond the Linear Barrier*, in "Journal of Cryptology", October 2018, vol. 31, n^{o} 4, pp. 917-964 [*DOI :* 10.1007/s00145-017-9274-8], https://hal.inria.fr/hal-01723012

[4] B. ALLOMBERT, N. BRISEBARRE, A. LASJAUNIAS. *On a two-valued sequence and related continued fractions in power series fields*, in "The Ramanujan Journal", 2018, vol. 45, n^{o} 3, pp. 859-871, https://arxiv.org/abs/1607.07235 [*DOI :* 10.1007/s11139-017-9892-7], https://hal.archives-ouvertes.fr/hal-01348576

[5] S. BAI, T. LEPOINT, A. ROUX-LANGLOIS, A. SAKZAD, D. STEHLÉ, R. STEINFELD. *Improved Security Proofs in Lattice-Based Cryptography: Using the Rényi Divergence Rather than the Statistical Distance*, in "Journal of Cryptology", April 2018, vol. 31, n^o 2, pp. 610 - 640 [*DOI :* 10.1007/s00145-017-9265-9], https://hal.archives-ouvertes.fr/hal-01934177

[6] N. BRISEBARRE, S.-I. FILIP, G. HANROT. *A Lattice Basis Reduction Approach for the Design of Finite Wordlength FIR Filters*, in "IEEE Transactions on Signal Processing", 2018, vol. 66, n^o 10, pp. 2673-2684 [*DOI :* 10.1109/TSP.2018.2812739], https://hal.inria.fr/hal-01308801

[7] F. BRÉHARD, N. BRISEBARRE, M. JOLDES. *Validated and numerically efficient Chebyshev spectral methods for linear ordinary differential equations*, in "ACM Transactions on Mathematical Software", July 2018, vol. 44, n^o 4, pp. 44:1-44:42 [*DOI :* 10.1145/3208103], https://hal.archives-ouvertes.fr/hal-01526272

[8] L. DUCAS, E. KILTZ, T. LEPOINT, V. LYUBASHEVSKY, P. SCHWABE, G. SEILER, D. STEHLÉ. *CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme*, in "IACR Transactions on Cryptographic Hardware and Embedded Systems", 2018, https://hal.archives-ouvertes.fr/hal-01934176

[9] G. HEROLD, E. KIRSHANOVA, A. MAY. *On the asymptotic complexity of solving LWE*, in "Designs, Codes and Cryptography", January 2018, vol. 86, n^o 1, pp. 55 - 83 [*DOI :* 10.1007/s10623-016-0326-0], https://hal.archives-ouvertes.fr/hal-01934181

[10] C.-P. JEANNEROD, S. M. RUMP. *On relative errors of floating-point operations: optimal bounds and applications*, in "Mathematics of Computation", 2018, vol. 87, pp. 803-819 [*DOI :* 10.1090/MCOM/3234], https://hal.inria.fr/hal-00934443

[11] B. SALVY. *Linear Differential Equations as a Data-Structure*, in "Foundations of Computational Mathematics", 2018, pp. 1-35, https://arxiv.org/abs/1811.08616 - Based on an invited talk at FoCM'2017, https://hal.inria.fr/hal-01940078

[12] A. VOLKOVA, M. ISTOAN, F. DE DINECHIN, T. HILAIRE. *Towards Hardware IIR Filters Computing Just Right: Direct Form I Case Study*, in "IEEE Transactions on Computers", 2018 [*DOI :* 10.1109/TC.2018.2879432], https://hal.sorbonne-universite.fr/hal-01561052

Invited Conferences

[13] B. SALVY. *Recursive Combinatorial Structures: Enumeration, Probabilistic Analysis and Random Generation*, in "STACS 2018 - 35th Symposium on Theoretical Aspects of Computer Science", Caen, France, February 2018, Tutorial [*DOI :* 10.4230/LIPICS.STACS.2018.1], https://hal.inria.fr/hal-01926094

International Conferences with Proceedings

[14] P. R. ARANTES GILZ, F. BRÉHARD, C. GAZZINO. *Validated Semi-Analytical Transition Matrices for Linearized Relative Spacecraft Dynamics via Chebyshev Series Approximations*, in "SCITECH 2018 - AIAA Science and Technology Forum and Exposition, 28th Space Flight Mechanics Meeting", Kissimmee, United States, SCITECH 2018-AIAA Science and Technology Forum and Exposition, 28th Space Flight Mechanics Meeting, American Institute of Aeronautics and Astronautics, January 2018, pp. 1-23 [*DOI :* 10.2514/6.2018-1960], https://hal.archives-ouvertes.fr/hal-01540170

[15] S. BAI, D. STEHLÉ, W. WEN. *Measuring, Simulating and Exploiting the Head Concavity Phenomenon in BKZ*, in "ASIACRYPT", Brisbane, Australia, 2018, https://hal.archives-ouvertes.fr/hal-01934174

[16] D. Boneh, Y. Ishai, A. Passelègue, A. Sahai, D. J. Wu. *Exploring Crypto Dark Matter: New Simple PRF Candidates and Their Applications*, in "TCC 2018 - Theory of Cryptography Conference", Goa, India, LNCS, Springer, November 2018, vol. 11240, pp. 699-729 [*DOI :* 10.1007/978-3-030-03810-6_25], https://hal.inria.fr/hal-01929288

[17] J. W. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. Schanck, P. Schwabe, G. Seiler, D. Stehlé. *CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM*, in "EuroS&P 2018 - IEEE European Symposium on Security and Privacy", London, United Kingdom, IEEE, April 2018, pp. 353-367 [*DOI :* 10.1109/EuroSP.2018.00032], https://hal.archives-ouvertes.fr/hal-01934169

[18] A. Bostan, F. Chyzak, P. Lairez, B. Salvy. *Generalized Hermite Reduction, Creative Telescoping and Definite Integration of D-Finite Functions*, in "ISSAC 2018 - International Symposium on Symbolic and Algebraic Computation", New York, United States, July 2018, pp. 1-8 [*DOI :* 10.1145/3208976.3208992], https://hal.inria.fr/hal-01788619

[19] Z. Brakerski, A. Jain, I. Komargodski, A. Passelègue, D. Wichs. *Non-Trivial Witness Encryption and Null-iO from Standard Assumptions*, in "SCN 2018 - International Conference on Security and Cryptography for Networks", Amalfi, Italy, LNCS, Springer, September 2018, vol. 11035, pp. 425-441 [*DOI :* 10.1007/978-3-319-98113-0_23], https://hal.inria.fr/hal-01929279

[20] Z. Brakerski, E. Kirshanova, D. Stehlé, W. Wen. *Learning with Errors and Extrapolated Dihedral Cosets*, in "PKC 2018 - 21st International Conference on Practice and Theory of Public Key Cryptography", Rio de Janeiro, Brazil, March 2018, https://hal.archives-ouvertes.fr/hal-01934165

[21] N. Brisebarre, G. Constantinides, M. Ercegovac, S.-I. Filip, M. Istoan, J.-M. Muller. *A High Throughput Polynomial and Rational Function Approximations Evaluator*, in "ARITH 2018 - 25th IEEE Symposium on Computer Arithmetic", Amherst, MA, United States, IEEE, June 2018, pp. 99-106 [*DOI :* 10.1109/ARITH.2018.8464778], https://hal.inria.fr/hal-01774364

[22] F. Bréhard. *A Newton-like Validation Method for Chebyshev Approximate Solutions of Linear Ordinary Differential Systems*, in "ISSAC 2018 - 43rd International Symposium on Symbolic and Algebraic Computation", New York, United States, ISSAC 2018-43rd International Symposium on Symbolic and Algebraic Computation, ACM, July 2018, pp. 103-110 [*DOI :* 10.1145/3208976.3209000], https://hal.archives-ouvertes.fr/hal-01654396

[23] G. Castagnos, F. Laguillaumie, I. Tucker. *Practical Fully Secure Unrestricted Inner Product Functional Encryption modulo p*, in "ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security", Brisbane, Australia, T. Peyrin, S. Galbraith (editors), Advances in Cryptology – ASIACRYPT 2018, December 2018, vol. LNCS, n^{o} 11273, pp. 733-764, https://hal.archives-ouvertes.fr/hal-01934296

[24] J. Chen, J. Gong, L. Kowalczyk, H. Wee. *Unbounded ABE via Bilinear Entropy Expansion, Revisited*, in "EUROCRYPT 2018 - Annual International Conference on the Theory and Applications of Cryptographic Techniques", Tel Aviv, Israel, J. B. Nielsen, V. Rijmen (editors), LNCS - Lecture Notes in Computer Science, Springer, April 2018, vol. 10820, pp. 503-534 [*DOI :* 10.1007/978-3-319-78381-9_19], https://hal.inria.fr/hal-01899901

[25] J. CHEN, J. GONG, H. WEE. *Improved Inner-product Encryption with Adaptive Security and Full Attribute-hiding*, in "ASIACRYPT 2018 - 24th Annual International Conference on the Theory and Application of Cryptology and Information Security", Brisbane, Australia, December 2018, https://hal.inria.fr/hal-01900153

[26] J. CHEN, D. STEHLÉ, G. VILLARD. *Computing an LLL-reduced Basis of the Orthogonal Lattice*, in "ISSAC 2018, 43rd International Symposium on Symbolic and Algebraic Computation (ISSAC 2018)", New York, United States, July 2018, https://arxiv.org/abs/1805.03418 [*DOI :* 10.1145/3208976.3209013], https://hal.archives-ouvertes.fr/hal-01921335

[27] C. CHUENGSATIANSUP, C. MARTINDALE. *Pairing-friendly twisted Hessian curves*, in "Indocrypt 2018 - 19th International Conference on Cryptology", New Delhi, India, December 2018, https://hal.archives-ouvertes.fr/hal-01934160

[28] L. DUCAS, A. PELLET–MARY. *On the Statistical Leak of the GGH13 Multilinear Map and some Variants*, in "Asiacrypt 2018", Brisbane, Australia, December 2018, pp. 465-493, https://hal.archives-ouvertes.fr/hal-01895645

[29] J. GONG, B. LIBERT, S. C. RAMANNA. *Compact IBBE and Fuzzy IBE from Simple Assumptions*, in "SCN 2018 - 11th Conference on Security and Cryptography for Networks", Amalfi, Italy, Security and Cryptography for Networks (SCN) 2018, September 2018, pp. 1-29, https://hal.inria.fr/hal-01686690

[30] L. GRÉMY. *Higher dimensional sieving for the number field sieve algorithms*, in "ANTS 2018 - Thirteenth Algorithmic Number Theory Symposium", Madison, United States, University of Wisconsin, July 2018, pp. 1-16, https://hal.inria.fr/hal-01890731

[31] G. HEROLD, E. KIRSHANOVA, T. LAARHOVEN. *Speed-Ups and Time-Memory Trade-Offs for Tuple Lattice Sieving*, in "PKC 2018 - 21st International Conference on Practice and Theory of Public Key Cryptography", Rio de Janeiro, Brazil, March 2018, https://hal.archives-ouvertes.fr/hal-01934183

[32] C.-P. JEANNEROD, J.-M. MULLER, P. ZIMMERMANN. *On various ways to split a floating-point number*, in "ARITH 2018 - 25th IEEE Symposium on Computer Arithmetic", Amherst (MA), United States, IEEE, June 2018, pp. 53-60 [*DOI :* 10.1109/ARITH.2018.8464793], https://hal.inria.fr/hal-01774587

[33] M. JOYE, A. PASSELÈGUE. *Function-Revealing Encryption: Definitions and Constructions*, in "SCN 2018 - International Conference on Security and Cryptography for Networks", Amalfi, Italy, LNCS, Springer, September 2018, vol. 11035, pp. 527-543 [*DOI :* 10.1007/978-3-319-98113-0_28], https://hal.inria.fr/hal-01929272

[34] E. KIRSHANOVA. *Improved Quantum Information Set Decoding*, in "PQCrypto 2018 - The Ninth International Conference on Post-Quantum Cryptography", Fort Lauderdale, United States, April 2018, https://hal.archives-ouvertes.fr/hal-01934186

[35] J. LI, J. GONG. *Improved Anonymous Broadcast Encryptions: Tight Security and Shorter Ciphertext*, in "ACNS 2018 - 16th International Conference on Applied Cryptography and Network Security", Leuven, Belgium, Springer, July 2018, pp. 497-515 [*DOI :* 10.1007/978-3-319-93387-0_26], https://hal.archives-ouvertes.fr/hal-01829132

[36] B. LIBERT, S. LING, K. NGUYEN, H. WANG. *Lattice-Based Zero-Knowledge Arguments for Integer Relations*, in "CRYPTO 2018 - Annual International Cryptology Conference", Santa Barbara, United States,

Springer, August 2018, vol. LNCS, n^{o} 10992, pp. 700-732 [*DOI :* 10.1007/978-3-319-96881-0_24], https://hal.inria.fr/hal-01911886

[37] B. LIBERT, T. PETERS, C. QIAN. *Logarithmic-Size Ring Signatures With Tight Security from the DDH Assumption*, in "ESORICS 2018 - 23rd European Symposium on Research in Computer Security", Barcelone, Spain, LNCS, Springer, September 2018, vol. 11099, pp. 288-308 [*DOI :* 10.1007/978-3-319-98989-1_15], https://hal.inria.fr/hal-01848134

[38] B. LIBERT, D. STEHLÉ, R. TITIU. *Adaptively Secure Distributed PRFs from LWE*, in "TCC 2018 - 16th International Conference on Theory of Cryptography", Panaji, India, LNCS, Springer, November 2018, vol. 11240, pp. 391-421 [*DOI :* 10.1007/978-3-030-03810-6_15], https://hal.inria.fr/hal-01911887

[39] A. PELLET–MARY. *Quantum Attacks against Indistinguishablility Obfuscators Proved Secure in the Weak Multilinear Map Model*, in "Crypto 2018 - 38th International Cryptology Conference", Santa-Barbara, United States, Springer, August 2018, pp. 153-183 [*DOI :* 10.1007/978-3-319-96878-0_6], https://hal.archives-ouvertes.fr/hal-01895639

[40] M. ROCA, D. STEHLÉ, A. WALLET. *On the Ring-LWE and Polynomial-LWE Problems*, in "EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications", Tel Aviv, Israel, April 2018, https://hal.archives-ouvertes.fr/hal-01934170

[41] R. SERRA, D. ARZELIER, F. BRÉHARD, M. JOLDES. *Fuel-optimal impulsive fixed-time trajectories in the linearized circular restricted 3-body-problem*, in "IAC 2018 - 69th International Astronautical Congress; IAF Astrodynamics Symposium", Bremen, Germany, CSA/IAF Special issue IAF Astrodynamics Symposium (69TH international astronautical congress), International Astronautical Federation, October 2018, pp. 1-9, https://hal.archives-ouvertes.fr/hal-01830253

[42] *Best Paper*
G. VILLARD. *On Computing the Resultant of Generic Bivariate Polynomials*, in "ISSAC 2018, 43rd International Symposium on Symbolic and Algebraic Computation, New York, USA, July 16-19, 2018", New York, United States, July 2018, https://hal.archives-ouvertes.fr/hal-01921369.

Scientific Books (or Scientific Book chapters)

[43] J.-M. MULLER, N. BRUNIE, F. DE DINECHIN, C.-P. JEANNEROD, M. JOLDES, V. LEFÈVRE, G. MELQUIOND, N. REVOL, S. TORRES. *Handbook of Floating-point Arithmetic (2nd edition)*, Birkhäuser Basel, July 2018, pp. 1-627 [*DOI :* 10.1007/978-3-319-76526-6], https://hal.inria.fr/hal-01766584

Other Publications

[44] N. BRISEBARRE, M. JOLDES, J.-M. MULLER, A.-M. NANEŞ, J. PICOT. *Error analysis of some operations involved in the Fast Fourier Transform*, December 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01949458

[45] N. FABIANO, J.-M. MULLER. *Algorithms for triple-word arithmetic*, September 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01869009

[46] C.-P. JEANNEROD, V. NEIGER, G. VILLARD. *Fast computation of approximant bases in canonical form*, January 2018, working paper or preprint, https://hal-unilim.archives-ouvertes.fr/hal-01683632

[47] F. QURESHI, A. VOLKOVA, T. HILAIRE, J. TAKALA. *Multiplierless Processing Element for Non-Power-of-Two FFTs*, January 2018, working paper or preprint, https://hal.inria.fr/hal-01690832

[48] A. VOLKOVA, T. HILAIRE, C. LAUTER. *Arithmetic approaches for rigorous design of reliable Fixed-Point LTI filters*, November 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01918650

[49] F. DE DINECHIN, L. FORGET, J.-M. MULLER, Y. UGUEN. *Posits: the good, the bad and the ugly*, December 2018, working paper or preprint, https://hal.inria.fr/hal-01959581